



POLICÍA 3.0 REDES SOCIALES EN LA NUEVA DIMENSIÓN DE LA SEGURIDAD



PUBLICACIONES
DE LA FUNDACIÓN POLICÍA ESPAÑOLA
Colección Estudios de Seguridad



POLICÍA 3.0 REDES SOCIALES EN LA NUEVA DIMENSIÓN DE LA SEGURIDAD

**PUBLICACIONES
DE LA FUNDACIÓN POLICÍA ESPAÑOLA**
Colección Estudios de Seguridad

Con la colaboración de:

Telefonica

Edita: Fundación Policía Española
Conde de Aranda, 16, 3º Izq.
e-mail: iep@dgp.mir.es
Coordinador Editorial:
José Cabanillas Sánchez
Equipo Editorial:
María Dolores Guede Fernández
Equipo de Traducción:
IEP
Imprime: Tecnología Gráfica
Maquetación: Félix Gil
ISBN: 978-84-616-4472-8
Depósito legal: M18551-2013

Todos los derechos reservados.

No se permite la reproducción total o parcial de este libro,
ni su incorporación a un sistema informático, ni su transmisión en cualquier forma
o por cualquier medio, sea éste electrónico, mecánico, reprográfico,
gramofónico u otro, sin el permiso previo y por escrito
de los titulares del copyright.

ÍNDICE

<u>PRESENTACIÓN</u>	7-9
---------------------	-----

CONFERENCIA INAUGURAL

- José Manuel Pérez Pérez Subdirector General del Gabinete Técnico de la Dirección General de la Policía	13
---	----

PRIMER PANEL

- El impacto de las redes sociales en la sociedad actual. Dionisio Fernández Nespral Gerente de Innovación de Everis	17
- Crimen organizado y nuevas tecnologías. Francisco Javier Rodríguez Rodríguez Inspector del Cuerpo Nacional de Policía. Miembro del Grupo II, de la Brigada de Investigación Tecnológica, de Fraudes en Internet	49
Luis García Pascual Inspector Jefe del Cuerpo Nacional de Policía. Jefe del Grupo Operativo I, de la Brigada de Investigación Tecnológica, de Protección al Menor	55
César Lorenzana González Capitán de la Guardia Civil. Miembro del Grupo de Delitos Telemáticos de la Unidad Central Operativa (UCO)	61

SEGUNDO PANEL

- Las redes sociales y la transformación de la gestión pública. Eduardo Baeza Pérez-Fontán Director del Departamento de Análisis y Estudios. Gabinete de la Presidencia del Gobierno	69
Andrés Medina Medina Director de Programas de Análisis y Estudios. Gabinete de la Presidencia del Gobierno	77
- Redes sociales y protección de datos personales. Antonio Troncoso Reigada Profesor Titular de Derecho Constitucional. Universidad de Cádiz	97
- Proteger a los menores en las redes sociales. Arturo Canalda González Defensor del Menor de la Comunidad de Madrid (2006-2012)	147
Celia Carreira Vigo Inspectora del Cuerpo Nacional de Policía. Jefa del Grupo III, de la Brigada de Investigación Tecnológica, de Protección al Menor	153
Jorge Villamayor Ibías Inspector del Cuerpo Nacional de Policía. Jefe del Grupo de Delitos Tecnológicos de la Brigada Provincial de la Policía Judicial de Madrid	177

TERCER PANEL

- Redes sociales y nuevas formas de delincuencia. 193
Manuel Vázquez López
Comisario Principal del Cuerpo Nacional de Policía.
Jefe de la Brigada de Investigación Tecnológica de la UDEF Central
- Ciberterrorismo. 203
Alfonso Estévez Ochoa
Inspector Jefe del Cuerpo Nacional de Policía
- Manuel Enrique Marlasca García* 215
Periodista

CUARTO PANEL

- Redes sociales y colaboración ciudadana en la acción policial. 225
Juan José Esteban Servus
Director de Comunicación de la Dirección General de la Policía
- Policía 3.0. 247
Santiago Cuadro Jaén
Excomisario General de Seguridad Ciudadana (1996-2004)
- Redes sociales y delitos sexuales. 261
Alfonso San Román Ibarrondo
Fiscal Delegado de Criminalidad Informática de Madrid
- Manuel Alcaide Alcaide* 277
Inspector Jefe del Cuerpo Nacional de Policía.
Jefe de la Sección de Delitos Sexuales y Servicio de Atención a la Mujer (SAM) de Madrid
- Beatriz Ramos Iglesias* 289
Inspectora del Cuerpo Nacional de Policía.
Jefa del Grupo II, de la Brigada de Investigación Tecnológica, de Protección al Menor

QUINTO PANEL

- El uso de las redes sociales en la empresa. 305
Manuel Carpio Cámara
Director de Seguridad de la Información y Prevención del Fraude de Telefónica
- La autorregulación como sistema de protección de la seguridad 313
en las redes sociales: el caso de Tuenti.
Óscar Casado Oliva
Director de la Asesoría Jurídica de Tuenti. Grupo Telefónica

CLAUSURA

- José Cabanillas Sánchez* 339
Director General de la Fundación Policía Española y Director del curso
- Mercedes Molina Ibáñez* 341
Vicerrectora de Transferencia de la Universidad Complutense de Madrid.
Directora General de la Fundación General de la Universidad Complutense de Madrid
- Ignacio Cosidó Gutiérrez* 345
Director General de la Policía

Presentación del curso

Los seres humanos de nuestro tiempo operan en dos escenarios paralelos: el tradicional o real y el virtual o del ciberespacio. En ambos tienen problemas de seguridad y es deber de las Fuerzas y Cuerpos de Seguridad garantizarla.

La Estrategia Española de Seguridad define el “Ciberespacio”, como: *“el espacio virtual donde se agrupan y relacionan usuarios, líneas de comunicación, páginas web, foros, servicios de Internet y otras redes. Creado por el ser humano es un entorno singular para la seguridad, sin fronteras geográficas, anónimo, asimétrico, que puede ser utilizado de forma casi clandestina y sin necesidad de desplazamientos. Es mucho más que la Red, pues incluye también dispositivos como los teléfonos móviles, la televisión terrestre y las comunicaciones por satélite”*.

El ciberespacio no solo genera problemas de seguridad virtuales sino que afecta a la vida, integridad física, patrimonio, una larga lista de derechos y libertades públicas que defendemos en el mundo real y que parecen no preocuparnos en el mundo virtual. No tenemos inconveniente en que perfiles de nuestra identidad se generen y circulen en Internet, y no solo en las redes sociales.

Gracias al ciberespacio, cada día operamos en mayor medida en redes o grupos, como los descritos por McLuhan en su *Aldea global*, donde también hay terroristas, ladrones, matones y la delincuencia organizada se mueve con medios y soltura. También puede verse afectada la seguridad interior y exterior del Estado y el funcionamiento de los servicios públicos esenciales. Son las ciberamenazas.

Las redes sociales en Internet están cambiando la forma de comunicarnos y permiten a las personas ser ellas y también su “alter ego” (alteri) o quien quieren ser, planteándose el eterno conflicto del bien y el mal, dentro de un aparente escenario de anonimato, con consecuencias para la seguridad.

Queremos reflexionar sobre ello en este Curso.

José Cabanillas Sánchez
Director General de la Fundación Policía Española
y Director del curso

Presentación de la Fundación Policía Española

La Fundación Policía Española es una entidad privada de carácter cultural y sin ánimo de lucro que fue constituida en el año 1999. Según establecen sus estatutos, sus funciones generales son: formación asistencial, educación, asistencias sociales y formativas, y están dirigidas, principalmente, a los miembros del Cuerpo Nacional de Policía y a incrementar la imagen y prestigio del Cuerpo entre la sociedad. Para lograr estos fines, la Fundación lleva a cabo diversas actividades culturales, tales como: cursos, exposiciones y la publicación de libros, siendo algunos de los títulos difundidos: *Hacia una policía europea*, *Blanqueo de capitales, fuente de dinero negro*, *Violencia, edad y género*, y *Globalidad y delincuencia*. Las escasas acciones que no puede llevar a cabo se deben a razones ajenas a la Fundación.

9

La Fundación se financia con el patrocinio de entidades privadas, y está regulada e inscrita en el Registro General de Fundaciones del Ministerio de Cultura, dando cuenta de sus resultados económicos al protectorado del Ministerio, responsable del control de las fundaciones. En el primer trimestre de cada año, la Fundación Policía Española presenta al protectorado su Memoria anual de Actividades, que incluye un control económico de los proyectos que ha realizado en el ejercicio analizado y una planificación de los previstos para el año en curso, junto con el desarrollo planificado para ese ejercicio.

La institución está gobernada por una Junta Rectora, constituida por un presidente y un consejo de patronos. Todos sus miembros han ocupado cargos en la Dirección General de la Policía.

En aras de ampliar sus actuaciones, la Fundación ha constituido en 2012 sus Premios de Periodismo, destinados a premiar los artículos de prensa que pongan de relieve la mejor y mayor actividad del Cuerpo Nacional de Policía. Está previsto que instituya otros galardones para reconocer los valores humanos que representan estos funcionarios en su trabajo diario, tales como la solidaridad, la entrega a los demás, etc. Ese tipo de virtudes son los que se van a tener en cuenta en la concesión de esas nuevas distinciones.

En ese grupo de proyectos cumplidos también se enmarca su nueva **web: www.fundacionpoliciaespañola.es**, que dispone de toda la información relativa a la Fundación.

El decimocuarto curso de la Fundación Policía Española, “Policía 3.0: Redes Sociales en la nueva dimensión de la seguridad”, copatrocinado por las entidades privadas **Banco Santander y Telefónica**, pretende dar a conocer las nuevas herramientas con que trabaja la policía en el actual mundo globalizado, en el que hay un espacio real y uno virtual, el ciberespacio, a través del cual todas las ramas de la delincuencia llevan a cabo sus acciones con mayor anonimato y, sobre todo, con más facilidad a través de las redes sociales. Son ciberamenazas, y la policía está desarrollando métodos y estrategias para prevenirlas y reprimirlas, pues afectan a la seguridad virtual, física y personal, van en contra de las personas, del patrimonio, contra la libertad sexual, etc. Esta delincuencia internacional, estas mafias, tienen en las redes sociales una herramienta muy fácil para ellos, que la policía combate con todos los medios que están a su alcance.

Miguel Ángel Alonso de la Fuente
Patrono de la Fundación Policía Española



CONFERENCIA INAUGURAL

JOSÉ MANUEL PÉREZ PÉREZ
Subdirector General del Gabinete Técnico
de la Dirección General de la Policía

La elección de la temática “Policía 3.0: Redes Sociales en la nueva dimensión de la seguridad” es el resultado de la búsqueda del contenido más novedoso, de mayor interés e influencia hoy día, un tema que se ha puesto de moda a una velocidad increíblemente rápida.

Actualmente, el Cuerpo Nacional de Policía (CNP) es la segunda policía del mundo con más *tuiteros*, 215.000 seguidores en *twitter@policia*, después del Federal Bureau of Investigation (FBI) estadounidense. Cuando el CNP puso en marcha ese canal en el microblog Twitter, analizaron sus ventajas e inconvenientes. Entre las primeras destacan las pistas o datos que se han proporcionado en más de 2.000 investigaciones, y entre las segundas que se utiliza para entorpecer el trabajo de los funcionarios de policía. A pesar de eso, es necesario ir por delante del delincuente, aunque, en gran parte de las ocasiones, las normas jurídicas y los medios de investigación policiales van por detrás del delincuente, también en la *ciberdelincuencia*.

13

Se estima que en pocos años la delincuencia tradicional –el atraco a un banco, el hurto, etc.– habrá desaparecido en gran parte. No hará falta arriesgarse a atracar un banco con un arma cuando será, ya es, más fácil a través de un ordenador, de las redes sociales, etc. En esa dirección se mueve ya no la delincuencia española, que ya no existe, sino la delincuencia mundial.

En el seno de la Unión Europea cualquier banda, que suele estar integrada por miembros de distintas nacionalidades (españoles, italianos, rumanos, etc.), se desplaza allá donde puede obtener rentabilidad, en función de qué medios y con la mayor impunidad, y las redes sociales facilitan esos movimientos y esa sensación, o esa realidad más que sensación, de impu-

nidad. Son delitos muy difíciles de perseguir, ya que, mientras se gestionan y controlan desde cualquier punto del globo, se está atacando en el otro extremo de la Tierra, con lo cual hay que llegar al origen y conocer la legislación de aquel país.

Las redes sociales son de una trascendencia tremenda y muy importante para la Policía.



PRIMER PANEL

EL IMPACTO DE LAS REDES SOCIALES EN LA SOCIEDAD ACTUAL

DIONISIO FERNÁNDEZ NESPRAL
Gerente de Innovación de Everis

*Es probable que en los próximos años todo el mundo pueda entender,
adaptarse y crecer dentro de la Red, aunque la sociedad va
a una velocidad tal que en la empresa, en el trabajo o en el entorno
familiar no habrá tiempo para alcanzarlo todo.
Es el mundo que nos ha tocado vivir.*

17

Voy a explicar por qué las personas “se enganchan” a las redes sociales, las muchas cosas que están pasando en ese entorno y cómo pueden utilizarse en el ámbito laboral. Al final, actuar en las redes sociales es una cuestión que depende, casi exclusivamente, de cada persona.

En la Red hay que tener una identidad potente que debe ser la que el usuario quiera que aparezca, la que él ha determinado. Ha de ser una identidad igual de fuerte que la que ha desarrollado en su vida real, con su experiencia, conocimiento, trabajo. ¿Alguien considera que todo lo que hace, lo que ha hecho y lo que puede hacer está también representado en la Red?, la respuesta en la mayoría de las ocasiones es “No”. Éste es uno de los grandes errores que ha cometido la sociedad española -lo que tenemos en la vida real no está en la vida virtual-, una de sus grandes diferencias con otras culturas como la americana, la anglosajona, los canadienses, etc.

Habría que llegar al objetivo de que todo el mundo tenga una identidad potente, ésta es una de las claves para entender la Red, porque intentar comprender Internet desde fuera es muy complejo, las redes hay que interpretarlas desde dentro.

En el libro *La lógica oculta de la vida*, de Tim Harford, hay un capítulo en el que este economista reduce la historia de la Humanidad a un año natural. El 1 de enero comienza y durante 364 días no pasa casi nada, pero en los últimos 40 minutos del último día ocurre casi todo. El hombre tardó unos diez mil años en pasar de una piedra redonda a un arma, puliéndola llegó a un arma perfecta, pero tardó otros 10.000 años. Si trasladamos esa metáfora al trabajo, ¿contaríamos con 10.000 años para hacer algo?

La vida que nos ha tocado vivir no es la que pensábamos que iba a ser, y lo que viene no lo podemos imaginar. Pero sí tenemos una referencia: el mundo en que vivimos es instantáneo. Y si no que se lo digan a los que leen el periódico digital que, en cuanto van dos veces a ese medio durante la misma hora, ya lo consideran obsoleto (Uno de los grandes problemas de los *mass media* es la velocidad a la que va la información). El mundo es inmediato, todo ocurre en este momento, y la capacidad de adaptarnos es muy poca.

LOS NODOS EN LA RED

18 España es, hoy día, el país de Europa que más uso hace de redes sociales, también en el trabajo. En el año 2007 éramos 100 seguidores las que usábamos Twitter y en ese grupo decíamos: “Este formato transformará en algún momento la manera en que nos vamos a comunicar”.

En la Red, y en cualquier sistema, lo importante son los nodos que la conforman y éstos son muy complicados. Bill Gates tiene siete millones de seguidores en Twitter, y eso significa que si Bill Gates un día dice: “@DioniNespral, me ha gustado mucho tu charla”, esto lo verían siete millones de usuarios de golpe. La importancia de la Red no está en lo que haces sino en los nodos de relación que tienes y en su potencia. Por tanto, cuando una persona u organización está tejiendo su red, el mayor de los problemas es qué nodos tiene, que fuerza y quién y en qué está participando. Es muy portante encontrar esos nodos y no abandonarlos, igual que en la vida real.

1/9/90

El 1 por ciento de los usuarios de la Red crean el contenido, el 9 por ciento lo distribuyen y el 90 por ciento restante escucha o lee. ¡Esto es clave! Mucha gente dice: “Estar dentro de la red social no me va”, pero eso depende del objetivo que tengas en la Red y de si eres “1”, “9” ó “90”. Si eres “90” debes estar “bien orientado” para localizar lo que quieres escuchar y, en el caso concreto, actuar. Esa es una de las grandes potencias que tiene la Red.

Durante mucho tiempo fui “1” y ahora soy más bien “90”. Tengo creada toda mi red y puedo conocer todo lo que me interesa y por tanto proceder. Cualquier cosa que ocurre en el mundo de la Red y que mí me interesa la puedo leer al momento.

En los próximos años nos tendremos que adaptar a lo que venga. La sociedad a la que nos vamos a enfrentar es, nos guste o no, hiperdigital, hiperconectada, de comunicación muy intensa. En el caso del Cuerpo Nacional de Policía, las preguntas que deben formularse son: ¿cómo podremos integrar a los próximos miembros?, ¿cómo gestionaremos su entrada en el trabajo?, ¿cómo hacemos para que convivan con nosotros?, ¿cómo se puede adaptar la actual experiencia y conocimiento a lo que ellos traen, que es pensar de otra forma distinta? Es un reto grande, el mayor que tenemos en España: la adaptación al medio. Sólo podremos conseguir lo mejor de la gente si entendemos cómo piensa.

VIVIMOS EN TRANSFORMACIÓN

¿Cómo atendemos a lo que dice la Red? Aquí se pone en funcionamiento un tema complicado: cómo se comunican las personas y qué es lo que va a comunicarse. Lo primero es entender qué es un concepto de comunicación. Cuando se produjeron los disturbios de Londres (agosto 2011), una persona grabó a la policía y lo que estaba sucediendo y lo colgó en la Red, generando así un gran ruido en ese entorno al que se sumó la acción con Blackberry, que era utilizada por mucho ciudadanos como soporte para grabar y colgarlo, el Messenger, etc. Las redes socialmente pueden tener unas consecuencias rápidas. La fuerza de la Red para esto es muy buena y hay que entenderla y aprovecharla.

19

En este momento hay que intentar discernir este tipo de nuevas situaciones para prevenirlas. La policía de todo el mundo está trabajando en ello desde arriba, pero va a jugar un papel fundamental la integración desde abajo, es decir, desde el estrato del ciudadano. Entender las redes es aprehender a quiénes las hacen, y participan en la Red y que crean los espacios para identificar, denunciar y detener a los que han causado los disturbios. Éste es el futuro para los próximos años.

Para comprenderlo es fundamental que la gente con experiencia participe, porque son los que van a poder proponer y realizar iniciativas. Lo que ocurre ahora es que la gente que delinque en la Red conoce este medio muy bien, mientras que del otro lado: el de las empresas, la policía, etc. no existen personas con experiencia y con un manejo de ese entorno tan profundo. Y esto es el salto evidente que en todas las organizaciones se han

dado cuenta que deben dar. Aquella entidad que más “talentos”, ideas de más gente, mayor presencia, etc., incorpore, más potente será en la Red.

TODO TIENDE A LO SOCIAL

“Estamos viviendo cambios que sitúan a las personas en el centro de todas las operaciones y relaciones. La sociedad reclama atención y protagonismo”

Hay dos cosas que mueven a la gente en la Red:

- Pertenecer a algo, desde el club de seguidores de alguien hasta los que se reúnen para conseguir dinero para algo
- Ser significativamente “importantes”, porque quieren contar lo que saben hacer al resto. Es importante para la policía localizarlas y que quieran desarrollar esa experiencia, porque son fundamentales para poder luchar contra el crimen

20 Hay varios ejemplos de personas que tienen capacidad, que quiere ser alguien y que lo que hacen lo realizan muy bien. Se pueden encontrar en distintas redes sociales, por ejemplo las dedicadas a la policía. Son internautas especialistas en algo que quieren colaborar y ponen su conocimiento a disposición de otro, en este caso para resolver el problema de los ciudadanos. También las corporaciones y las organizaciones tienen que descubrir a esos talentos. Ésta es otra de las claves para interpretar las redes sociales: el impacto que tienen es que impactan en las personas.

CAMBIO

Caminamos hacia un tipo de sociedad en la que el ciudadano se va a integrar en las redes sociales para producir otra forma de trabajar, que es entrelazándose con la sociedad y no entrando a descubrir lo que puede pasar, que es lo que ahora mismo están haciendo. Un ejemplo es una iniciativa de colaboración ciudadana en Estados Unidos en las que los electores pueden formular al Presidente del Gobierno y al Senado propuestas.

Lo importante es establecer un nuevo formato de colaboración que nos permitan adaptarnos a este nuevo mundo. Ya hay algunas iniciativas que nos acercan un poco hacia esta evolución, por ejemplo las gafas de Google, Google Glass Explorer Edition, que integran una cámara que graba y te conecta con tus redes. Son solo un ejemplo, porque en los próximos cinco años va a haber una gran cantidad de innovaciones tecnológicas que cambiarán nuestro día a día totalmente, aunque no para todo el mundo de la misma

forma. Saber integrarse tecnológicamente es relativamente fácil, pero saber relacionarse en un entorno tan digital no es tan fácil.

Telefónica estima que dentro de unos años habrá 50.000 millones de móviles de Interface conectados, ahora hay unos 6.000 millones. Esto quiere decir que nos conectaremos con cualquier electrodoméstico de la casa, con el coche... Serán millones de datos ¿Estamos preparados?

Los *big data* (centros de datos que circulan por la Red) son el negocio para los próximos años. Con ellos, la información debe estar y va a estar disponible en todo el universo. Lo ideal es que los *big data* eliminen un gran número de delitos físicos. Es importante que todo lo que sea lanzar la información hacia fuera va a ser positivo.

Hoy día están trabajando para introducir o extraer información del cerebro a través de un chip. El objetivo final es que cuando alguien tiene un problema, un trauma, poder extirpárselo y curarle. La sociedad va a cambiar éticamente, porque un país desarrollado y con acceso a esa tecnología, que permite transformar el cuerpo y desarrollar ciertas acciones, podría utilizarla frente a otros países que no pueden llevarla a cabo. La capacidad de transmitir información con la mente nos va a hacer replantear cómo esto afecta la seguridad, incluso cómo se genera el conocimiento a través de las redes.

21

Siguiendo con los ejemplos, otro lo proporciona Trevor Blackwell, creador de los Anybots, que son androides de los que ha vendido miles de unidades y que sustituyen al hombre en tareas rutinarias, por ejemplo, atender al teléfono, abrir puertas, ir a reuniones... Los seres humanos tienden a generar valor para las organizaciones en las que están, para la sociedad, pero la Red les obliga a intentar ser más válidas para lo que hacen. Pasan de ser recursos que trabajaban a personas que aportan ideas en esa organización, lo cual es una ventaja. Esto obliga a trabajar un poco más, pero no está mal tampoco. Trevor Blackwell sólo se ha adelantado un poco a este concepto.

En otra parte del mundo, en París, una compañía se dedica a crear réplicas digitales exactas de individuos, y nos es posible distinguir en una imagen hablando y en movimiento quién es la persona real y quién no. Lo hacen para desarrollar actores, dobles en las películas. Hay empresas que pueden hacer un buen uso de la tecnología y otras no.

Para finalizar, otro ejemplo de una firma que, también en la capital gala, trabaja en un sistema que se llama "la segunda piel". Es un chip que se coloca en la piel, no se ve prácticamente, y lo que hace es que interactúa con quien quieras. La corporación lo comercializa bajo este mensaje: si te vas

de viaje puedes grabar previamente un abrazo tipo con tu mujer y, si ella te echa de menos, puedes enviarle un abrazo a distancia con sólo apretar un botón, estés donde estés. Este tipo de desarrollos nos pueden llevar al final a sustituir a las personas, casi los sentimientos, y el problema será enorme. Las redes serán un juego de niños comparado con esto.

Y también está el mundo virtual: Google ha lanzado Indoor Maps, una aplicación de mapas que permite ver el interior de los espacios allá por donde vas caminando, y otros están trabajando en un método que graba absolutamente todo lo que haces (aquí ya entramos en derechos de imagen) ¡Esto es imparable!

La parte buena es que se puede compartir información entre cientos, miles de ciudadanos, y trabajar conjuntamente. Repetimos, la gente quiere ser algo y pertenecer a algo. ¿Es bueno o es malo? Si la policía es reactiva los datos irán hacia ella, podrá analizar, trabajar con ese equipo y tomar decisiones. Es clave la capacidad policial para generar confianza. Ese es el gran desafío. No es tanto un reto tecnológico como un objetivo de personas que, con alta capacidad, interconectan. No hay que esperar a que la tecnología siga aumentando, sino introducirse en ese nuevo mundo.

22

DE LA INTEGRACIÓN A LA RELACIÓN TECNOLÓGICA

La tecnología no es buena ni es mala. La tecnología es agnóstica. Del uso que nosotros hacemos de eso y de la capacidad no de guardarla y limitarla, sino abrirla, va a depender el éxito en el futuro.

La gente se empeña en guardar el conocimiento. El conocimiento hay que liberarlo. Cuanto más libre sea el conocimiento estará más accesible a más personas y podremos tomar decisiones más rápido.

DE UNA RED DE PERSONAS A PERSONAS EN RED

Vamos a una sociedad abierta formada por seres en red, donde la gente quiere colaborar y quiere ser protagonista. En la sociedad actual solo hay una solución para la crisis: poner el talento a funcionar. Algunos de vosotros lleváis en el Cuerpo 20 ó 30 años, habéis vivido cosas que otros compañeros no han podido vivir. La única forma de entender lo que está ocurriendo con el conocimiento y la experiencia de otros es que todo ello se pueda poner en común. Esta es la clave y es lo más complejo de organizar: una sociedad conectada. Pero no solo conectada conmigo usuario, sino con mi red.

Yo soy un nodo dentro de la Innovación porque tengo toda la información de ese tema que me interesa a golpe de clic y la puedo compartir en un segundo, no porque lo sepa, sino porque sé dónde está. No me interesa sólo un equipo en red sino un equipo actualizado en lo último en aquello que es competencia suya. Es un equipo de personas hiperconectadas con otros nodos del mundo que está preparado para trabajar frente a lo que va a venir.

En estos momentos vivimos el principio de la eclosión de la sociedad del talento (talent network).

LA GESTIÓN DEL CONOCIMIENTO: DESDE LA ECONOMÍA DEL CONOCIMIENTO A LA ECONOMÍA DEL TALENTO CONECTADO

“El talento conectado establece una nueva dimensión del talento que, de una forma colaborativa y diversa, se organiza activamente para resolver los retos de una sociedad cada vez más compleja y dinámica”.

Toda policía de Toronto tiene identificaciones personales en aquello en lo que son competencia y se relacionan con la ciudadanía. Lo que me interesaría también es saber si el funcionario que aquí presento está conectado con todo lo que ocurre en gestión de recursos humanos con otros sistemas de policía en el mundo. Si es así, es una persona clave, un talento, porque conoce todo lo que puede suceder, está vinculado con toda la ciudadanía, enlazado internamente dentro del ámbito de la policía y puede ejecutar todo aquello que quiera.

23

Por tanto, no es tan importante en esta sociedad tener el conocimiento, el talento, sino tener acceso al mismo. Para mí lo importante no es conocer lo que ocurre hoy, el desafío es cómo conectar nuestra experiencia de hoy con la de alguien que lleva 40 años.

IN-PRENDIMIENTO. EL NUEVO ENTORNO: EMPRENDIMIENTO EN LAS ORGANIZACIONES

Para aquéllos con responsabilidades, con equipos a su cargo o que quieren poner en marcha una nueva empresa, tenéis que uniros con productores de nuevas ideas, iniciadores de actividades que antes no se han llevado a cabo, individuos que quieran transformar vuestro Cuerpo policial, personas que estén muy bien conectadas. Todos estos perfiles son los que hacen que una organización esté preparada para encontrarse con todo lo que viene.

HACIA NUEVAS COMPETENCIAS: LA PERSONA SOCIO DIGITAL CONECTADA

Entre las habilidades (*skills*) que se exigirán a los hombres en los próximos años hay algunas muy importantes, como son la alfabetización y el funcionamiento cognitivo, es decir, cómo funciona el cerebro en red. Yo me imagino el futuro muy conectado, donde yo pueda en un momento determinado vincularme con quién tiene cargo en mi área de seguridad, que es la Policía, con el cual puedo enviar información de una forma rápida, instantánea y que sea capaz de procesarla y de actuar. El grupo tiene que tener capital social (*social capital*), que es la capacidad que tiene un conjunto de semejantes de trabajar conectados al mundo. Y es tan importante la persona que está de administrador como las que están fuera o en los mandos superiores.

24

Esto es la alineación hacia el futuro. Para entender todas las relaciones externas que una compañía tiene, ésta tiene que cambiar la totalidad de su entorno. Aquellas empresas, organizaciones, organismos públicos que están focalizando su atención en los sistemas pero no están desarrollando el cambio cultural estratégico de las personas, probablemente cometan un error, es decir, la tecnología siempre les va a superar. Hay que ir poco a poco capacitando, explicando y entendiendo para integrar a los equipos, sobre todo culturalmente, en una nueva forma de vivir la Red.

ESTAR VS SER DIGITAL. EL CAMINO HACIA LA ENTIDAD DIGITAL

Hay valores que aceleran la presencia en la Red. Un organismo que además de tener una presencia en la Red es horizontal, es decir, hace que su organización sea plana y, por tanto, la información fluye, dentro de unos límites, entre todos los miembros, es una entidad que está acelerando para llegar a un mundo cada vez más en Red. Cualquier persona que esté trabajando en un universo conectado debe ser un nodo más de información, que fluya la información hacia el resto. Esto no tiene que ver tanto con la tecnología sino con el cambio de cultura.

En el siglo XIX decía Andrew Carnegie que el único capital irremplazable que una compañía poseía era el conocimiento y la habilidad de su gente. Rodeaos siempre de quiénes tienen toda la capacidad del mundo y que quieran y puedan compartirla con vosotros. Si empezáis a partir de mañana a desarrollar una nueva estructura, cambiáis vuestros organismos para que sean cada vez más horizontales y permitan que todo el mundo pueda interactuar, estaréis preparados para interactuar mucho mejor con las redes sociales, que van a cambiar a una velocidad enorme. Ya lo explicaba

Charles Darwin: “el que sobrevive no es el más inteligente sino el que mejor se adapta al medio”.

REDES. EL PODER DE LA COMUNICACIÓN EN RED

Las redes son un mundo fantástico, es una alegría que nos hayan llegado para poder desarrollarnos personalmente, ponernos en contacto con otros, trabajar y colaborar con los ciudadanos o con otras entidades, con otros compañeros, etc. Cuánto más integrados estéis más fácil será el futuro, porque lo que viene va a ser muy complicado.

Vosotros sois los que vais a crear la policía del mañana, y va a salir de vosotros, de vuestra inteligencia y capacidad de crear nuevas iniciativas, la nueva Red. Tenéis que luchar para que el futuro en esta red sea vuestro.

*“Lo relevante no es conocer las herramientas y la tecnología,
sino todo aquello que el talento individual y el conocimiento colectivo
puede hacer con ellas para crear bienestar, modificar y mejorar las condiciones
personales, sociales y globales de lo que nos rodea”.*



POWERPOINT

DIONISIO FERNÁNDEZ NESPRAL
Gerente de Innovación de Everis



27



El impacto de LAS REDES

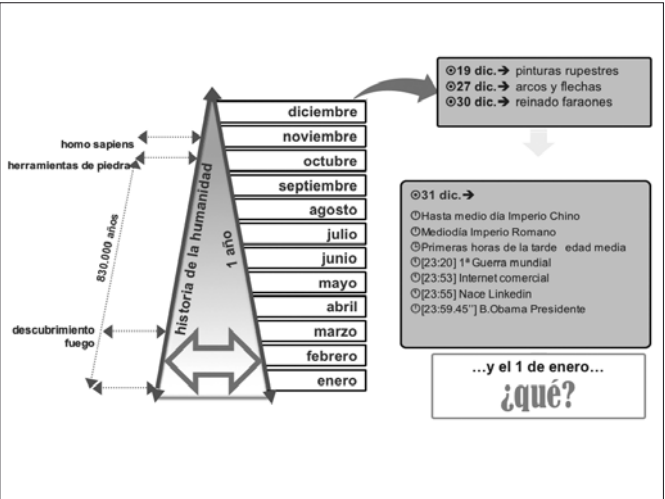


San Lorenzo de El Escorial, julio de 2012



Vivimos **tiempos exponenciales**

Y el tiempo es el mayor activo en nuestras manos



Vivimos **hiperconectados**

Hoy día quien no tiene un hipervínculo, no es nadie

situación

el potencial de la Red y las redes sociales





#social



#digital



#world



#people

#instantánea

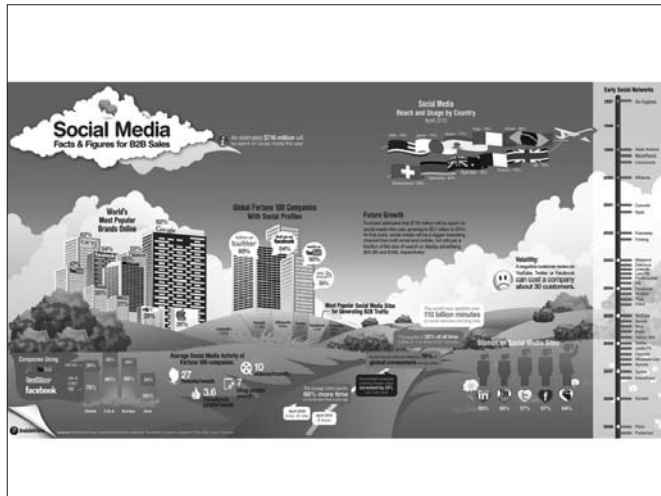
La nueva sociedad digital

Vivimos tiempos exponenciales donde los cambios son constantes y las acciones instantáneas.

En un entorno hiper-conectado, los formatos se vuelven digitales, y los modelos se transforman, convirtiendo a la persona en el centro estratégico de una sociedad que cada vez es más social, conectada y abierta.

Las organizaciones buscan adaptarse y gestionar los nuevos tiempos hacia una organización del siglo XXI.

7



Información » Vida y Estilo » Tecnología

España, líder de la UE en uso de redes sociales

Es también el país de la Unión Europea que utiliza en mayor proporción Internet para las descargas


EP / MADRID España se posiciona como el país de la Unión Europea que más utiliza Internet para visitar redes sociales y, además, permanece a la cabeza en el ranking de uso de la red para descargas audiovisuales, según una encuesta realizada por Ipsos a ciudadanos de 24 países en todo el mundo.

En concreto, el uso más común de Internet en España se destina a enviar y recibir correos electrónicos (89%), seguido de las visitas a redes sociales o blogs, con un 70%, frente al 65% de los británicos, el 61% de los italianos, el 55% de los alemanes o el 50% de los franceses.

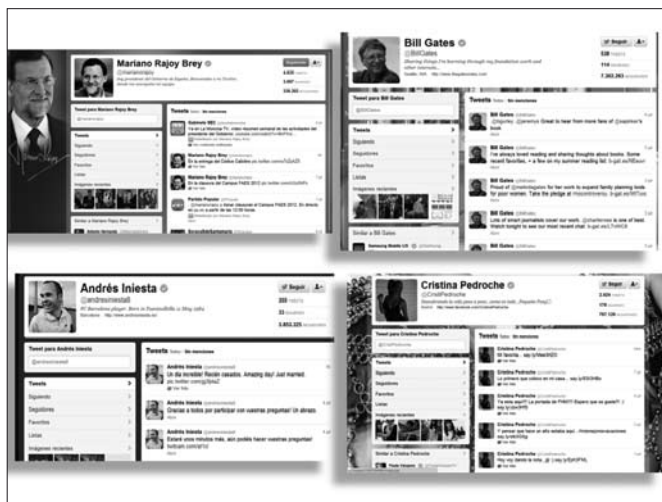
En cuanto a las descargas audiovisuales, España permanece a la cabeza de los países de la Unión Europea, con un 49%, y, le superan a nivel global, China (72%), Turquía (62%), Argentina (60%), Indonesia (60%), Rusia (60%) y México (56%).

Asimismo, la encuesta revela que los españoles se encuentran a la cola en lo que a búsqueda de información sobre actividades lúdicas, hobbies o temas de interés personal se refiere. En este sentido, los españoles, con un 45%, se encuentran por detrás de Gran Bretaña, con un 61%, de Alemania, con un 60%, o de Francia, con un 54%.

En cuanto a la búsqueda de trabajo, los españoles, con un 48%, se encuentran por encima de la media de los 24 países recogidos en la encuesta, aunque por detrás



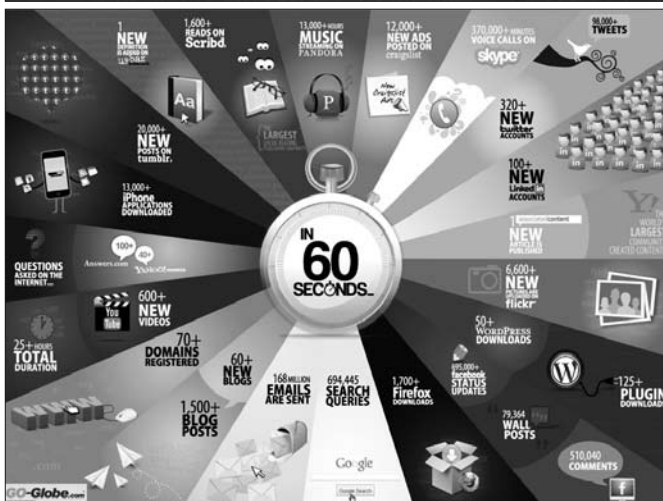
9



1/9/90

Vivimos en formato digital

Hoy día lo que no se digitaliza, no ha ocurrido



Vivimos en transformación
La gran oportunidad en tiempos de crisis



@dtapscott
Don Tapscott

RT @DanielLegere: Don Tapscott "The industrial economy has finally run out of gas...This is now a pervasive communications revolution"

hace 7 horas vía TweetDeck ☆ Eliminar de favoritos ↻ Retwittear ↩ Responder

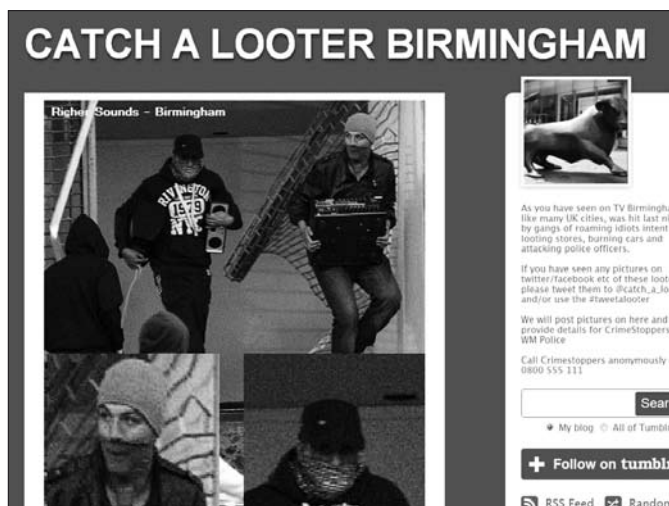
Todo tiende a lo social



#londonriots



#riotcleanup



“Estamos viviendo cambios que sitúan a las **personas en el centro** de todas las operaciones y relaciones. La sociedad reclama atención y **protagonismo**”

Es la hora **del crowd**
Conociendo de la multitud



INNOCENTIVE
Where the world innovates

Welcome to Innocentive
Tell me more »

Open Challenges: **Featured Challenge** There are 42 open challenges

Challenge	Prize
Extraordinary & Unorthodox Philanthropy Deadline: 11/16/2010 10 active solvers	\$10,000 USD
Estimation of Motor Vehicle Diagnostics Deadline: 11/16/2010 100 active solvers	\$5,000 USD
Room Temperature Oxidation Catalyst Deadline: 11/16/2011 100 active solvers	\$50,000 USD
Better Cat Litter, Please! Deadline: 11/16/2011 100 active solvers	\$7,000 USD

Winning Solvers

Solver	Challenge
Scott Fisher	Extraordinary & Unorthodox Philanthropy
George Spergel	Room Temperature Oxidation Catalyst

Solvers Wanted
We have thousands of Challenges that need your brainpower and companies that are willing to pay you to think. Get in on the action.
Learn more » Register now »

Refer a Friend. Earn a Bonus.
Do you know someone who would make a great Solver? Refer them and earn up to \$1,000 the first time they solve an Innocentive Challenge!

Start Referring Now!

Start Referring Now!

More Information

Follow us on Twitter »
Visit our Facebook page »
Check out our blog »

Vtrulia crime maps beta

MAP OPTIONS
Heatmap, Colors

Heatmap
0.0 50 100 150 200 250+
Incidents per block per year

Individual Crimes
From 5/1 to 6/15

- ☒ All types
- ☒ Shooting
- ☒ Robbery
- ☒ Assault
- ☒ Arson
- ☒ Burglary
- ☒ Theft
- ☒ Vandalism
- ☒ Arrest
- ☒ Other

MOST CRIMES
See dangerous intersections

CROSS STREETS	# OF CRIMES
1 East Washington Street	7
2 E 83rd St and S Coles	6
3 E 71st St and S Coles	5
4 E 73rd St and S Coles	4
5 Lafayette Ave and W	4

663 crimes in this area add a comment »

Crime Trends in Chicago
My Heatmap by Day

the WHITE HOUSE PRESIDENT BARACK OBAMA

BLOG PHOTOS & VIDEO BRIEFING ROOM ISSUES ADMIN

WE the PEOPLE
YOUR VOICE IN OUR GOVERNMENT

How We the People works in 3 easy steps

STEP #1
Create or Sign a Petition
Anyone 13 or older can create or sign a petition on WhiteHouse.gov asking the Obama Administration to take action on a range of important issues facing our country. To get started you'll need to create an account and enter your email address. Start thinking about the issues that matter to you, what you would like the Obama Administration to do to address the important challenges facing our country, and who you'd ask to join you.

STEP #2
Build Support and Gather Signatures
Creating or signing a petition is just the first step. It's up to you to build support for a petition and gather even more signatures. Use email, Facebook, Twitter and word of mouth to tell your friends, family and coworkers about the petitions you care about.

STEP #3
The White House Reviews and Responds
If a petition meets the signature threshold, it will be reviewed by the Administration and an official response will be issued. And we'll make sure that the petition is sent to the appropriate policy makers in the Administration.
The initial threshold to get a response from the Administration is 5,000 signatures.



too bright. Well, we have an awful lot of products, some of which people don't seem

“En los próximos 5 años, van a haber una gran cantidad de innovaciones que nos afectarán en el día a día y cambiarán nuestras vidas... (totalmente)”.

Larry Page, CEO Google



Llegan los sensores cerebrales

25/07/2010 Editorial RWMS [Comentarios](#)



¿Llamar por teléfono a una persona simplemente pensando en ella? Será posible. Las **Interfaces Informáticas cerebrales**, una tecnología que crea una conexión directa de nuestros **cerebros** a los **ordenadores**, está comenzando a llegar al mercado mediante juguetes y controladores para juegos, aunque tendrán otras muchas aplicaciones en poco tiempo.

Internet a la velocidad del pensamiento

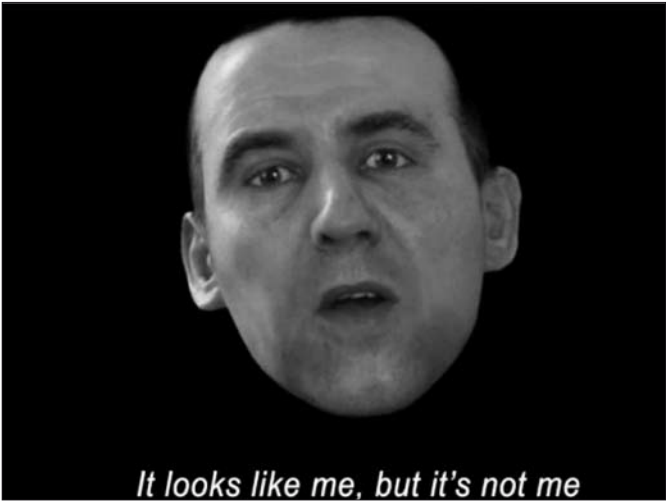
Desde el primer tweet generado mediante el pensamiento hasta la financiación por parte del ejército estadounidense del desarrollo de miembros artificiales avanzados o los sensores cerebrales implantables. Los avances en este tipo de interfaces no sólo están transformando las vidas de quienes se encuentran aquejados de parálisis total, sino que también están abriendo una era en la que podremos crear **Internet** tan rápido como podamos pensar.

El primer tweet "pensado"

El 1 de abril de 2009, el estudiante de doctorado de la Universidad de Wisconsin Adam Wilson fue la primera persona en pensar un tweet: "USING EEG TO SEND TWEET" "Usando EEG para enviar un tweet". Wilson llevaba un gorro conectado a un electroencefalógrafo estándar mientras observaba una pantalla de letras parpadeantes. Sólo tardó unos días en escribir el software que conectaba su cerebro con Twitter. Según la nota de prensa, "Wilson forma parte de un grupo cada vez mayor de investigadores en todo el mundo que pretenden perfeccionar un sistema de comunicación para usuarios cuyos cuerpos no funcionan, pero cuyos cerebros funcionan con normalidad". La revista



38



De la integración a la relación tecnológica

Las redes sociales no crean los actos, acentúan una realidad y permiten una transmisión instantánea de los hechos o actos.

La tecnología es agnóstica, ni buena ni mala. Fomenta y activa nuestras condiciones psicológicas, sean estas destructivas, o creativas.

Limitar por tanto, las tecnologías, limitará nuestra capacidad para mostrar y probar nuestras condiciones positivas. Los problemas residen en las personas, no en las herramientas.

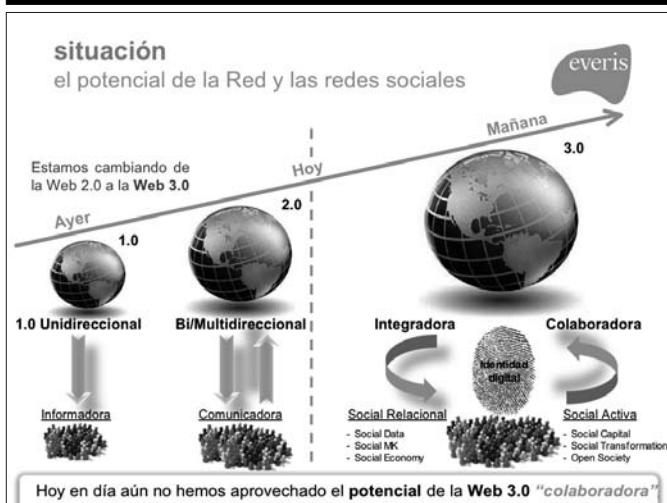
Graham Brown. Co-founder Ofmobile Youth

37

“ De una Red de Personas a **Personas en Red** ”

Del contacto a la conexión.

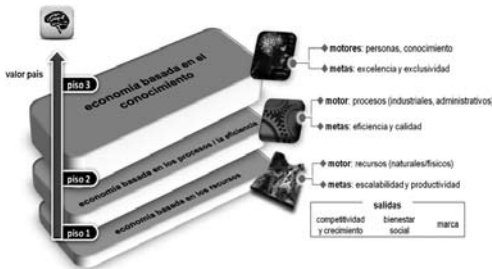
39



En estos momentos vivimos
el principio de la
eclosión de la sociedad del
talento

la gestión del conocimiento

Desde la economía del conocimiento ...



41

la gestión del conocimiento

la economía del talento conectado.



[talento Network]

42

la gestión del conocimiento
la economía del talento conectado ...

everis

«El talento conectado establece una nueva dimensión del talento que, de una forma colaborativa y diversa, se organiza activamente para resolver los retos de una sociedad cada vez más compleja y dinámica»

43

everis

www.torontopolice.ca

Chris Boddy
@TPSChrisBoddy
Staff Sgt, Human Resources Management, Toronto Police Service.
(This account is not monitored 24/7. To report a crime call 911 or in
emergencies, or 416-922-2222)
Toronto, Canada · <http://www.torontopolice.ca/cr>

9,829 TWEETS
2,895 FOLLOWERS
2,653 FOLLOWINGS

Connect with us
torontopolice
TorontoPolice

Tweet para Chris Boddy
@TPSChrisBoddy

Tweets

Gigando
Seguidores
Favoritos
Listas
Imágenes recientes

Similar a Chris Boddy
Derechos reservados

Tweets

Chris Boddy @TPSChrisBoddy
@LambMyLunchie I will put some in my carry on.
#Ver conversable

Chris Boddy @TPSChrisBoddy
The 1st team is through to the semi-finals at the #Hockeyrookie
pic.twitter.com/0u0d50CH
#Ver foto · #Reportar · #Retweetar · #Favorito

Chris Boddy @TPSChrisBoddy
@Karyncimena Thanks for that!
#Ver conversable

Chris Boddy @TPSChrisBoddy
Playoff round begins at the #Hockeyrookie pic.twitter.com/Hu0u0d50
#Ver foto

Kevin Prekiet (@kprekiet)
The riot by the Lake Shore today with the #Hondaindy in #Toronto
#Hondaindy pic.twitter.com/0u0d50CH
#Ver foto

44

**«Lo importante no es ya
retener el talento, sino tener
ACCESO al talento»**

@CKPrahald 2008

In-prendimiento

el nuevo entorno: emprendimiento en las organizaciones.





Talento Conectado

- La persona como centro
- Personas en Red
- Inno-emprendiendo

 productores

 iniciadores

 transformadores

 conectores



46

Hacia nuevas competencias

la persona sociodigital conectada



Future Work Skills 2020



Inteligencia social

Pensamiento adaptativo

Competencia intercultural

Nueva alfabetización

Transmultidisciplinar

Nuevo funcionamiento cognitivo

Colaboración virtual

Orientado al Diseño

47

dirección y habilidades digitales

knowledge mobile: conocimiento instantáneo y móvil



ADOPTION RATE OVER TIME

75% of all workers will have some level of mobility associated with their jobs

Tablets Expected to Ship

Year	Tablets Expected to Ship
Q1 2011	16.1 MILLION
Q1 2012	147.2 MILLION

Shares bought by business websites

According to Forrester, by 2015, 1 in 3 US online consumers will be using a tablet.

SMALL & LARGE BUSINESS ADOPTION

Enterprise Adoption of Tablets

Category	Adoption Rate
Tablets being personally purchased	41%
Small teams are piloting tablet use	16%
Who have purchased tablets for specific	28%
Who do not have tablets in place	1%

AA The University of Southern Mississippi

Plans to roll out 8,000 tablets as flight entertainment devices for first and business-class passengers.

Plans to roll out 1,000 tablets to students and professors.

48

everis



#social capital?

How do you rank in social capital?

49

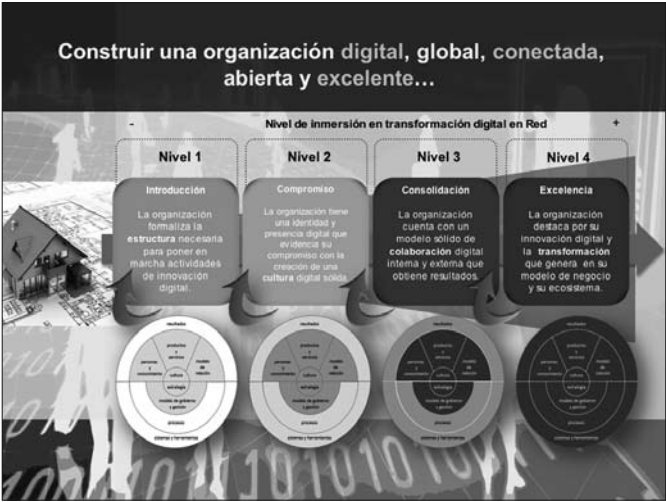


Organización SocioConectada

Vamos hacia una organización **sociodigital**, abierta, colaborativa, innovadora, conectada y en red.

43







Redes

El poder de la comunicación en Red.



Las redes (sociales, de talento, profesionales...) son un medio, no un fin. Son **canales de relación**, que permiten **potenciar la comunicación** y transformar usos, valores y formatos. Por ello, **potencian a los individuos, al talento, a la opinión y a la participación**. Y son uno de los elementos claves para adaptarnos al entorno y los tiempos tan dinámicos.

@persona

“We are better than me”

“The only irreplaceable capital an organization possesses is the knowledge and ability of its people. The productivity of that capital depends on how effectively people share their competence with those who can use it.” Andrew Carnegie. (19th century)



59





**“It is not the strongest of
the species that survive,
nor the most intelligent,
but the one most
responsive to change.”**

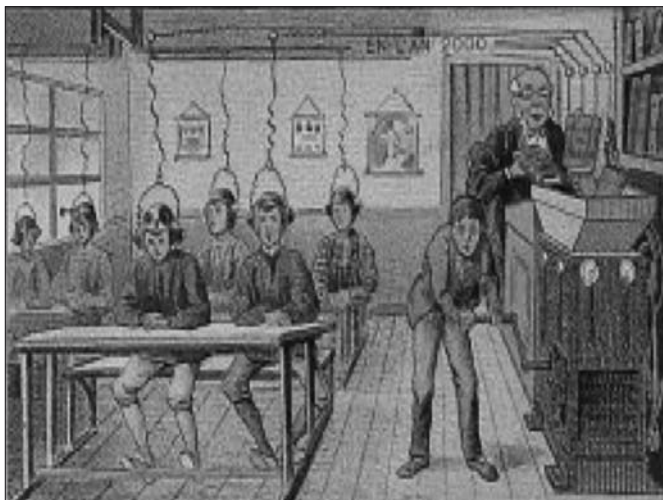
Charles Darwin, 1809-1882

61

**“El que inventó la rueda era un idiota....el
que realmente era un
genio es el que inventó
las otras tres”**

Sid Caesar

47





Lo relevante **no es conocer las herramientas y la tecnología**, sino todo aquello que el talento individual y el conocimiento colectivo puede hacer con ellas **para crear bienestar, modificar y mejorar las condiciones personales, sociales y globales de lo que nos rodea.**

64

MESA REDONDA:

CRIMEN ORGANIZADO Y NUEVAS TECNOLOGÍAS

FRANCISCO JAVIER RODRÍGUEZ RODRÍGUEZ
Inspector del Cuerpo Nacional de Policía.
Miembro del Grupo II, de la Brigada de Investigación
Tecnológica, de Fraudes en Internet.

49

En el entorno en el que nos movemos hoy en día, hablamos de la sociedad de Internet, y escuchamos continuamente ideas y planteamientos sobre la importancia de las nuevas tecnologías, la transcendencia de la Red. Entendemos que es una herramienta fundamental para el desarrollo económico y social, y eso vincula a cualquier sociedad moderna que se precie.

En el escenario en el que nos encontramos las tecnologías de la información y de la comunicación están en desarrollo continuo, lo que propicia un cambio social, un importante desarrollo del comercio y la banca on-line, nuevas formas de relaciones humanas, el fenómeno de la globalización, etc. Todo ello va a materializar nuevas oportunidades y, por supuesto, novedosas amenazas.

En ese marco de desconocidas amenazas encontramos lo que sería el área del delito en Internet, con un aumento en su complejidad vinculado a las nuevas tecnologías, con un desarrollo cada vez más rápido de esas nuevas formas delictivas, en constante evolución, y con una rápida difusión de los datos a través de la Red, que propicia que las organizaciones criminales vean en las nuevas tecnologías un nuevo caldo de cultivo bastante más rentable.

EL DELITO Y LAS NUEVAS TECNOLOGÍAS EN EL FUTURO

Ante las amenazas que acabamos de mencionar nos preguntamos: ¿qué es lo que queda por ver?, ¿qué nos deparará el futuro en relación al delito y a las nuevas tecnologías?

En este caso nos referimos a la *ciberdelincuencia* vinculada, sobre todo, al crimen organizado, a la acción de los piratas informáticos (*hacker*) en el ámbito político, industrial, etc., al *ciberterrorismo*. Son actividades que no conocen fronteras y que, en muchas ocasiones, están interrelacionadas entre sí. Es imposible poner puertas al mundo, nos comunicamos y nos responden desde cualquier parte del mundo y eso va a propiciar que la criminalidad organizada se desarrolle exponencialmente en un nuevo campo, en una nueva área de trabajo como es la Red.

50

La acción punible en Internet podemos encontrarla en todos los campos que conocemos de desarrollo de la propia Red, de progreso de las nuevas formas de comunicación, de avance de las nuevas tecnologías: en páginas web, a través del correo electrónico, del comercio electrónico, la banca on-line, los servicios de mensajería instantánea, las redes sociales, los canales para conversaciones *Internet Relay Chat* (IRC), las líneas de interrupción *Interrupt ReQuest* (IRQ), los foros públicos y privados y, en definitiva, todo aquello que pueda abarcar la imaginación o el ingenio del delincuente. Hasta ahí llegará el campo del delito dentro del marco de las nuevas tecnologías.

Cualquier infracción puede cometerse por o con la presencia de la Red. Las nuevas tecnologías de la sociedad de la información hacen las veces de instrumentos del delito en cualquier modalidad criminal. Por ello, en la investigación policial es necesaria, o ve necesaria, la recogida de vestigios que aportan pruebas y que, en muchas ocasiones, van a estar en el ámbito de las nuevas tecnologías o en la prueba electrónica o digital.

TRATAMIENTO JURÍDICO

El tratamiento jurídico actual después de la última reforma del Código Penal diferencia entre:

- Organización criminal: es la agrupación formada por más de dos personas, con carácter estable, por tiempo indefinido, que de manera concertada o coordinada confluyen al objeto de cometer delitos o de manera continua faltas

- Grupo criminal: es la unión de más de dos personas que, sin llegar a ser considerado como organización criminal, tengan prácticamente las mismas finalidades, es decir, concertada para la comisión de delitos o reiterada de faltas

Prácticamente, en el 90 por ciento de los casos, la actividad delictiva nunca es cometida única y exclusivamente por un solo sujeto. Por lo tanto, sea de manera concreta según el tipo penal, según la jurisprudencia, según las instrucciones, circulares sobre delincuencia organizada, los convenios internacionales y demás, o sea, desde un punto de vista más global, siempre hay que mirar hacia la delincuencia organizada en muchos casos por la necesidad de confluir varias personas. Unos sin otros no podrían ejecutar esas infracciones a través de la Red.

VISIÓN GLOBAL

Partir de una visión global del fenómeno, es decir, de una sinergia continua entre la idea del crimen organizado e Internet, se puede plantear desde dos puntos de vista:

- La actividad tradicional de crimen organizado. Léase, por poner un ejemplo, el tráfico de drogas, de armas, de personas, etc., que obtiene en Internet un medio, un instrumento, un soporte más en su ejecución para llevar a cabo su actividad organizada
- Y, el siguiente punto de vista, que quizás sea en donde más se produce esa evolución continua de la criminalidad organizada. Es decir, conceputar a la red Internet, a las nuevas tecnologías, como un nuevo marco para la actuación de la criminalidad organizada: Internet es el medio a través del cual se comete el delito. Cuando hablamos en este sentido de criminalidad organizada, siempre, a excepción de algunos casos, nos vamos a centrar en actividades, principalmente, de delincuencia económica

51

TIPOLOGÍA DE DELITOS

La tipología delictiva que se puede encontrar en la ejecución de delitos a través de la Red es inmensa: libertad e indemnidad sexual, amenazas, delitos contra el honor, calumnias e injurias, estafas, blanqueo de capitales, usurpación de estado civil, falsedad documental, descubrimiento y revelación de secretos, propiedad intelectual, etc. Pero, dentro de esa visión de la Red como un nuevo campo de actuación de la criminalidad organizada, nos podemos centrar en

un campo de actuación más concreto, máxime, el de las estafas, con el fenómeno del *carding* (uso ilegítimo de tarjetas de crédito o de sus números), el del *phishing* (suplantar a identidad), programas maliciosos, etc.

En este caso son grupos que, encargándose de diferentes actividades que conforman el delito, no actúan de manera directa conociéndose, pero sí de manera coordinada. Se trata de la unión de dos o más personas que no se puede identificar en el marco de la criminalidad organizada tradicional, pero sí es una coalición necesaria desde un punto de vista logístico para que la actividad del crimen organizado a través de la Red pueda llevarse a cabo.

Otro campo de acción orientado al beneficio económico son las denominadas “cartas nigerianas” (estafas a través de e-mail), todos los tipos de spam existentes, las pirámides financieras, los juegos y casinos virtuales, chantajes y extorsiones a través de la Red, etc.

¿Qué está propiciando que la criminalidad organizada tradicional, que a lo mejor hasta hace unos años se dedicaba al tráfico de drogas o de armas, ahora encuentre en Internet una actividad bastante más rentable desde el punto de vista económico y, sobre todo, desde un punto de vista punitivo? A continuación se detallan las razones.

52

ANONIMATO, Y MUCHO MÁS...

El anonimato: la actividad delictiva cometida a través de la Red normalmente genera una sensación de anonimato, tanto para el delincuente, como, en muchos casos, para la concepción que tiene el propio usuario del delito cometido a través de la Red. No sabemos quién hay al otro lado de la línea.

La globalización: a través de ese concepto se tiene acceso a un mercado mundial y, por lo tanto, las posibilidades de éxito y que la actividad delictiva llegue a buen puerto se multiplican de forma exponencial.

El desarrollo de las tecnologías: éstas constituyen un recurso al servicio de la sociedad y del delincuente. Es decir, para la actividad delictiva de los grupos organizados puede llegar a ser la propia arma para la ejecución de esa ocupación.

La legislación: al tratarse de una actividad supranacional, ¿quién le pone límites, puertas al mundo? Es el conflicto de carácter jurídico-legislativo, problemas de territorialidad, problemas jurisdiccionales, problemas legislativos en cuanto a la concepción de cada delito en cada uno de los países en donde se actúa.

La globalización de la Red permite la posibilidad de conectarnos desde cualquier parte del mundo. Y en función de esa actividad tenemos problemas para saber qué jurisdicción, qué legislación poder aplicarle, a quién podemos acudir para obtener los datos técnicos de información de cara a la investigación necesarios, en definitiva, una serie de dificultades que tenemos que ir salvando.

La criminalidad organizada a través de la Red conlleva la necesidad de actuar de forma global, no solo desde nuestro país sino desde todos aquéllos implicados en un caso concreto. Eso entraña una investigación integral, desde un punto de vista policial o desde un punto de vista judicial, para que cada uno de los Estados implicados responda de forma unísona.

En este tipo de amenazas, la rapidez en la actuación y la colaboración nacional y supranacional son fundamentales ya que el tiempo que pasa, evidentemente, es un beneficio total y absoluto para las redes delincuenciales, sobre todo porque se produce una pérdida de información que es, en muchas ocasiones, la base para seguir la línea de investigación hasta llegar a la cabeza de la organización.

COOPERACIÓN INTERNACIONAL

53

Si antes hablábamos del fenómeno local de Internet pues ahora, ante la evolución de las nuevas tecnologías, tenemos que hablar de una manifestación delictiva global. Internet no conoce fronteras ni límites y, por tanto, la actividad contra los grupos del crimen organizado tampoco debería conocerlas. Ese proceder contra el crimen organizado tiene que adaptarse a las nuevas circunstancias, a la nueva realidad.

La cooperación internacional se tiene que producir desde tres puntos de vista esenciales, más todos aquellos que creamos necesarios:

- Desde un punto de vista policial, mediante los mecanismos de colaboración policial internacional
- Desde un punto de vista judicial, con la intención de unificar las legislaciones. Ya existe, de alguna forma, esa inquietud en el propio Convenio sobre Ciberdelincuencia de Budapest, al objeto de que el ámbito de aplicación de la ley de estas tipologías de hechos delictivos que se cometan a través de la Red, sean, más o menos, uniformes en los países firmantes de ese convenio

- La implicación de agentes externos, tanto públicos como privados, del marco de las nuevas tecnologías. Es esencial y fundamental

Los esfuerzos tienen que ir en la línea de la información, el análisis, la investigación, una vez más la asociación internacional, los contactos continuos con los Proveedores de Servicios de Internet (ISP según sus siglas en ingles), la Oficina Europea de Policía (EUROPOL), la organización Internacional de Policía Criminal (INTERPOL), los centros de cooperación policial internacional, el agilizar los mecanismos hasta ahora existentes de las comisiones rogatorias, la necesidad en cuanto a esa relación entre entidades y usuarios afectados de implantar alertas de seguridad, comenzando sobre todo por la información y una formación dirigida a la prevención, una legislación homogénea, una coordinación informativa y operativa destinada a la ejecución de actividades que nos lleven a un resultado global sobre el propio fenómeno y, principalmente, unos planes de actuación de todos los países implicados concretos para cada uno de los fenómenos delictivos de la criminalidad organizada. No todo el crimen organizado tiene las mismas características y por lo tanto, las diferentes tipologías, incluso las propias del área de las nuevas tecnologías, exigen planes de actuación concretos internacionales.

CRIMEN ORGANIZADO Y NUEVAS TECNOLOGÍAS

LUÍS GARCÍA PASCUAL

**Inspector Jefe del Cuerpo Nacional de Policía.
Jefe del Grupo Operativo I, de la Brigada de Investigación
Tecnológica, de Protección al Menor**

55

La pornografía infantil ha sido considerada hasta ahora una actividad privada, que entraba dentro del ámbito de la persona, el ordenador y en su casa, por eso no se califica como crimen organizado. La llegada de Internet ha facilitado la creación de algo que no existía antes: la comunidad pedófila, que es un grupo de personas que se refuerza en su perversión sexual, y entre sí se facilitan enlaces y legislación sobre la utilización de Internet y las leyes nacionales, reforzando la actividad desviada del individuo.

Hemos pasado de un alguien retraído, que normalmente iba al parque, a la salida de los colegios, que buscaba siempre la soledad y que se venía abajo si le detenías, a una persona que está reforzada, que tiene un ambiente, un grupo que le fortalece, le asesora en su conducta desviada para conseguir niños, para burlar la acción de la justicia y, además, le hace tener la sensación de que la pedofilia va a ser una opción sexual en un futuro próximo, igual que lo ha sido la homosexualidad, que antes estaba prohibida y ahora se ve como natural.

Esto es lo que está produciendo esta comunidad que ha creado Internet. En ella existen foros donde se intercambian opiniones, se facilitan imágenes, salas virtuales donde se producen abusos, dando al individuo pedófilo la sensación de que nada inapropiado está teniendo lugar, es decir, que es una cosa normal y que lo hace todo el mundo.

Bajo mi punto de vista esto es una forma de organización de esa comunidad pedófila. Lógicamente, esto no tiene nada que ver con el crimen organizado como tal, es decir, el crimen organizado como asociación de delincuentes que se conciertan para cometer los delitos y, además, buscan una finalidad generalmente económica. En este caso, no, pero buscan una finalidad lucrativa de otro modo: la pornografía infantil, como todas las pornografías, se consume con la visión. Es decir, quien consume pornografía infantil necesita, constantemente, cada vez más, una vez que ha sido vista una foto necesita ver otra diferente, todo esto es el gran negocio de la pornografía.

Esas personas que adquieren pornografía necesitan renovarla asiduamente. Esto ha dado lugar a que haya un mercado, un negocio de la pornografía infantil, en el que ha entrado el crimen organizado.

En el año 2003, la Operación ORE, Landslide la llamaron también en otros países, determinó la compra de pornografía infantil en webs, solo en el Reino Unido, por parte de más de 7.000 personas, que fueron detenidas. En estas páginas de Internet la suscripción varía entre 80 y 100 euros mensuales, pero ha habido operaciones en las que un solo DVD de pornografía especialmente fuerte puede valer 500.000 euros.

56

¿Cuál es el grave problema que existe con el crimen organizado en relación con este tema? El conflicto es que tenemos una legislación nacional para un problema que es internacional, es decir, la globalización de Internet hace que una víctima pueda estar en Holanda, el agresor en Tailandia, el *hosting* en Estados Unidos y el registro en Panamá. Existe un amplio abanico de países implicados y hay que homogeneizar las leyes y dar una respuesta rápida en la colaboración, lo cual no siempre es posible debido a las soberanías y normativas nacionales.

Voy a presentar una investigación internacional, como no puede ser de otro modo en este tipo de cuestiones en las que el campo nacional no existe. En nuestra brigada, nuestros equipos están conectados con un determinado departamento internacional, unos con Lyon y otros con la Oficina Europea de Policía (EUROPOL), pero todo el mundo está interrelacionado porque necesitamos que la colaboración sea instantánea. Ésta era una operación de venta de pornografía infantil en la que había un grupo organizado que tenía una estructura en la que unos organizaban el dinero, otros abrían cuentas bancarias, otros localizaban la pornografía infantil, otros procedían a crear empresas falsas y otros creaban las páginas web donde se vendía la pornografía infantil, que también es importante para organizar todo esto.

La investigación se inició en Estados Unidos, pero rápidamente fue ramificada a todos los países porque los compradores estaban en todas partes. Una vez que pones en una página web anuncios de pornografía infantil es muy fácil lincarlos, prácticamente, desde cualquier sitio. En este momento la policía dispone del sistema CIRCAM de retirada de páginas web, en el que España está intentando apuntarse al carro de poder cerrar y/o limitar el acceso a pesar de que estén en países donde no tengan legislación sobre el tema o sean reacios a retirar las páginas. Por ejemplo, si ese site tiene el *hosting* en una isla perdida, y por sus leyes se podría tardar un año en “tumbar” esa página web, el CIRCAM, a través de la organización Internacional de Policía Criminal (INTERPOL), consigue que las personas no tengan acceso a esas páginas.

Antes eso no era posible, era muy fácil para cualquier persona acceder a una web de pornografía infantil. De hecho, TERRA, de Telefónica, tuvo alojadas miles de estos sitios, fundamentalmente eran anuncios, en sus servidores gratuitos. Como digo, con anterioridad era sencillo acceder a estos sitios, una persona tecleaba “sexo con jovencitas” o la palabra “pedo”, “lolita” o “kid” (niño) en cualquier buscador y accedía a una página de pornografía infantil.

“myillegalsite.net” parecía una web comercial, luego fue cambiando el nombre: “pedoland.com”, “kidporn.net”, etc., pero la estructura era similar: se ponían una serie de fotografías de pornografía de niños prepúberes, es decir, de cuatro o cinco años hasta 10 o 12 doce. El sitio mostraba nueve imágenes de niños y niñas realizando actos sexuales con adultos y ofrecía a la venta ese contenido. En sus anuncios lo ponía claramente, e incluso había eslóganes como: “Fastidia al FBI”, “Te facilitamos un sistema seguro”, “Las imágenes no son falsas”. Había miles de imágenes y cientos de vídeos almacenados en el sitio. Lincando en una página ibas a otra, y así sucesivamente, hasta llegar a una que era el “*join on*”, la de compra.

¿Qué se hizo? Primero se investigaron todas las páginas sobre este tema, se hizo una salvaguarda de todo el material que se podía ver, dado que un usuario normal únicamente puede acceder a unas pocas imágenes y no al espacio para miembros. Se realizó una operación de agente encubierto, se cogió una tercera encubierta y se procedió a adquirir el material de pornografía infantil. Se creaba una cuenta en la pasarela de pago e-gold, que luego se cambio a PayPal, y posteriormente a e-Bay, y en ellas se introducían los datos y se hacían las transferencias, normalmente a otras cuentas de esos sistemas de pago, primero fueron 80 dólares, luego varió hasta 95 dólares... Cuando se abonaba se facilitaba la dirección con el usuario y contraseña del sitio web. Éste fue el primer método que se utilizó.

Los clientes era redireccionados desde el sitio de anuncios a uno de pago, que disponía de un index (página principal) falso con el propósito de falsear la compra, de tal forma que redireccionaba y cuando se hacía la compra te indicaba: “La compra todavía no ha sido efectuada”, “No hemos cargado el importe de la tarjeta, envíenos un correo diciendo nos que efectivamente ha hecho usted el pago, nosotros los comprobaremos y le diremos lo que tiene usted que hacer”. Tuvimos acceso a los datos introducidos en esa base de datos y obtuvimos la lista de los clientes que habían comprado pornografía infantil. En España detuvimos a 64 personas en la posterior Operación Tornado, y también encontramos parte de la organización internacional, seis de los cuales estaban en España.

En ese site falso señalan al comprador qué producto debe adquirir, que tiene el importe exacto de la compra de pornografía infantil. Unas veces era un reproductor de vídeo, otras un software antivirus, etc, para ocultar el motivo de la transacción, de tal forma que cuando pulsaba en “my billion” o en “Orion”, otro site también dedicada a esto, se falseaba la compra, pues figuraba una adquisición y una factura por un reproductor de vídeo, un software, etc. A una empresa que, además, estaba radicada en Panamá.

- 58 ¿Qué es lo que había en España? Los individuos de la organización que se encontraban en nuestro país con documentación falsa y que eran de origen bielorruso, se dedicaban, básicamente, a abrir cuentas que vinculaban a otra en PayPal y ésta la redireccionaban a una bancaria. Los pagos luego los transferían a Bielorrusia. También constituían empresas con el fin de que, igual que Orion, que estaba radicada en Estados Unidos, se hicieran las compras de *software*. Este grupo creó en España la compañía Malcone, por la que le dimos el nombre a la investigación. Malcone recibía los pagos de los usuarios de otros países y los usuarios españoles comprábamos en Orion. Eso dificultaba el seguimiento del dinero. Lo que se hizo fue bali-zar el dinero, la tarjeta de crédito que se utilizó para la compra y se llegó a todas estas investigaciones.

Averiguamos que Malcone iba cambiando de propietario, es decir, fue revendida varias veces durante el proceso. En dos o tres años, hasta seis veces a diferentes personas que facilitaban su cara (no su identidad) para abrir empresas (en este caso era Malcone) o cuentas bancarias. Los que abandonan la empresa abrían cuentas bancarias y el que dejaba de abrir cuentas bancarias creaba la compañía. Y así fueron revendiéndola sucesivamente. Como consecuencia detuvimos a seis personas vinculadas a la organización en España, todas de Rusia o Bielorrusia. Posteriormente detuvieron a 64 personas relacionadas con los compradores.

Esto demuestra que el crimen organizado también se dedica a la pornografía infantil, y que éste, además, parece ser que es un buen negocio. Sólo la Operación ORE, con 7.000 personas a una media de 50 euros, permite hacer una idea, así que imagínense en una país como Estados Unidos, que podía tener el triple de usuarios en aquella ocasión. En España había cientos y no intervenimos en aquella ocasión porque no teníamos la posesión de pornografía infantil todavía tipificada en el año 2003, la modificación de la legislación se realizó más adelante, creo recordar en octubre de 2004.

Recientemente se han realizado otras operaciones como Koala, en la que estaban implicadas más de 20 niñas y el pago era alto, DVD's con una tarifa mucho mayor de 50 euros. Esta organización criminal tenía también su estructura, unos hacían las fotos de las niñas, otros las captaban, otros vendían el material, otros creaban la página web, etc.

El crimen organizado puede llevar sus tentáculos allá donde haya beneficio y uno de esos sitios es también la pornografía infantil.

CRIMEN ORGANIZADO Y NUEVAS TECNOLOGÍAS

CÉSAR LORENZANA GONZÁLEZ
Capitán de la Guardia Civil.
Miembro del Grupo de Delitos Telemáticos de
la Unidad Central Operativa (UCO)

*La Administración está prácticamente adaptada al uso de estas tecnologías,
tenemos firmas y certificados digitales, DNI-e, pasaportes electrónicos.*

61

Considero, y así lo prevé uno de los mayores gurús de Internet, Bruce Schneier, criptógrafo, experto en seguridad informática, y escritor, que la Red ha sido el mayor salto generacional desde la aparición del rock and roll, ha creado una brecha entre nativos e inmigrantes digitales. Estoy seguro que, prácticamente, todos los que estamos aquí no hemos nacido con esta tecnología, hemos tenido que adaptarnos, aprender a utilizarla y convivir con ella, y ha dado una vuelta a muchos de los conceptos e ideas que tradicionalmente se habían establecido en nuestra sociedad.

A día de hoy todos disponemos de un teléfono inteligente, un smartphone, para poder ver el correo, nuestro perfil en las redes sociales, trabajamos desde casa, nos conectamos, y estoy totalmente convencido de que acudimos varias veces al día al terminal para leer nuestros e-mails, si ha salido algo nuevo en Twitter o actualizar el perfil de Facebook. Esto es un comportamiento normal dentro de la sociedad, no resulta anómalo que la gente se desenvuelva, de forma más o menos resuelta, en el entorno digital.

El crimen organizado no iba a ser una excepción, lógicamente. Los grupos organizados forman parte de la sociedad en la que se mueven, con lo cual ellos también se han adaptado a estas tecnologías, al uso de

Internet, sobre todo porque para ellos representa un beneficio. A ninguno se nos escapa que la razón de existir de los grupos organizados no es cometer delitos por el mero hecho de realizarlos o por hacer el mal, su objetivo es económico: ganar dinero. Internet les ha facilitado esa rentabilidad monetaria, les ha ofrecido una serie de ventajas que hacen que sus negocios puedan generar mucho más beneficio, y que la posibilidad de ser descubierto por los cuerpos policiales sea mucho menor. Las nuevas tecnologías han sido un dinamizador para las actividades ilegales de los grupos criminales.

Los cuatro principales factores que ha empujado a estos grupos de delincuencia organizada a poner sus ojos en Internet y a desarrollar ahí su actividad habitual son:

INMEDIATEZ

62 Internet brinda una rapidez que era imposible hace 10 o 15 años. A día de hoy, podemos saber al minuto, al instante, qué es lo que está pasando prácticamente en todo el mundo, y contactar con otra persona en menos de 10 minutos. Cuando no existía Internet, los grupos del crimen organizado carecían de esa inmediatez -no podían comunicarse rápidamente entre sí, necesitaban concertar citas, estar escondidos, adoptar medidas de seguridad, etc-. A día de hoy, simplemente con una cuenta de correo electrónico de usar y tirar, que se crea ex profeso para eso, o un sistema de comunicación encriptado les basta. La agilidad que al resto de la sociedad beneficia, y que ha potenciado los negocios y la economía mundial, también ha provocado este efecto en los grupos de delincuencia organizada.

ACCESIBILIDAD Y FACILIDAD PARA ALCANZAR A LAS VÍCTIMAS

En Internet no hay limitaciones geográficas, no existen fronteras. Desde Madrid puedo organizar una estafa en todo el mundo y alcanzar a muchísimos usuarios, de tal manera que la inversión que hay que realizar para alcanzar a las posibles víctimas es mucho menor que si lo hiciese en la vida real. Basta con enviar un correo masivo, como los que hemos recibido que nos anuncian que hemos ganado un premio en una lotería. Y aunque únicamente caiga en la estafa un 0,1 por ciento de los remitentes ¡es más que suficiente! Se trata de envíos de 10 millones de correos, y si de ese número responden 1000 o 5000 que son estafados con 300 euros o 400 euros ya es rentable. El retorno de inversión es muy alto sobre la inversión realizada.

Ese ejemplo es también aplicable al fraude con las tarjetas en banca electrónica. Hace 10 años para utilizar las tarjetas robadas había que tener acceso físico a esa tarjeta para duplicarla. A día de hoy, basta con enviar un correo electrónico y hasta 40 personas voluntariamente, y engañados, darán los datos de una de sus tarjetas. También ahora se puede comprar por la Red con una tarjeta robada, basta con tener su numeración. Estas ventajas de accesibilidad y facilidad para localizar a víctimas potenciales, es otra de las grandes “excelencias” que ha empujado a estos grupos criminales a poner sus ojos en Internet.

OCULTAR LA IDENTIDAD DEL USUARIO

A nadie se le escapan las posibilidades que ofrece Internet para ocultar la identidad real de las personas que la están utilizando. No es tan elevado como algunos piensan porque si no nosotros no estaríamos aquí, pero sí que ofrece ciertas capacidades sencillas y rápidas para poner trabas a la investigación e intentar dificultar la identificación del usuario. Trabas y mecanismos que en la vida real son mucho más complejos, es decir, obtener un pasaporte o un Documento Nacional de Identidad falsificados es relativamente complejo y costaría dinero. En Internet, adquirir una identidad digital suplantada es relativamente sencillo, basta con enviar millones de correos solicitando cuentas de correo electrónico, contraseñas, o bien diciendo que el correo está lleno y que necesitamos la contraseña para resetearlo y alguien, voluntariamente, la proporcionará.

63

No hace mucho se produjo una filtración en una de las principales redes sociales, centrada en el mundo empresarial y de negocios, en la que se publicaron millones de contraseñas de sus usuarios. No eran contraseñas de 20 o 25 caracteres, sino que había personas que escribían “1234” o su propio nombre o su fecha de nacimiento. No es complicado tener una identidad digital para utilizarla y ocultar la identidad verdadera, y esa dificultad para obstaculizar la labor policial es mucho más sencilla en Internet.

IMPUNIDAD

La falta de castigo está creciendo a día de hoy en Internet. Este problema, que es responsabilidad de todos, se pone de manifiesto sobre todo a la hora de hablar del fraude bancario. Habitualmente, el fraude que sufre la víctima está en torno a los 300 euros, ya que una cantidad mayor llamaría la atención de la entidad bancaria, que podría pararlo. Además, 300 euros ni siquiera está considerado como delito en el Código Penal, con lo cual su persecución es todavía un poco más complicada.

En la mayoría de las ocasiones el banco reintegra la cantidad, con lo que el principal afectado no siente ese perjuicio económico y, por tanto, tampoco muestra excesivo interés en perseguir penalmente este tipo de delincuencia. Los bancos están asegurados y las entidades aseguradoras consideran esta apropiación indebida un fraude, con lo que reembolsan a la entidad bancaria el monto y, por tanto, ellas tampoco sufren esa pérdida. Es más, si alguna vez revelasen las cantidades reales de fraude que sufren o la vulnerabilidad de los sistemas que utilizan podrían perder muchísimo más en cuanto a volumen de negocios se refiere o a nivel de imagen y pérdida de clientes. Tampoco las aseguradoras denuncian porque a éstas les basta con incrementar las primas del seguro en la siguiente anualidad y puede recuperar fácilmente el dinero.

64

Si se echa un vistazo a todos los estamentos que están implicados, se observa que, realmente, nadie sufre esa pérdida, con lo cual nadie tiene verdadero interés en perseguirlo. Ese interés, esa responsabilidad de perseguir este tipo de delitos penalmente reposa, en última instancia, en la policía y estamentos judiciales. Nuestro problema es que 300 euros penalmente son muy difíciles de investigar, sobre todo porque las medidas que hay que aplicar para investigarlo afectan al secreto de las comunicaciones, requieren órdenes judiciales y para la investigación de este tipo de faltas no están previstas estas medidas.

Hace unos dos o tres años, el Tribunal Supremo tuvo que pronunciarse porque la reciente Ley de Conservación de Datos habla de que éstos solo serán entregados a las Fuerzas y Cuerpos de Seguridad para investigar delitos graves, que son aquéllos con una pena superior a cinco años. Entre el 90 y el 95 por ciento de los delitos que se cometen en Internet no alcanzan esas penas, con lo que, de entrada, bloqueaba toda la investigación. Tuvo que hacerse una sentencia aclaratoria diciendo que debido a la forma de comisión del delito y al alcance que podía tener se consideraba igualmente grave, y esto abrió la puerta para investigar.

Esa sensación o pequeño espacio de impunidad que estamos creando, entre otros, nosotros, por no perseguirlo debidamente, dado que carecemos de las herramientas judiciales y procesales para hacerlo, es otro de los factores que está potenciando que las bandas organizadas pongan sus ojos en ese terreno. Éstas saben que las probabilidades de ser descubiertos, de ser investigados a fondo, son mucho más bajas que si se dedicasen a cualquier otro tipo de actividad delictiva en el mundo físico.

Internet ha sido un salto generacional importante y entre otras cosas, lo que ha hecho es bloquear muchos de los principios de la sociedad, tanto de la sociedad civil como de la sociedad jurídica. El concepto de privacidad que manejamos a día de hoy o en el que viven los adolescentes, poco tiene que ver con el que las generaciones anteriores aprendieron. El concepto de intimidad, ciertos valores de secreto, de guardar información para uno mismo, no tienen cabida en la sociedad digital.

En la Red no existen fronteras, pero hoy día existe un intento desesperado por trasladar los tradicionales conceptos de nacionalidad, territorialidad y autoridad judicial de los Estados a Internet. Es un intento totalmente absurdo porque el entorno digital no conoce de espacios territoriales, no conoce de jurisdicciones. No se puede hablar de cuál es la parte que está en España y deben regular sus autoridades. Es uno de los principales problemas porque no existe una regulación específica para Internet.

La policía trabaja con normas que fueron creadas para el mundo físico, en el mundo on-line o hay ninguna norma de colaboración internacional, no hay procesos penales, no hay herramientas judiciales diseñadas específicamente para luchar contra la delincuencia en Internet. Esto hace todavía más complejo la labor policial de investigación, y es conocido por los grupos organizados.

65

Los marcos de tiempos en los que se mueve la delincuencia en Internet no son aplicables para la policía, porque ésta depende, en gran medida, de los datos asociados al tráfico, los que están en los servidores y que son extremadamente volátiles y desaparecen, no dan lugar a ninguna investigación.

Uno de los principales retos para cualquier estamento judicial, fuerzas y grupos de seguridad, los gobiernos y las administraciones, es poder regular este campo delictivo, esta nueva área de la sociedad. Existen parches, adaptaciones, reinterpretaciones, pero no hay nada específico, que sea realmente útil, y eso potencia ese pequeño espacio de impunidad.

Es indudable que la regulación, el marco jurídico, jamás va a estar a la altura de la realidad, pero ni en Internet ni en ningún otro sitio. El mundo de Internet en el que se mueven los “ciberpolicías”, policía 3.0, avanza muchísimo más rápido que el mundo tradicional, con lo cual ese espacio, ese gap que hay entre los comportamientos del mundo real y la tipificación penal, el derecho procesal y el aspecto jurídico que regula la vida en

sociedad, es cada vez es mayor y va a costar alcanzar y ponerse al mismo nivel de esos delincuentes.

El concepto de crimen organizado del mundo tradicional igual no es tan válido dentro de Internet. Por ello, es probable que haya que revisarlo y ver realmente cómo se está organizando la delincuencia en Internet, en lugar de intentar trasladar los conceptos que manejamos, esos principios antiguos, y pretender trasladarlos a la Red. Internet no va a encajar en nuestro sistema jamás, somos nosotros los que debemos encajar nuestro sistema a Internet, y dotarnos de herramientas válidas para trabajar en ella.

A día de hoy, todos los esfuerzos que se han hecho van en sentido contrario (adaptar Internet a la vida real, bloquear páginas, regular el acceso, aplicar conceptos nacionales, etc). Debemos olvidarnos de todo eso, que ha pasado a la historia. En Internet no hay países, nadie pregunta por la nacionalidad o se solicita el pasaporte cada vez que nos conectamos a un sitio web.

66 De la misma manera que el ciberespacio ha influido en todos los aspectos de nuestra vida, en los negocios, en las administraciones, en los gobiernos, en el concepto de sociedad que tenemos, también ha influido en la delincuencia organizada que, por supuesto, están creando sus propias formas de delinquir en Internet.



SEGUNDO PANEL

LAS REDES SOCIALES Y LA TRANSFORMACIÓN DE LA GESTIÓN PÚBLICA

EDUARDO BAEZA PÉREZ-FONTÁN
Director del Departamento de Análisis y Estudios.
Gabinete de la Presidencia del Gobierno

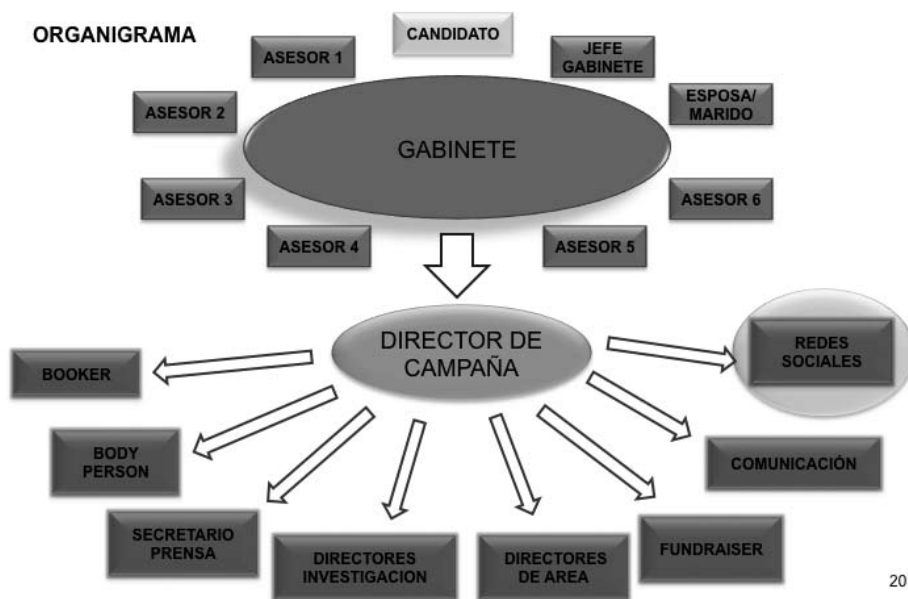
69

El planteamiento de las campañas electorales desde el punto de vista de la estrategia de comunicación digital u on-line se basa en seis aspectos. El primero no es directamente digital, pero es importante porque los siguientes cinco puntos versan sobre el primero. Soy abogado de profesión pero, desde muy pequeño, tuve interés en la gestión de las campañas electorales, en su día a día y en como un ciudadano de a pie se convierte en candidato y llega a ser diputado o presidente de un gobierno.

El último trienio he trabajado de forma muy activa en estas campañas. La más reciente fue la del actual Presidente del Gobierno español, Mariano Rajoy, a la que me incorporé para dirigir la campaña on-line en las elecciones generales del año pasado. Con anterioridad había colaborado con Mike Capuano, diputado del Estado norteamericano de Massachussets, que ganó su asiento en el año 2010; con el demócrata Deval Laurdine Patrick, actual Gobernador del Estado de Massachussets, para quién trabajé como voluntario en redes sociales; con el republicano Robert Portman, senador del Estado de Ohio, que obtuvo su victoria también en 2010; y con Gina Parody, que postuló a la alcaldía de Bogotá. En este caso perdimos, pero fue una experiencia muy bonita y enriquecedora porque me proporcionó una visión más profunda que cuando consigues la victoria.

ORGANIGRAMA PARA LA DIRECCIÓN DE UNA CAMPAÑA POLÍTICA

Creación de un equipo independiente dentro la campaña



70

20

El gabinete del candidato está constituido por los asesores más cercanos, su mano derecha, que es el jefe de su gabinete y, probablemente, también su marido, esposa, novia, novio, etc. Este órgano viene a ser como el consejo de administración de la empresa, el núcleo duro, y es el que elige al Director de la campaña, que es como el Director General de la compañía, es el máximo responsable de la gestión del día a día operativo, reportando directamente al gabinete.

La gran diferencia entre Estados Unidos y España es que en el primero el Director de la campaña no es un político, sino un profesional afiliado al partido pero sin cargo público que se dedica, exclusivamente, a esa tarea y con un sueldo bastante alto, que oscila entre 4.000 euros y 20.000 euros mensuales. En España se valora mucho la amistad o el compañerismo, y esta figura la suelen ocupar amigos cercanos del candidato, un ejemplo es el de la diputada Ana Mato en la campaña de Mariano Rajoy de 2011.

Otro puesto clave dentro del organigrama es la figura que en inglés se denomina booker o scheduler, y que se responsabiliza exclusivamente de administrar el tiempo del candidato, gestionar su agenda. Es una pieza que reporta directamente al Director de la campaña y decide el tiempo, dónde va y qué acepta el aspirante.

También es esencial el body person, que es quién acompaña al candidato en todos sus actos y desplazamientos durante la campaña. Su perfil es el de una persona joven y muy discreta, siempre en un segundo o tercer plano (le lleva el maletín, las gafas, le coge los papeles) y que reporta al Director, que no viaja con el aspirante. Juega un papel clave para el Director porque son sus ojos y oídos, reportándole todo lo que ocurre diariamente en torno al candidato.

En esa estructura también existe un equipo de investigación que se divide en dos áreas: los que investigan a tu candidato y los que investigan a aquél o a aquéllos con los que compite. Los resultados se recogen en unos documentos llamados “libros blancos” que se actualizan a diario y que, en el caso del postulante para el que trabajas, incluyen todos los datos de su vida: donde nació, qué estudió, cuánta familia tiene, sus habilidades, qué deportes practica, y permiten al Director y su equipo preparar los debates electores y conocer muy bien al hombre, al candidato al que asesoran, con sus puntos fuertes y débiles.

71

La parte más técnica de la campaña la suelen realizar profesionales, como por ejemplo profesores, que son expertos en nichos de mercado y que se denominan Directores de Área. Se encargan de analizar, estudiar e investigar las distintas áreas que serán foco de debate durante la campaña. Sus conclusiones servirán de base para montar un programa político.

El penúltimo puesto es el Director de Comunicación, que en nuestro mundo le llamamos el Secretario de Prensa. Es el que se encarga de trabajar con los medios de comunicación. Su papel es significativo porque, junto con el aspirante, es la única persona del equipo que tiene proyección pública, que habla con los medios.

Dado que en Estados Unidos las campañas electorales se financian con fondos privados, también existe una figura muy importante, que no hay en España, y que es el fundraiser. Es el responsable de recaudar el dinero a través de eventos, donaciones para la campaña, etc.

Y por último, está el área que centra la atención en esta ponencia: las redes sociales, con el Director de Nuevas Tecnologías y Redes Sociales.

LAS REDES SOCIALES EN LAS CAMPAÑAS ELECTORALES

Hasta el año 2008 no existía un Departamento de Redes Sociales, de Internet o de Estrategia de Nuevas Tecnologías dentro de las campañas electorales. Fue el Presidente de los Estados Unidos, Barack Obama, quien instauró, dentro de su equipo para la campaña de ese año, un departamento propio que se encargaba, exclusivamente, de las redes sociales. Lo que sí se daba con anterioridad, desde 1996, era una pequeña sección que reportaba al Secretario de Prensa, no era una Unidad autónoma.

En el Departamento de Redes Sociales de una campaña electoral hay cinco puntos:

- 1) La creación de un equipo independiente que se dedique exclusivamente a hablar y a transmitir en las redes sociales.
- 2) La inversión on-line, que está viviendo una tendencia al alza muy importante, dado que la cuota de mercado en ese ámbito está creciendo entre 2 y 3 puntos al año con respecto al mundo off-line.
- 3) La estrategia de comunicación, que debe ofrecer una respuesta rápida.
- 4) La maximización de momentos oportunos. Puedes hacerlo en situaciones muy concretas a través de las redes sociales.
- 5) La cercanía y capacidad de movilización de masas de forma muy rápida y gratuita.

Barack Obama implantó la figura del Director de Redes Sociales, con dependencia del Director de la campaña. Hay que tener en cuenta que, prácticamente, la mitad de las páginas web son espacios para compartir y conversar con el ciudadano, quién contribuye, envía sugerencias. Hasta hace cuatro años esto no existía y avanzan a un gran ritmo.

A continuación se muestra algunas homes de candidatos americanos.

Estrategia de campaña digital



ESTRATEGIA ON-LINE DE LA CAMPAÑA 2011 DE MARIANO RAJOY

73

Se identifican seis áreas estratégicas, que pueden trasladarse al mundo empresarial:

- Una página web sólida
- Presencia en las redes sociales. Aunque hay muchas, hay que identificar las que se considera que van a tener más incidencia. En este momento están identificadas: Twitter, Google +, LinkedIn y Flickr
- Los jóvenes utilizan más la combinación de vídeo con redes sociales que solo las redes sociales. El canal YouTube es el segundo motor de búsqueda más potente, después de Google
- Es clave emplear tecnología móvil
- Disponer de una base de datos de afiliados al partido, seleccionados por código postal, edad, etc. para hacer campañas sectoriales
- Contar con cibervoluntarios, que son la masa crítica de personas que se unen a la campaña para ayudar a movilizar el mensaje

El lanzamiento de la web de Mariano Rajoy supuso el análisis de varias opciones, hasta que optamos por la que transmitía mejor los valores que, en ese momento, estaba emitiendo el candidato durante la campaña. Mi opinión o la de los profesionales vale muy poco, al final son los ciudadanos los que toman la decisión.

www.rajoy.es

10 de julio 2012



36

Volviendo al tema de la inversión on-line, en el caso de los votantes norteamericanos un 68 por ciento de ellos buscan información en Internet, de los que cuatro de cada 10 acuden a medios tradicionales y seis a Google. En cambio, la financiación económica en las campañas, ha pasado de un 1,6 por ciento en 2008 y en el 11 por ciento en la actualidad. Es decir, hay un margen muy amplio para invertir más y llegar más al ciudadano.

ELABORACIÓN DEL MENSAJE

Hay 5 categorías de votantes (que también pueden ser consumidores de un producto):

- 1) Voto base leal, que son los votantes base del candidato. Pase lo que pase van a votar al partido.
- 2) Voto base adversario, que son los electores base de los adversarios. Pase lo que pase nunca van a votar al partido.

- 3) Voto persuasible leal, que son los ciudadanos con tendencia hacia nuestro partido pero que pueden ser inducidos hacia el adversario o a la abstención.
- 4) Voto persuasible adversario, aquellas personas con tendencia hacia el partido del adversario pero que pueden ser convencidos hacia nuestro candidato o a la abstención.

El 3 y el 4, el votante persuasible, es el más interesante desde el punto de vista de las redes sociales porque es en estos dos nichos es donde se gana o se pierde una campaña electoral. Se trata de que el 3 vote a tu partido o intentar que el 4 se convierta en indeciso. Es la guerra del día a día de los vendedores.

- 5) Voto indeciso: son los votantes desinteresados o sin tendencia histórica.

ELABORACIÓN DEL MENSAJE

Este cuadrante refleja el universo de una campaña electoral. Quien controle las cuatro cuadrículas del mensaje gana.

Campañas electorales

10 de julio 2012

ELABORACION DEL MENSAJE

La mayoría de las campañas conectan todas las variables mediante un sistema de cuadrantes que consiste en cuatro categorizaciones:

NUESTRO MENSAJE	SU MENSAJE
Lo que decimos sobre NUESTRA campaña	Lo que ellos dicen sobre SU campaña
Lo que decimos sobre SU campaña	Lo que ellos dicen sobre NUESTRA campaña

De otra manera

Tu sobre ti	Ellos sobre ellos
Tu sobre ellos	Ellos sobre ti

Si yo controlo muy bien lo que estoy diciendo sobre mi campaña o la del adversario y si sé lo que ellos están diciendo sobre mi campaña y sobre su propia campaña cada semana, hay muchas posibilidades de que la campaña vaya bien o muy bien. O dicho de otra manera: si controlo el “tú sobre ti” y el “tú sobre ellos” y lo que “ellos piensan sobre ellos” y “sobre mi (ti)”, nuestra

campaña va por buen camino. Ambos son dos ejemplos muy sencillos, aunque quizá no extrapolables a España.

En el ámbito del marketing on-line hay dos ejemplos claro en la campaña 2008 de Obama que tuvieron un gran éxito. Uno fue la calculadora en su página web, en la que el ciudadano marcaba su sueldo anual y salía la cantidad de dinero que iba a ahorrarse en impuestos si Barack Obama resultaba elegido Presidente. En realidad era una herramienta para que fuera el ciudadano el que acudiera a la web del candidato. Y la otra fue a través de SMS, en este caso Barack Obama animaba a los ciudadanos a que le remitieran su número de móvil, y les garantizaba que cuando supiera quién iba a ser su Vicepresidente se lo comunicaría. Esta acción captó en las 24 horas antes al anuncio de Obama de su candidato a ser Vicepresidente más de cuatro millones de móviles.

En las redes sociales es muy importante la actitud de cercanía y tener un canal de doble comunicación. Son detalles muy simples pero también trasladables a cualquier profesión. Está testadísimo que un correo electrónico cuanto más coloquial sea el tono más gente lo abre, independientemente del rango de la persona a quién nos dirigimos. Empezar el correo con “Carlos” en lugar de “Estimado/Querido Carlos”, no incluir el puesto en la firma sino simplemente “Eduardo” y acompañar los mensajes con un vídeo cercano en formato pop up (ves la imagen directamente no tienes que abrir un link) son éxito.

76

Campañas electorales



10 de julio 2012

Toby --

A record 100,000 people rallied with Barack in St. Louis yesterday, and another 75,000 in Kansas City last night. Back in Chicago, we were tallying up our latest fundraising numbers.

Supporters like you have completely transformed how political campaigns raise money, so I wanted you to be the first to know how we did in September.

I recorded a short video to share the latest numbers:

WATCH THIS VIDEO
TO GET THE
LATEST
NUMBERS

WATCH NOW

When Barack entered this race, he put his faith in the power of ordinary supporters like you coming together and building a movement for change from the bottom up.

That's exactly how we got this far -- and you should feel proud of all we have accomplished together.

But with just 16 days left in this election, we can't slow down now. Please take a minute to watch the video and find out where we stand:

<https://donate.barackobama.com/septembernumbers>

Thanks for everything you're doing,

David

David Plouffe
Campaign Manager
Obama for America

DONATE

LAS REDES SOCIALES Y LA TRANSFORMACIÓN DE LA GESTIÓN PÚBLICA

ANDRÉS MEDINA MEDINA
Director de Programas de Análisis y Estudios.
Gabinete de la Presidencia del Gobierno

La gestión pública en las redes sociales plantea dos enfoques:

77

- La gestión pública ha existido, y existirá, sin redes sociales
- Si no estás donde se encuentra el ciudadano pierdes legitimidad ante éste. Hay que hallarse donde está el ciudadano, porque sino la gestión pública corre el riesgo de que éste tenga una percepción inferior de la Administración de la que a ésta le corresponde

SITUACIÓN ACTUAL DE LAS REDES SOCIALES EN ESPAÑA

Recientemente, el Centro de Investigaciones Sociológicas (CIS) ha publicado un estudio sobre hábitos en Internet y en las redes sociales. Sus conclusiones son que, en general, los españoles consideran necesarias las redes sociales: por sexos, esta afirmación es de un 28 por ciento en los hombres y un punto menos en las mujeres; por edades, cuanto más longeva es la persona descende la necesidad de utilizarlas; y en cuanto a su frecuencia de uso, el 70 por ciento las ha usado en la última semana y el 90 por ciento si el dato se refiere a los jóvenes. Ellos son nativos digitales, y la Administración pública no puede darles la espalda, debe estar precavida y hablar su mismo lenguaje.

La Administración debe preguntarse qué hacer con las redes sociales y, si admite que son imparables, debe saber que quiere hacer con ellas, cuál es su estrategia, y poner en marcha proyectos reales para no perder la legitimidad frente al ciudadano.

BARRERAS DE LAS REDES SOCIALES EN LA ADMINISTRACIÓN

Las barreras que la Administración puede encontrar en ese nuevo enfoque son cuatro: cultural, procesos, organización y forma de relación. La Administración debe identificarlas y resolverlas o tendrá un problema.

Cultural

En la sociedad cohabitan gentes de distintas generaciones con distintas formas de pensar y maneras de actuar. La barrera cultural hay que romperla y, para ello, es necesario poner al ciudadano en el centro de la gestión de la institución pública, en su núcleo de la actuación: porqué, para qué y con qué motivos se hacen las cosas.

78

Procesos

Los cambios son muchos y de mucha calidad, lo que hace que los procesos vayan caducando. También prescriben los de la Administración, y ésta debe poner las soluciones para que el ciudadano perciba que la institución pública funciona. Hay que colocar al ciudadano en el centro.

Organización

Partimos de unas organizaciones jerárquicas estipuladas y burocratizadas que han de habituarse a una situación horizontal, la que representan las redes sociales, que rompen esos esquemas. Se plantea un conflicto que hay que solventar, hay que adaptarse a la sociedad.

Formas de relación

Las formas de relación, que en su día cambiaron con el teléfono, ahora lo hacen con el correo electrónico y las redes sociales. No sabemos que vendrá después, pero cambian continuamente.

La gestión pública debe ubicar al ciudadano en el centro y crear un canal en el que emita y que permita a la gente comunicarse con la Administra-

ción. Es diferente ser que estar. Hay dos ejemplos de instituciones públicas que puede servir:

- Uno es un tuit que publicó la policía solicitando la colaboración ciudadana para localizar a una persona en la zona de la Costa del Sol. Las fuerzas de seguridad consideraron que ésta era una herramienta para divulgar el mensaje y contar con la colaboración ciudadana. El problema que se plantea en este caso es que hay que diferenciar lo importante de lo superfluo entre las miles de respuestas recibidas, gestionando ese gran volumen
- Otro ejemplo es la página del Reino Unido Patient Opinión, que recoge la colaboración del paciente en la gestión del hospital para ayudar a mejorar esa institución

Si esta actitud no parte de la institución pública entonces lo hará el ciudadano, y se producirá un distanciamiento y una pérdida de legitimidad de la gente ante la Administración.



POWERPOINT

ANDRÉS MEDINA MEDINA
Director de Programas de Análisis y Estudios.
Gabinete de la Presidencia del Gobierno



Las redes sociales y la transformación de la gestión pública

10 de julio 2012



Índice parte I



10 de julio 2012

Introducción

Situación de las redes sociales en España

Estrategia

Ejemplos

La gestión pública y las Redes Sociales



10 de julio 2012

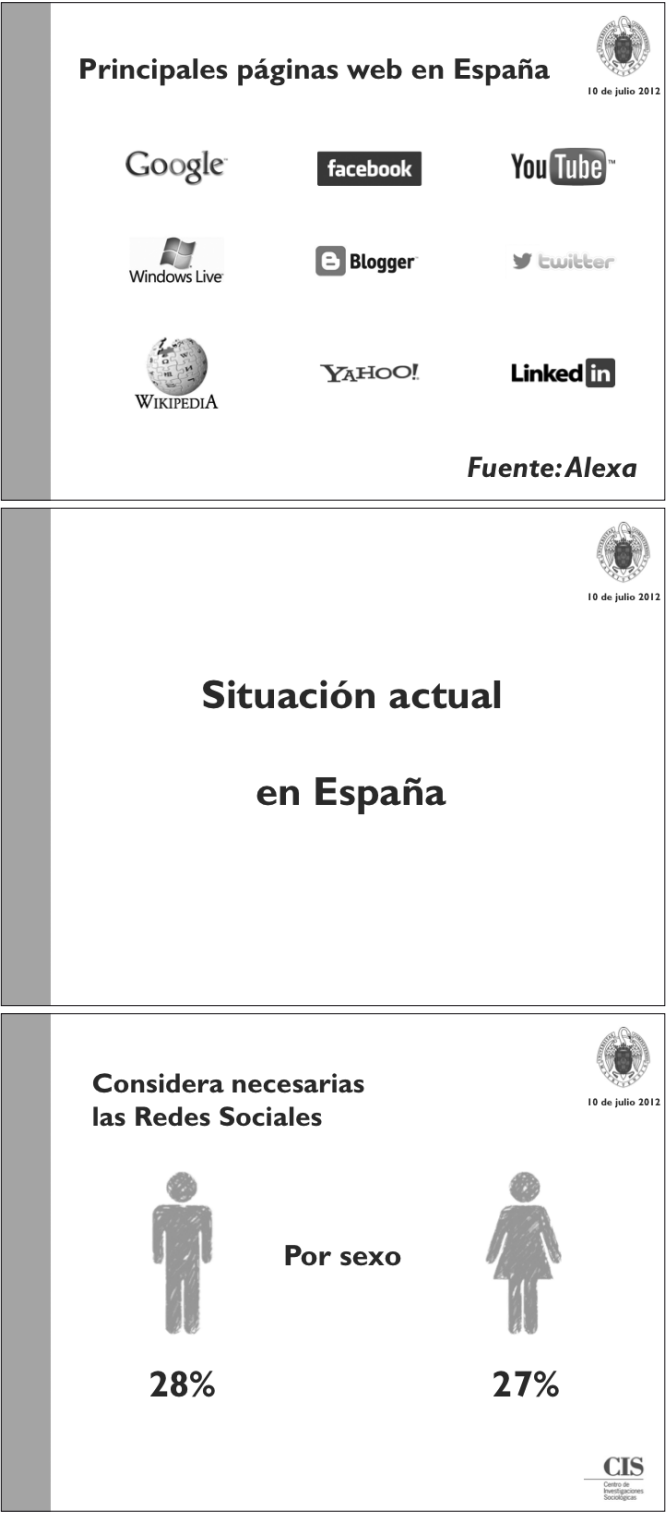
- **La gestión pública ha existido sin Redes Sociales**
- **Riesgo: pérdida de relevancia y de la percepción de legitimidad**

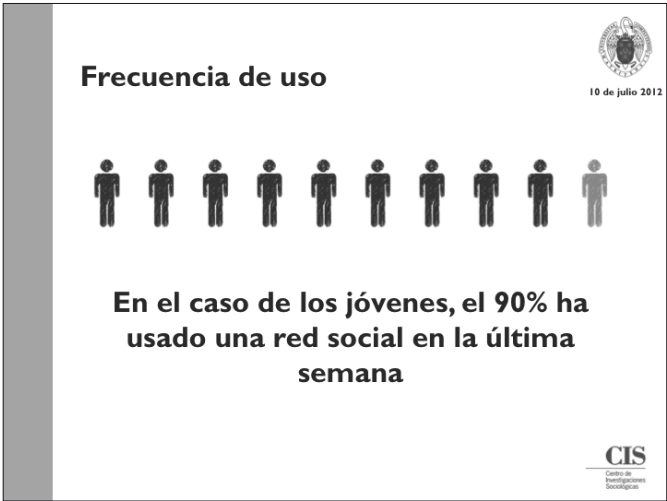
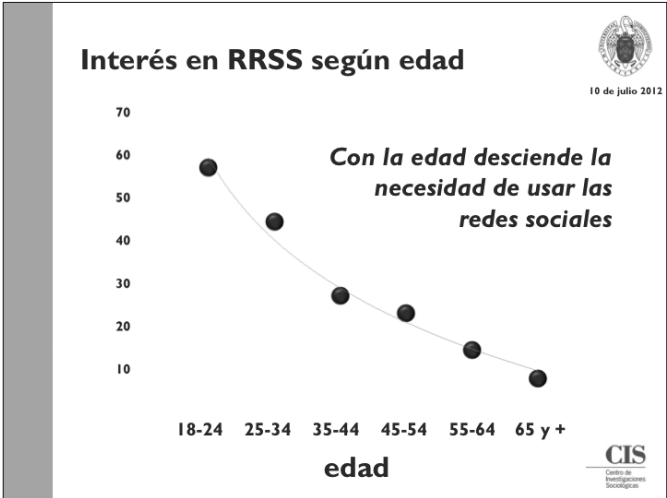
La gestión pública y las Redes Sociales



10 de julio 2012

***Hay que estar donde
está el ciudadano***







10 de julio 2012

VISIÓN

*“Si no sabes a dónde vas,
nunca sabrás si has llegado”*



10 de julio 2012

Principales barreras

- **Cultural:** el ciudadano es el centro
- **Procesos:** rediseñarlos
- **Organización:** jerarquía vs eficiencia
- **Formas de relación:** Del “sello” al email



10 de julio 2012

informar

vs

conversar

Ejemplos



Policía Nacional @policia

Por favor, RT: Buscamos al asesino de 4 personas en Reino Unido, que puede estar escondido en Costa del Sol, Cádiz.... yfrog.com/oc9r4yp



3,330
RETWEETS

31
FAVORITES

4:23 PM - 6 Jul 12 via TweetDeck · Details



10 de julio 2012
6 Jul

86

Patient Opinion
Every voice matters

An independent site about your experiences of UK health services, good or bad
We pass your stories to the right people to make a difference.
[More about Patient Opinion](#)

Home [Tell your story](#) [About us](#) [Search](#) Search for stories about...
ing Leeds General Infirmary, heart surgery, depression

We believe that patients' feedback - good or bad - is essential to improving UK health services.
Tell us what was good and what could be improved, say thanks or call for change - we'll pass your stories to the people in the health services who can make a difference.
[Tell your story - Make a difference](#)

Featured stories [View latest stories](#)

"We found one particular midwife *very rude*"
UNREAD STORY [Read more](#)
Experienced by 3 others
About: St Mary's Hospital / Maternity care

"The room they were in was stripped down *while they were still there*"
UNREAD STORY [Read more](#)
About: King's College Hospital (Denmark Hill) / Maternity

"The midwives were amazing and very helpful, and everything was explained"
STORY HAS A RESPONSE [Read more](#)

Who's listening to your stories?
40,245 stories told
1,868 staff listening
In the past month...
50 % of stories received a response
14 % of responses to concerns led to change

This week: what are people saying?



10 de julio 2012

arreglaMicalle BETA
Si el ayuntamiento olvida, la comunidad recuerda.

Inicio [Enviar denuncia](#) [Ver todas las denuncias](#) [Seguirnos](#) [Ayuda](#) [Contacto](#)

¿Para qué sirve arreglamicalle.com?
Desde arreglamicalle queremos animar a todos los Arreglamicalle.com es el lugar de encuentro de ciudadanos y ayuntamientos para la gestión de incidencias del municipio. Arreglamicalle es un plataforma web que ayuda a la cooperación local a gestionar eficientemente las incidencias con la participación ciudadana.

Ciudadanos
Regístrate para publicar incidencias sobre tu municipio

Ayuntamientos
Date de alta y gestiona las incidencias urbanas

Arreglamicalle
Arreglamicalle disponible para servicios móviles de Android 2.2 en adelante. Descarga en Android Market

Para la aplicación desde tu móvil
Para la aplicación desde tu móvil visita [http://m.arreglamicalle.com](#)
Llévate de móviles compatibles



10 de julio 2012

Las redes sociales y la gestión pública

Estrategia de comunicación online en campañas electorales

Eduardo Baeza
Director del Departamento de Análisis y Estudios
Gabinete de la Presidencia del Gobierno



Índice parte II

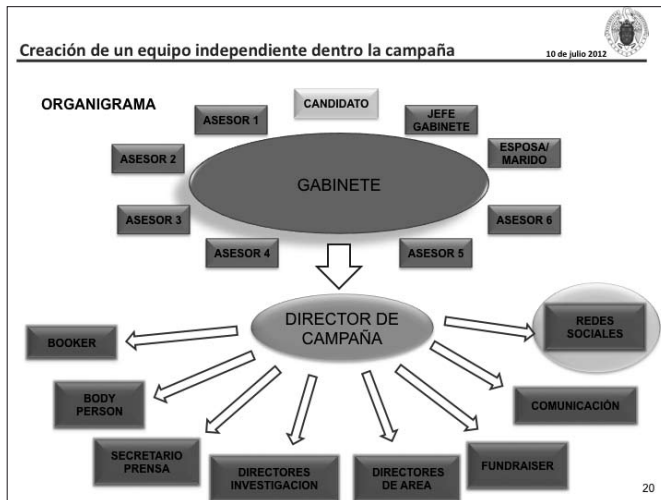
10 de julio 2012

1. Creación del gabinete y equipo directivo de campaña
3. Últimas tendencias en campañas online
4. Estrategia online campaña Rajoy 2011
5. Inversión online
6. Estrategia de comunicación
7. Online marketing
 - Cercanía
 - Maximización de momentos oportunos ("timing")

Campañas 2009-2012

10 de julio 2012





Gabinete y equipo directivo

1. GABINETE

- Máximo órgano de la campaña
- Presidido por el candidato
- Composición: 5 -10 personas
- No debe crecer en tamaño
- Sólo entra un nuevo miembro si sale otro. *Consistencia es vital*
- Propone las directrices generales de la campaña
- Se reúne regularmente en su sede central
- Convoa al Director de Campaña, asesores externos y demás directores

Equivale al consejo de administración de una empresa

- ✓ En campañas de EE.UU., el gabinete suele estar compuesto entre 6 y 12 personas.
- ✓ Incluyen: jefe de gabinete, esposa/marido/pareja del candidato, políticos (en activo y/o jubilados) y amistades o familiares cercanos al candidato.

Gabinete y equipo directivo

2. DIRECTOR DE CAMPAÑA

- 1 sola persona
- Responsabilidad máxima sobre la coordinación y el día a día operativo de la campaña
- Acceso directo y constante al candidato
- Reporta directamente al candidato y a su gabinete ejecutivo
- *Low profile* - no esta en primera línea de prensa. No es el protagonista
- Profesional, experto en campañas con experiencia en dirección de equipos
- Idealmente, sin aspiraciones políticas
- Suele ser la primera persona que se contrata en la campaña

- ✓ En EE.UU., los directores de campaña suelen ser personas afiliadas al partido pero sin cargo publico. Se dedican exclusivamente a dirigir campañas

- *David Plouffe* (08); *Jim Messina* (12): Barack Obama
- *Steve Schmidt*: John McCain
- *Patti Solis Doyle*, *Maggie Williams*: Hillary Clinton
- *David Wilhelm*, *James Carville*: Bill Clinton
- *Ken Mehlman*: George W. Bush



David Plouffe



Steve Schmidt

- ✓ Sueldo medio durante la duración de la campaña: €4.000 - €20.000/mes

Gabinete y equipo directivo

10 de julio 2012



3. SECRETARIA DE AGENDA

- "Booker" o "Scheduler" en anglosajón
- Profesional que se encarga exclusivamente de administrar el tiempo del candidato
- Reporta directamente al director de campaña
- Coordina el tiempo del candidato y lo reparte de acuerdo con las necesidades diarias de la campaña
- Suele ser una persona que conoce bien al candidato
- En EE.UU., suelen ser antiguas secretarías/secretarios
- No tiene contacto con la prensa
- No se encarga de las relaciones con la prensa

Gabinete y equipo directivo

10 de julio 2012



4. SECRETARIO PERSONAL

- "Body Person" en anglosajón
- Físicamente acompaña al candidato a todos los actos y desplazamientos durante la campaña.
- Es la sombra del candidato
- Mantiene al candidato informado sobre su horario
- Lleva los discursos, maletín, chaqueta, etc. del candidato
- Anota las personas a las que el candidato saluda
- Lleva una "Flic", graba y saca fotos
- Ojos y oídos del director de campaña
- Reporta directamente al director de campaña
- Organizado, metódico, (joven), discreto, que sabe "camuflarse" en los actos
- No habla con la prensa salvo instruido para ello



Reggie Love siguiendo y ayudando a Obama



✓ El Body Person de Barack Obama es Reggie Love

Perfil: joven, abierto, simpático, ex-jugador NFL
Actualmente trabaja en la Casa Blanca



Gabinete y equipo directivo

10 de julio 2012



5. EQUIPO DE INVESTIGACION DE CANDIDATOS

- Cada campaña tiene 2 equipos de investigación
- 1 para nuestro candidato y otro para el adversario (o adversarios)
- Juegan un papel fundamental dentro de la estrategia de la campaña
- Misión principal: Investigar y documentar TODO sobre nuestro candidato y sobre adversario
- Información es almacenada en 2 Libros Blancos, uno por candidato
- Contenido: información sobre familia, colegios, carreras, notas, impuestos, discursos, entrevistas, mítines, controversias, enfermedades, fotos, etc. TODO.
- Libros "vivos" - se actualizan a diario
- Es muy importante ser igual de riguroso con nuestro candidato que con el adversario
- Cargos estáticos y con base en la sede de la campaña
- Suelen tener un amplio equipo y trabajan en coordinación con el departamento de Prensa

Gabinete y equipo directivo

10 de julio 2012



6. DIRECTORES DE ÁREAS POLÍTICAS

- Cada campaña contrata a expertos en áreas políticas como Directores de Área
- Número de directores: comúnmente entre 4 – 8
- Contratan a los mejores
- Se encargan de analizar, estudiar e investigar las distintas áreas que serán foco de debate durante la campaña
- Sus conclusiones servirán de base para montar el programa político
- Suelen tener un equipo de apoyo
- Contratados por tiempo parcial o tiempo completo
- No necesariamente afiliados al partido

Gabinete y equipo directivo

10 de julio 2012



7. SECRETARIO DE PRENSA (DIRECTOR DE COMUNICACIÓN)

- Es la persona encargada de trabajar con los medios de comunicación
- Enlace directo y persona de contacto frente a los medios
- Director de todo el departamento de comunicación de la campaña
- Reporta al director de campaña
- Persona con dilatada experiencia profesional con los medios
- Gran comunicador, con credibilidad, diligente
- Sabe *lidar* con la prensa: no se precipita con la información, sabe cuando estar cayado
- Contrasta todos los comunicados de prensa con el Director de Campaña antes de anunciarlos
- Tiene un equipo de periodistas, escritores e investigadores interno
- Saldrá en la prensa a menudo. Buena presencia y trato con los medios

Gabinete y equipo directivo

10 de julio 2012



8. DIRECTOR DE NUEVAS TECNOLOGÍAS Y REDES SOCIALES


- Esta al frente del departamento de nuevas tecnologías (o redes sociales)
- Diseña y actualiza todo lo relacionado con el mundo de internet del candidato
- Pagina oficial de la campaña, blogs de la campaña y de los candidatos, *Facebook*, *Tuenti*, *Twitter*, *YouTube*, *foursquare*, etc.
- Su equipo se encarga de responder a TODOS los emails enviados a la campaña y actualizar los perfiles de los candidatos
- Estrecha coordinación con el Departamento de Prensa, para coordinar el mensaje vía email
- Decide la política de publicidad en internet (banners)
- Reporta al director de campaña
- Departamento con mayor número de voluntarios

Gabinete y equipo directivo


10 de julio 2012

9. FUNDRAISER

- Esta figura es novedosa en España
- Departamento clave en EE.UU. y extrapolable a España
- Equipo de personas "bien conectadas" social y económicamente ("door openers"), lideradas por una persona
- Están dispuestos a relacionarse para crear más visibilidad en ciertas áreas geográficas o sociales y organizar todo tipo de eventos, en coordinación con el secretario de agenda
- Finalidad: Recibir donaciones y aumentar la exposición del candidato en determinados círculos
- Incluyen: empresarios, deportistas, cantantes, figuras internacionales, etc.
- Sin sueldo. Como contraprestación se les permite acceso directo al candidato.
- Campaña de Obama les obsequiaba con divulgación de comunicados con anterioridad a hacerse públicos. Se tienen que sentir privilegiados.



Michelle y Barack Obama con Oprah



Terry McAuliffe – Chief Fundraiser de las campañas de 1992 y 1996 de Bill Clinton y de Hillary Clinton (2008)

91

Campañas electorales

10 de julio 2012

ULTIMAS TENDENCIAS EN CAMPAÑAS ELECTORALES
- ESTRATEGIA DIGITAL -

1

Creación de un equipo independiente dentro la campaña

2

Investir Online: del 4% en 2008 al 11% en 2012

3

Estrategia de comunicacion: ➡ Respuesta rápida

4

Maximización de momentos oportunos ("timing")

5

Cercanía y movilización

30

Organigrama de campaña

10 de julio 2012

ORGANIGRAMA

CANDIDATO

JEFE GABINETE

ESPOSA/MARIDO

ASESOR 1

ASESOR 2

ASESOR 3

ASESOR 4

ASESOR 5

ASESOR 6

GABINETE

DIRECTOR DE CAMPAÑA

BOOKER

BODY PERSON

SECRETARIO PRENSA

DIRECTORES INVESTIGACION

DIRECTORES DE AREA

FUNDRAISER

COMUNICACION

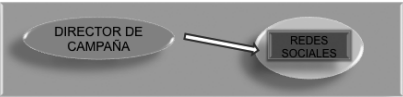
REDES SOCIALES

31

Estrategia de campaña digital

1. CREACIÓN DE UN EQUIPO INDEPENDIENTE DE REDES SOCIALES

- Prioritario desde el primer día
 - Primera vez que el departamento de Redes Sociales no depende del departamento de comunicación – mismo nivel estructural
 - Relevancia por tener el mismo estatus dentro de la campaña
 - Respuesta rápida. Tener el mismo estatus hace que el equipo pueda trabajar con independencia y mover las ideas con rapidez por la cadena de mando
- Emails son revisados, aprobados y enviados en pocas horas para poder capitalizar momentos críticos y crear nuevos ciclos de noticias sin tener que esperar a las tradicionales



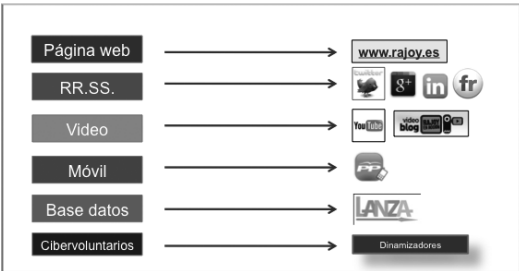
Estrategia de campaña digital



Estrategia online Rajoy – campaña 2011

10 de julio 2012

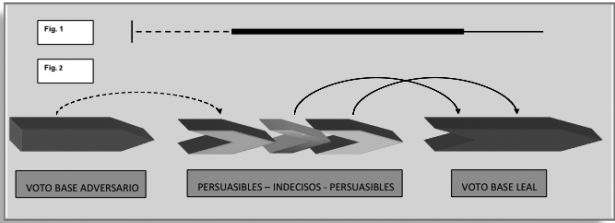
IDENTIFICACIÓN DE 6 ÁREAS ESTRATÉGICAS





Elaboración del mensaje

- 5 Categorías de votantes:
 1. Voto base leal - votantes base de nuestro candidato
 2. **Voto base adversario** – votantes base de los adversarios
 3. **Voto persuasible leal** – votantes con tendencia hacia nuestro partido pero que pueden ser persuadidos hacia el adversario o abstención
 4. **Voto persuasible adversario** – votantes con tendencia hacia el partido del adversario pero que pueden ser persuadidos hacia nuestro candidato a abstención.
 5. Voto indeciso – votantes desinteresados o sin tendencia histórica



Campañas electorales

10 de julio 2012

ELABORACION DEL MENSAJE

La mayoría de las campañas conectan todas las variables mediante un sistema de cuadrantes que consiste en cuatro categorizaciones:

NUESTRO MENSAJE	SU MENSAJE
Lo que decimos sobre NUESTRA campaña	Lo que ellos dicen sobre SU campaña
Lo que decimos sobre SU campaña	Lo que ellos dicen sobre NUESTRA campaña

De otra manera

Tu sobre ti	Ellos sobre ellos
Tu sobre ellos	Ellos sobre ti

39

Campañas electorales

10 de julio 2012

MARKETING ONLINE

- \$16M en anuncios online (McCain \$3.6M)
- \$10M en Google Ads

Marketing para jóvenes y primeros votantes



"Calculadora Obama"

"Sé el primero en conocer la noticia"

A través de la pagina web o por SMS



V.P. ANNOUNCEMENT

OBJETIVO: BASE DE DATOS

40

Campañas electorales – gestión online

10 de julio 2012



CERCANÍA

- Establecer contacto de forma "personal" con votantes online
- *"Shine the light"* (poner el foco) en las personas que participan online
- Tono en los emails mas personal e informal

"Carlos" en vez de "Estimado/Querido Carlos"
firma: "Pedro" en vez de "Pedro García"

- Videos menos producidos ("un-cut") para que parezca que lo ha hecho el mismo Director de Campaña o candidato y lo ha enviado a sus "amigos"
- El video se ve dentro del mismo email como un pop-up – sin enlaces
- No poner siempre el titulo o cargo de la persona.
- Crear narrativa que enlace emails y haya continuidad en los relatos
- Actualizar perfiles terminando en una pregunta: ("¿qué opináis vosotros?")

41

Campañas electorales

10 de julio 2012



Toby --

A record 100,000 people rallied with Barack in St. Louis yesterday, and another 75,000 in Kansas City last night. Back in Chicago, we were tallying up our latest fundraising numbers.

Supporters like you have completely transformed how political campaigns raise money, so I wanted you to be the first to know how we did in September.

I recorded a short video to share the latest numbers:



WATCH THIS VIDEO
TO GET THE
LATEST
NUMBERS
WATCH NOW

When Barack entered this race, he put his faith in the power of ordinary supporters like you coming together and building a movement for change from the bottom up.

That's exactly how we got this far -- and you should feel proud of all we have accomplished together.

But with just 16 days left in this election, we can't slow down now. Please take a minute to watch the video and find out where we stand:

<https://donate.barackobama.com/sepembernumbers>

Thanks for everything you're doing.

David

David Plouffe
Campaign Manager
Obama for America

DONATE

42

Últimas tendencias en campañas electorales EE.UU.

10 de julio 2012

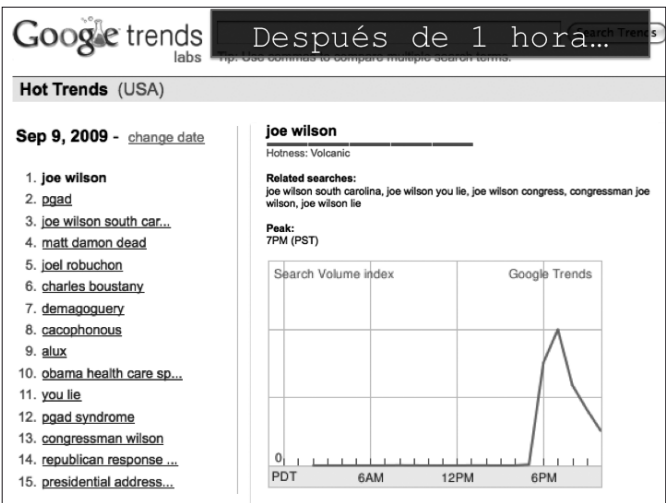


MAXIMIZACIÓN DE MOMENTOS OPORTUNOS ("TIMING")

"Timing is more important than perfection"

- David Plouffe, *Director de Campaña Obama for America 2008*

43



Google joe wilson you lie

Search Advanced Search

JOE WILSON
REPUBLICAN FOR CONGRESS

Thank You
for your contribution

Stand with Joe Today
<http://www.joewilsonforcongress.com>

**Stand for Truth:
Stand with Joe Wilson**

\$1,739,065.00 donated

Instead of working on the important issues facing our nation, the Democratic leadership has proven once again that they would rather play political games and the taxpayer's dollar than work to create jobs or reform health care.

The liberal supporters of a government takeover of health care are using my very vocal opposition as an excuse to muzzle the American people who have been outspoken against their risky plan. But I will not give up and I will not back down from our fight. I will continue to speak the truth.

Will you please make a donation to help me fight back against these partisan attacks?

Thank you for standing with me in this fight.

Joe Wilson
U.S. Representative

Personal Information

FIRST NAME: MIDDLE NAME: LAST NAME:

EMAIL: HOME PHONE:

Support Joe Wilson
www.JoeWilson.com

Video results for joe wilson

You lie! to Rep. Joe Wilson

STAND WITH JOE WILSON

Joe Wilson
Sep 10, "You lie to Rep. Joe Wilson"

Rep. Joe Wilson Yell UPDATE*** GOP Rep. Joe Wilson's health care speech in the House

www.huffingtonpost.com/joe-wilson/you-lie-to-rep-joe-wilson

Cached - Similar -

Sponsored Links

Anti-Joe Wilson Shirt

Joe Wilson
led the President.
Make a donation!

Message
nt Obama

La siguiente

REDES SOCIALES Y PROTECCIÓN DE DATOS PERSONALES¹

ANTONIO TRONCOSO REIGADA
Profesor Titular de Derecho Constitucional.
Universidad de Cádiz

1. INTERNET Y LAS REDES SOCIALES COMO INSTRUMENTOS DE CIVILIZACIÓN

97

Todas aquellas personas nacidas después de 1995 son conocidas como *digital babies*, un término que acuñó el tecnólogo Marc Prensky en 2001 para definir a aquellas personas que no han conocido –ni conciben– un mundo sin Internet y sin telefonía móvil. Desde que tiene uso de razón, esta generación de jóvenes se ha acostumbrado a la presencia constante de las modernas tecnologías de la información y la comunicación. Una de sus señas de identidad es que no sólo emplean las nuevas tecnologías –no son meros usuarios– sino que viven dentro de redes sociales virtuales, donde pasan el tiempo compartiendo novedades y vivencias personales. La extensión del acceso a Internet y la mejora de la velocidad de conexión han posibilitado en los últimos años el nacimiento de las redes sociales –Facebook, MySpace, Tuenti, Twitter, etc.–. Éstas se encuentran influidas por la teoría de “Los seis grados de separación” elaborada por el húngaro Frigyes Karinthy en 1929. En una corta historia denominada “Chains” (Cadenas). Karinthy afirmaba que cualquier individuo puede estar conectado con otra persona del planeta

1.- Una primera versión de este texto fue presentada en la Conferencia Europea de Protección de Datos, celebrada en Edimburgo el 24 de abril de 2009. Con posterioridad, he tenido la oportunidad de exponer esta posición en el Seminario “Privacidad del menor en las redes sociales”, organizado por la Fundación Solventia y el Colegio de Abogados de Madrid en junio de 2009.

a través de una cadena de conocidos que no supere en más de seis el número de intermediarios. Duncan J. Watts, de la Universidad de Columbia, realizó un envío masivo de correos electrónicos a nivel mundial para comprobar que la teoría de Karinthy era correcta y se aplicaba al medio *on-line*². Aunque las redes sociales comenzaron antes –en 1998 comenzó *SixDegrees* y en el 2002 *Friendster*–, la mayoría de éstas se crean y afianzan a partir del año 2003³. Las redes sociales pueden ser generalistas –Myspace, Facebook o la española Tuenti–, que tienen como objetivo facilitar las relaciones personales y de ocio entre los usuarios que las componen, o de profesionales –LinkedIn–, que quieren fomentar las relaciones entre profesionales, siendo un punto de encuentro entre los miembros de un sector⁴.

La red social es esencialmente una aplicación on-line que permite a los usuarios generar un perfil con sus datos en páginas personales y compartirlo con otras personas, haciendo pública esta información, lo que facilita la interrelación con otros usuarios a partir de los perfiles publicados. Es una herramienta que favorece las relaciones sociales –de ahí la expresión red social–.

98 Muchas redes sociales ofrecen un formulario, animando a completar el mayor número de datos posibles: nombre, edad, domicilio, teléfono, área de residencia, sexo y foto; pero también la formación académica, profesión, aficiones, gustos musicales o cinematográficos, orientación sexual, etc. Al inscribirse, la red social le anima a invitar a las personas con las que ya tiene una relación, incorporando así la lista de contactos del correo electrónico.

2.- Cfr. D. WATTS, *Six Degrees: the Science of a Connected Age*, W.W. Norton & Company, 2003 –también autor de *Small Worlds: The Dynamics of Networks between Order and Randomness*, Princeton University Press, 1999. Cfr. también M. BUCHANAN, *Nexus: Small Worlds and the Groundbreaking Theory of Networks*, Norton, W. W. & Company, Inc., 2003; S. N. DOROGVTSEV y J. F. F. MENDES, *Evolution of Networks: from biological networks to the Internet and WWW*, Oxford University Press, 2003; J. H. FOWLER, “Turnout in a Small World,” en A. ZUCKERMAN (coord), *Social Logic of Politics*, Temple University Press, 2005, págs. 269-287. Cfr. el Informe del Instituto Nacional de Tecnologías de la Comunicación -INTECO- “Redes sociales, menores de edad y privacidad en la red”, elaborado por el Área Jurídica del Observatorio de la Seguridad de la Información y accesible en su web -www.inteco.es-; más recientemente el *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales on line*, 2009, realizado por INTECO y la AEPD.

3.- Cfr. D. BOYD y N. ELLINSON, “Social Networks Sites: Definition History and Scholarship”, *Journal of Computer Mediated Communication*, 13(1), article 11. <http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html>

4.- Classmates.com es una red social para contactar con excompañeros del colegio. Facebook nació para los estudiantes universitarios americanos pero es utilizada actualmente como una red social general. Una primera información sobre la extensión de las redes sociales puede verse en el informe “Social Networking Goes Global” elaborado por la Compañía Comscore y publicado el 31 de julio de 2007 -www.comscore.com-.

Normalmente, cuando los invitados reciben un mensaje de adhesión, es necesaria la confirmación para poder añadirse a la lista de contactos del usuario. Por tanto, al principio, los contactos están compuestos por aquellas personas con las que se dispone ya de una relación off-line, fortaleciendo los vínculos existentes.

Sin embargo, las redes sociales tienen pocas restricciones preestablecidas, con la finalidad de fomentar un libre acceso a los perfiles que amplíe progresivamente el número de contactos de cada usuario. Inicialmente, no tiene nada de especial que los usuarios accedan a los perfiles de las personas que forman parte de su lista de contactos pero, además, la red social establece por defecto la accesibilidad del perfil no sólo para los amigos sino también para los amigos de los amigos –las personas que forman parte de la lista de contactos de los amigos–, permitiendo conocer así a otros usuarios desconocidos. Además, las redes sociales facilitan al usuario no sólo buscar sino ser buscado por otras personas, de manera que puede agregarlas a su grupo de conocidos, dando la posibilidad también a éstos de conocer a personas con las que se ha entrado en contacto. Las redes sociales permiten generar grupos de interés en virtud de los datos personales contenidos en los perfiles de los usuarios. Así, las redes sociales facilitan agruparse por ubicaciones geográficas, aficiones, formación académica, etc. En definitiva, se aprovecha la red social para contactar con personas que ya se conocen pero, también, para ampliar el círculo de contactos, iniciando lazos con otras desconocidas.

99

En algunas ocasiones, los perfiles pueden salir de la red social. Así, hay algunas que permiten la indexación por motores de búsqueda de contenidos de sus integrantes. De hecho, Internet no habría llegado a ser lo que es sin la existencia de esos buscadores, unos sistemas informáticos programados para rastrear la Red y facilitar búsquedas con palabras clave. Además, la red social proporciona todas estas relaciones sociales a través de herramientas de chat, mensajería instantánea, inclusión de vídeos y fotos, que pueden ser etiquetadas por distintas personas, etc. Existe un sistema de notificación dirigido a las cuentas de correo electrónico con cualquier novedad, tanto en el perfil propio como en el de las personas de las listas de contactos. De esta forma, estas redes permiten que sus usuarios estén constantemente compartiendo aficiones, fotografías, vivencias personales, de forma que han llegado a sustituir al correo electrónico y a la televisión⁵.

5.- En muchas ocasiones, los jóvenes dejan de ver la televisión porque les aburre –les parece algo estático– y prefieren la red social que les permite estar en contacto con mucha gente y saber qué pasa, por ejemplo, con las fotos que van colgando. Así, las redes sociales se han convertido para los jóvenes en un sustituto de la televisión. Desde este planteamiento, hay que reconocer que una persona está más aislada frente a un televisor que delante de un ordenador. Cfr. el reportaje de *El País*, 21-12, 2008, “El tam-tam de los nativos digitales”.

La Comisión Europea ha señalado que en el 2012 serán 120 millones los europeos que tengan un espacio en Internet. Las redes sociales tienen ya más de 270 millones de usuarios en todo el mundo. Los estudios más recientes señalan que algo más de nueve de cada diez jóvenes dicen haber participado o accedido a una de esas redes on-line, y ocho de cada diez jóvenes afirman tener su propio perfil en alguna de estas comunidades digitales⁶. Ante esta realidad, como ocurre en muchas facetas de la vida, las posiciones frentistas tienen la batalla perdida.

Es imprescindible no dar una imagen negativa de las nuevas tecnologías, que sería contradictorio con el esfuerzo de los poderes públicos en fomentar su accesibilidad. Los aspectos negativos, que también están presentes, no deben esconder las oportunidades y ventajas. Internet es, sobre todo, un instrumento de libertad y de civilización. Las redes sociales favorecen la participación de los ciudadanos, un valor procedimental necesario para el principio democrático y para el mantenimiento de una sociedad abierta⁷. Lo que aportan realmente las redes sociales es la posibilidad de asociarse con otros en los procesos de participación, a diferencia de lo que ofrecen los espacios institucionales de participación electrónica o los propios medios de comunicación digitales, donde se puede ejercer la libertad de expresión pero no formar grupos⁸. Así, las redes sociales han descubierto una manera inédita de hacer política, que no se limita a que los candidatos creen un perfil personal sino que abre la posibilidad de tener una malla de colaboradores y pedirles

100

6.- Cfr. el *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales on line*, de INTECO y la AEPD, ya citado. El Informe de la Fundación Pfizer sobre la “Juventud y las Redes Sociales en Internet”, de septiembre de 2009, señala que un 92 por ciento de los jóvenes españoles entre 11 y 20 años son usuarios de redes sociales.

7.- Las redes sociales han favorecido la configuración de grupos de oposición política como el movimiento del 15M o de los Indignados y han permitido o canalizado el posicionamiento crítico de los ciudadanos ante la Corona –incidente del Rey en Bostwana; negocios del marido de la Infanta Cristina, Iñaki de Urdangarín, renovación de su contrato con Telefónica, etc.–, situaciones que antes se podían haber silenciado con el control de dos o tres medios de comunicación. Véase en esta dirección a ELY, que justifica el activismo procedimental –la preferencia de los valores procedimentales sobre los sustantivos– y representa una justificación dogmática de la jurisprudencia Warren. Cfr. J. H. ELY, *Democracy and distrust. A Theory of Judicial Review*, Harvard University Press, Massachussets, 1980.

8.- Las redes sociales no son en sí mismas un instrumento de transparencia administrativa, aunque puedan coadyuvar a ella. Sobre las ventajas que ofrece la administración electrónica para la transparencia administrativa, cfr. EL trabajo “*Transparencia administrativa y protección de datos personales*”, en A. TRONCOSO REIGADA (Dir.), *Transparencia administrativa y protección de datos personales*, Civitas-APDCM, 2008, págs. 23-188, esp. 23-40. Sobre los problemas que plantea la democracia electrónica, cfr. A. SÁNCHEZ NAVARRO, “*Sistema electoral y nuevas tecnologías: oportunidades y riesgos para la legitimación democrática del poder*” Nuevas Políticas Públicas. *Anuario multidisciplinar para la modernización de las Administraciones Públicas*, núm. 1, 2005, págs. 83-109 y en el trabajo “*La Administración electrónica y la protección de datos personales*”, en J. L. PIÑAR MAÑAS (Dir.), *Administración electrónica y ciudadanos*, Civitas-Thomson Reuters, 2011, págs. 171-288, esp. págs. 96-97.

que hablen por ti, lo que facilita la participación política, especialmente a los jóvenes⁹.

Internet es también un espacio de libertad de expresión, que favorece la existencia de una opinión pública libre e informada en tiempo real –con imágenes y vídeos–, especialmente cuando están cerrados los canales tradicionales de información, como hemos visto recientemente en Irán o en los procesos revolucionarios de los países árabes¹⁰. Las redes sociales, al igual que los foros o los blogs, son canales que permiten expresar opiniones y son un lugar de participación, entretenimiento y búsqueda de información. Es, por tanto, un espacio de libertad. Además, el hombre es un ser social, necesita sentirse parte de un grupo donde poder compartir ideas y vivencias personales¹¹. La existencia de una comunidad virtual de grupos de amigos –y, por tanto, con el máximo grado de privacidad– donde se comparten experiencias y fotografías, es, en sí mismo, algo positivo. Las redes sociales, como Tuenti, Facebook o Myspace, responden también a estas necesidades de comunicación y socialización¹², y pueden evitar situaciones de exclusión

9.– No se trata de que el candidato tenga un perfil en una red social para pedir el voto y después no lo actualice ni conteste a los correos. Se trata de tener una red de colaboradores, como ha hecho Obama en las elecciones presidenciales americanas de 2008 y Patxi Lopez en las elecciones vascas de 2009.

10.– El candidato a la Presidencia de Irán en el año 2009, Hossein Mousavi, empleó las redes sociales –Facebook, Myspace– y creó una red social –Green Path of Hope– para convocar manifestaciones y ofrecer la información y las imágenes que omitían los canales estatales. Se evidenció, de esta manera, lo que ya se suponía: que Internet y las redes sociales son un poderoso instrumento de participación –de oposición política–, de libertad de expresión y de información, en ámbitos geográficos donde estos derechos no existen o están muy limitados. Recientemente, la cumbre del G-8 dedicada a Internet, celebrada en la ciudad francesa de Deauville, de mayo de 2011 resaltó la importancia de Internet para la libertad de expresión, algo clave en las revoluciones de Túnez y Egipto. En todo caso, también señaló la necesidad de establecer un marco jurídico eficaz para asegurarse de que Internet prospere sobre la base del respeto a la privacidad, a la propiedad y a los derechos de las personas. En el discurso inaugural, Sarkozy señaló: “Internet no es un universo paralelo, liberado del imperio de la ley, sin moral y sin los principios fundamentales que gobiernan la vida social en los países democráticos”. Así, “si bien la población árabe ha mostrado que Internet no pertenece a los Estados, sin embargo, en esta tercera mundialización de la historia no puede marginarse a los Estados democráticos. Olvidar que son los representantes legítimos de la voluntad popular sería apostar por un riesgo claro, el caos democrático, la anarquía”. El Presidente francés recalcó que, si la tecnología es neutra, no lo son sus usos y que no debe permitirse que la revolución digital pueda atentar contra los derechos elementales. Detrás está el debate de fondo sobre el papel regulador –principal o subsidiario– de los Gobiernos en Internet.

11.– Como señala Ratzinger, el hombre no puede ser privado de su dimensión relacional, que es parte de él mismo y que necesita para llegar a ser él mismo. Cfr. J. RATZINGER, *La sal de la tierra*, Ed. Palabra, Madrid, 5º ed. 2005, pág. 178.

12.– Las redes sociales son por definición instrumentos de comunicación personalizada y no anónima. Así, hay redes, como Tuenti, a la que se accede por invitación. No obstante, también el anonimato que ofrece en ocasiones Internet ayuda a perder la timidez y facilita el inicio de relaciones sociales.

social, aunque también pueden crear otras¹³. Por ello, aislar a un hijo de las redes sociales, prohibírselas, es, posiblemente, condenarle al desarraigo. El acceso a Internet es un derecho fundamental de la persona, lo que no quiere decir que no esté sometido a límites, que requiere una regulación legal y un control judicial, sin perjuicio de la posible intervención en este ámbito de autoridades administrativas independientes.

2. LAS REDES SOCIALES: UN CAMBIO DE PARADIGMA EN LA PRIVACIDAD PERSONAL

Las redes sociales no sólo tienen beneficios sino también riesgos. Por ello, son aplicables a éstas las distintas Recomendaciones elaboradas por diferentes instituciones en relación al uso de Internet por menores¹⁴, en las que, por ejemplo, se hace hincapié en la necesidad de controlar el tiempo –especialmente en el caso de los más jóvenes– que pasan frente al ordenador o utilizando la telefonía móvil, ya que cualquier herramienta debe ser empleada con moderación para que no se convierta en un obstáculo a las propias relaciones familiares y sociales y, en definitiva, para que no sea una adicción¹⁵. Otro problema de las redes sociales es el respeto a los derechos de propiedad intelectual¹⁶.

102

-
- 13.- La diferencia entre la pobreza y la exclusión social está en que en la primera permanecen elementos de socialización.
- 14.- Cfr. los Manuales recientemente editados por la CLI dentro del Proyecto Prometeo, que ha contado con la colaboración de las distintas Agencias de Protección de Datos –Española y Autonómicas– o las *Recomendaciones-Derechos de niños y niñas y deberes de los padres y madres*, de la Agencia Española de Protección de Datos, accesible en su web. Hay que destacar también la web www.chaval.es, llevada a cabo por Red.es, que trata de concienciar a los jóvenes en el uso de Internet. Recientemente, el Parlamento Europeo ha aprobado un programa comunitario para reforzar la protección de los niños en Internet, a través de la reducción de los contenidos ilícitos. Esta iniciativa, a propuesta de la Comisión Europea, se desarrolla entre 2009 y 2013 con un presupuesto de 55 millones de euros y da prioridad a las redes sociales y a las comunicaciones por medio de teléfonos móviles –elmundo.es, 23 de octubre de 2008–. Hay que mencionar también el proyecto “Dadus”, de la Comisión Portuguesa de Protección de Datos Personales –cfr. *Dataprotectionreview*, num. 7, octubre 2008–.
- 15.- Si bien, las tecnologías de la información pueden mejorar las relaciones entre personas que, por razones de espacio o de tiempo, no pueden verse presencialmente, no hay que olvidar que en muchas ocasiones las nuevas tecnologías –en especial el uso de redes sociales– fomentan la conexión entre gente desconocida. Sin embargo, las relaciones personales no pueden sostenerse únicamente sobre conexiones virtuales con gente que no se conoce verdaderamente. Además, la red social tiende a agitar relaciones pasadas o imaginarias, olvidando el afecto que se debe al prójimo, que es el próximo que está presente, consecuencia también de un deber de justicia. Preferir la compañía de desconocidos a través del ordenador a la de los amigos o a la de los familiares debe ser ya preocupante. Puede afirmarse que alguien está enganchado al ordenador cuando esto le impide hacer otras cosas que se deberían hacer. Por tanto, es necesario limitar el tiempo que se pasa en Internet, no siendo bueno que los menores dispongan de un ordenador en la habitación –aunque esta recomendación ha perdido parcialmente su sentido desde que el acceso a Internet se realiza en dispositivos portátiles o teléfonos–.
- 16.- Algunas redes sociales han establecido en sus condiciones generales de uso la cesión obligatoria de los derechos de propiedad intelectual sobre los contenidos generados por el usuario en esta plataforma.

Hay que ser conscientes también de que en Internet hay mucha información falsa. Los profesores y los padres, en la era de Internet, si bien no son los poseedores de todos los datos –que puede encontrarse en la red–, sí son guías que pueden ayudar a distinguir la información veraz de la que no lo es. Además, Internet, si bien facilita mucho la búsqueda de la información y ahorra tiempo, tiende a favorecer la mera reproducción de textos –una actividad que se limite a cortar y a pegar–. Por tanto, Internet también facilita la pérdida de la capacidad de análisis y de reflexión cuando deriva en una compulsiva actividad de acumulación de textos.

Son muchas las amenazas que provienen de las propias herramientas técnicas. Los virus –programas informáticos que pueden destruir o sustraer información del ordenador– se propagan con mucha facilidad, lo que exige la utilización de antivirus y cortafuegos. Así, por ejemplo, es posible activar una cámara web de un ordenador a través de un virus informático –de un troyano– y grabar a personas en situaciones comprometidas. También son muchas las molestias que generan los *pops-ups* o ventanas emergentes, que llevan a páginas que no se desea visitar mientras el usuario intenta cerrarlas, y que aconsejan utilizar la herramienta de bloqueo de elementos emergentes. No obstante, en las campañas desarrolladas con los jóvenes en los centros educativos es conveniente centrarse, fundamentalmente, en los riesgos que las nuevas tecnologías de la información y la comunicación presentan a la privacidad de las personas. El ordenador lo guarda todo –las páginas web visitadas, la músicas o las películas descargadas, las búsquedas hechas en Google o Yahoo, las conversaciones en programas de mensajería instantánea, las contraseñas–. Es importante, por ello, eliminar periódicamente historiales –donde están las páginas web visitadas–, las *cookies* –archivos con la dirección de las páginas visitadas–, los archivos –las imágenes y contenidos de las páginas web visitadas– y las contraseñas automáticas, especialmente en lugares de acceso público a Internet, como cibercafés.

103

Al mismo tiempo, las redes sociales, basadas en que los usuarios comparten información a veces muy sensible, suponen un reto a la privacidad personal e implican un cambio de paradigma¹⁷. De hecho, nuevas realidades como las redes sociales, unido a otras como la biometría, el Radio Frequency IDentification (RFID), el Internet de las Cosas o la computación en nube, suponen tales amenazas a la privacidad que ha llegado a afirmarse que

17.- Cfr. J. L. PIÑAR MAÑAS y P. LUCAS MURILLO DE LA CUEVA, *El derecho a la autodeterminación informativa*, Fundación Coloquio Jurídico Europeo, Madrid, 2009; P. LUCAS MURILLO DE LA CUEVA, *El derecho a la autodeterminación informativa*, Tecnos, Madrid, 1990; e *Informática y Protección de Datos Personales*, CEC, Madrid, 1993; M. CARRILLO, *El derecho a no ser molestado. Información y vida privada*, Aranzadi, Navarra, 2003; A. TRONCOSO REIGADA (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas, Cizur Menor, 2010.

hay que resignarse a no tener privacidad –*you already have zero privacy. Get over it*– o si se consigue esa privacidad es porque alguien tolera que el usuario disponga de ella¹⁸. De hecho, el propio concepto de red social conlleva una cierta renuncia de los usuarios a su privacidad¹⁹. Las personas ponen en común aficiones, gustos y vivencias con la finalidad de facilitar el acceso a esta información por una red de contactos que incluye una mayoría de personas a las cuales no conocen.

Las redes sociales son grandes fuentes de información no sólo sobre sus miembros sino sobre las personas que éstas conocen, o han contactado alguna vez, y suponen tratamientos masivos de datos personales, lo que representa un riesgo para la privacidad de la personas²⁰. La información publicada por un usuario en su página personal no sólo permite fácilmente establecer un perfil personal sino que incluye, en muchas ocasiones, datos sobre vida sexual, ideología, religión, que son datos de especial protección. Toda esta información señala pautas de consumo y permite personalizar la publicidad –el principal objetivo de muchas bases de datos privadas–, pudiéndose comercializar a su vez esta información²¹. Además, los perfiles de las redes sociales pueden

18.- La afirmación –del año 1999– es del Presidente y co-fundador de *Sun Microsystems*, Scott McNealy y se encuentra en el comienzo del interesante trabajo de J. L. PIÑAR MAÑAS, “¿Existe privacidad?”, en *Protección de datos personales*, Alonso Editores, México, 2010.

19.- La privacidad y la intimidad es un requisito necesario, como ha señalado el Tribunal Constitucional español, para tener una mínima calidad de vida. Carecer de privacidad –que toda la información personal sea pública– afecta a la propia identidad y a la libertad, ya que la actuación tiende a ajustarse a unas pautas previas esperadas. En otro momento se han diferenciado los círculos de intimidad y privacidad. Cfr. “Transparencia administrativa y protección de datos personales”, cit. págs. 75-86.

20.- Esta es una cuestión sobre la que se ha pronunciado la 30ª Conferencia Internacional de Privacidad, celebrada en Estrasburgo en octubre de 2008, que aprobó la Resolución sobre Protección de la Privacidad en las Redes Sociales. Cfr. también el Memorándum de Roma, del Grupo de Trabajo internacional de Berlín sobre protección de datos en las telecomunicaciones, de marzo de 2008. http://www.privacyconference2008.org/adopted_resolutions/STRASBOURG2008/resolution_social_networks_en.pdf Cfr. especialmente el Dictamen 5/2009 del Grupo de Trabajo sobre Protección de Datos del art. 29, sobre las redes sociales en línea, de 12 de junio de 2009 –http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm La Agencia Europea de Seguridad de las Redes y de la Información –ENISA– ha elaborado una lista de riesgos potenciales del uso de las redes sociales: “*Security Issues and Recommendations for Online Social Networks*”, octubre 2007, disponible en www.enisa.europa.eu. Esta preocupación también se ha trasladado a los medios de comunicación. Cfr. por ejemplo “¿Sabe Facebook demasiado sobre sus usuarios?”, *El País.com*, 3-11-2008.

21.- Aunque los usuarios de redes sociales utilicen un seudónimo, existe por parte de las redes sociales un tratamiento de las direcciones IP, que han sido consideradas hasta ahora un dato de carácter personal. De hecho, la dirección IP es utilizada frecuentemente por los prestadores de servicios de estas redes sociales para segmentar la publicidad que se dirige a los distintos tipos de usuarios registrados. Cfr. C. VELA SÁNCHEZ-MERLO, “La privacidad de los datos en las redes sociales”, *Revista Española de Protección de Datos* núm. 5, 2008, págs. 246-247. La dirección

ser archivados, facilitando la creación de bases de datos de personas con fines ilícitos²². A ello se une los problemas que plantea la protección de los datos personales en un mundo globalizado e interconectado, donde usuarios y proveedores de servicios se encuentran frecuentemente en países y continentes distintos y donde no existen unos estándares internacionales en este ámbito. Todo ello obliga a repensar y a reforzar la normativa europea de protección de datos personales, como hace la propuesta de Reglamento General de Protección de Datos Personales que ha presentado la Comisión el 25 de enero de 2012, para que contemple y regule estas nuevas realidades que, si bien aportan principalmente oportunidades y ventajas, también conllevan la aparición de nuevos riesgos²³. La Comisión ha justificado la

IP como dato de carácter personal ha sido ya analizado tempranamente en el trabajo “La Administración electrónica”, cit., págs. 67–68. Recientemente, la propuesta de Reglamento General de Protección de Datos que ha presentado la Comisión, precisa el concepto de dato personal como toda información relativa a un interesado y define interesado como toda persona física identificada, directa o indirecta, por medios que puedan ser utilizados razonablemente por el responsable o por cualquier otra persona física o jurídica, añadiendo elementos que no estaban en la Directiva 95/46/CE, pero que ya habían sido expresamente admitidos por el Grupo de trabajo del Artículo 29 como la dirección IP o el identificador en línea. El TJUE ha señalado que el derecho a la protección de los datos personales y el derecho a la vida privada –arts. 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea– se aplica a toda información sobre una persona física identificada o identificable –Sentencia, de 9.11.2010, as. *Völker und Markus Schecke y Eifert*, apdo. 52. El considerando 26 de la Directiva 95/46/CE y el Considerando 23 y el art. 4.1) de la propuesta de Reglamento señalan que, para determinar si una persona es identificable, deben tenerse en cuenta todos los medios que razonablemente pudiera utilizar el responsable del tratamiento o cualquier otro individuo para identificar a dicha persona, en el sentido de lo expresado en el Dictamen 4/2007 del Grupo de Trabajo del Artículo 29 sobre el concepto de datos personales http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_es.pdf Así, en relación con los identificadores en línea, el Considerando 24 de la propuesta de Reglamento señala: “cuando utilizan servicios en línea, las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como las direcciones de los protocolos de internet o los identificadores de sesión almacenados en *cookies*. Ello puede dejar huellas que, combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas e identificarlas. De ello se deduce que los números de identificación, los datos de localización, los identificadores en línea u otros factores específicos *no necesariamente tienen que ser considerados datos de carácter personal en toda circunstancia*”. Entendemos, como se ha señalado en otro momento, las *cookies*, con independencia de la información almacenada en las mismas, pueden vincularse con el usuario de un determinado dispositivo conectado a Internet y permite obtener el perfil del mismo. Si bien la dirección IP no siempre es estática, sino que puede ser dinámica, además de que no identifica a un usuario sino un equipo –que puede ser de utilización compartida, por ejemplo en puntos de acceso público a Internet o en un cibercafé– en muchas ocasiones es una “información concerniente a personas físicas identificadas o identificables”.

- 22.– Como señala el Dictamen 5/2009 del Grupo de Trabajo del Art. 29 –ya citado–, las redes sociales “generan la mayoría de sus ingresos con la publicidad que se difunde en las páginas web que los usuarios crean y a las que acceden. Los usuarios que publican en sus perfiles mucha información sobre sus intereses, ofrecen un mercado depurado a los publicitarios que desean difundir publicidad específica y basada en esta información”.
- 23.– Esta cuestión la hemos abordado en “Hacia un nuevo marco jurídico europeo de protección de datos personales”, en *Revista Española de Derecho Europeo*, núm. 43, 2012.

aprobación de un Reglamento en la necesidad de disponer de un nuevo marco jurídico coherente y homogéneo de protección de datos en todo el territorio de la Unión Europea, que reduzca o suprima las diferencias en el nivel de protección de datos personales entre los Estados miembros²⁴. De hecho, esta situación afecta especialmente a las empresas multinacionales, como las que prestan servicios de redes sociales que operan a nivel europeo y que tienen que cumplir diferentes obligaciones en los Estados miembros, lo que impide desarrollar políticas paneuropeas sobre protección de datos y falsea la competencia –no existe tampoco una supervisión coherente y sanciones equivalentes en todo el territorio de la Unión–²⁵.

Son tres los aspectos que deben abordarse cuando se analiza la protección de los datos personales en las redes sociales: la legislación aplicable, las posibilidades que brinda la autorregulación y la importancia de la concienciación de los usuarios.

3. EL MARCO JURÍDICO

- a) *El responsable del tratamiento en el servicio de red social, la delimitación de las actividades personales o domésticas y el problema de aplicación de la Directiva 95/46/CE. La regulación de la propuesta de Reglamento general de protección de datos personales de las Corporaciones que tienen su sede fuera de la Unión Europea.*

La Normativa de protección de datos personales, a diferencia de la relativa al derecho a la intimidad, reconoce al ciudadano unos principios y derechos de protección de datos, estableciendo al mismo tiempo un conjunto de obligaciones al responsable del tratamiento, de forma que permite al titular de los datos el control sobre su propia información personal sometida a tratamiento, también dentro de las redes sociales. No obstante, la propia naturaleza de Internet –y de estas redes sociales– que facilita las relaciones con personas de ámbitos geográficos muy alejados plantea algunos interrogantes a la hora de determinar la aplicación de la Directiva 95/46/CE –art. 4– y de

24.– Las divergencias entre las legislaciones de los Estados miembros supone un impedimento a la libre circulación de los datos de carácter personal en la Unión y, por tanto, significan un obstáculo para el ejercicio de las actividades económicas y para la realización del mercado interior. El Reglamento es, pues, el instrumento jurídico adecuado para lograr una mayor armonización y seguridad jurídica, estableciendo un modelo uniforme que sirva para superar la fragmentación jurídica que se derivan de las distintas aplicaciones nacionales de la Directiva, y permita las transferencias de datos personales a través de las fronteras interiores y el desarrollo de la economía digital en la Unión Europea.

25.– Basta comparar las diferencias en el ámbito de la supervisión entre la empresa española Tuenti y otras redes sociales.

la LOPD -art. 2.1-, teniendo en cuenta, además, que algunas redes sociales tienen su sede fuera de la Unión Europea²⁶.

Los titulares de los servicios de redes sociales son responsables del tratamiento de datos personales y, si están establecidos en algún Estado miembro de la Unión Europea o utilizan medios de tratamiento ubicados en la misma, deben cumplir la normativa europea -española si están establecidos en ese país- sobre protección de datos personales. Así, la Directiva 95/46/CE señala en el art. 4 que serán de aplicación las disposiciones nacionales que traspongan la Directiva a todo tratamiento de datos cuando el responsable no esté establecido en la Unión Europea pero recurra, para el tratamiento de datos personales, a medios situados en el territorio de dicho Estado, salvo que tales medios se utilicen únicamente con fines de tránsito. Las redes sociales emplean medios ubicados dentro de la Unión Europea, no sólo por la utilización de *cookies* o *banners*, sino porque la recogida de datos se produce en parte dentro de la Unión Europea²⁷. Los proveedores del servicio de red social son responsables del tratamiento de datos porque han decidido la finalidad, contenido y uso del tratamiento -art. 3.d) LOPD-. Como ha señalado el Grupo de Trabajo del Artículo 29 en el Dictamen 5/2009, éstos: “proporcionan los medios que permiten tratar los datos de los usuarios, así como todos los servicios «básicos» vinculados a la gestión de los usuarios (por ejemplo, el registro y la supresión de cuentas). Los proveedores de servicios de red social -SRS- determinan también la manera en que los datos de los usuarios pueden utilizarse con fines publicitarios o comerciales, incluida la publicidad proporcionada por terceros. Los proveedores de aplicaciones también pueden ser responsables del tratamiento de datos, si desarrollan aplicaciones que funcionan además de las de los SRS y que los usuarios deciden utilizar”.

107

26.- Hay redes sociales como Facebook que están adheridas al puerto seguro lo que significa que han asumido los principios y derechos de protección de datos personales presentes en la Directiva 95/46/CE.

27.- Ésta es la interpretación que a nuestro juicio debe darse al “Documento de trabajo relativo a la aplicación internacional de la legislación comunitaria sobre protección de datos al tratamiento de los datos personales en Internet por sitios web establecido fuera de la UE”, del Grupo de Trabajo del Artículo 29, aprobado el 30 de mayo de 2002 -http://ec.europa.eu/justice_home/fsj/privacy-. El Grupo de Trabajo del Artículo 29, en el Dictamen 5/2009, señala que las disposiciones de la Directiva relativas a la protección de datos se aplican en la mayoría de los casos a los proveedores de servicios de redes sociales, aunque su sede se encuentre fuera de la Unión Europea. El Grupo de Trabajo del artículo 29 remite a su dictamen previo sobre los motores de búsqueda, con el fin de obtener información complementaria sobre las cuestiones del establecimiento y la utilización de equipo, como determinantes para la aplicabilidad de la Directiva relativa a la protección de datos y de las normas derivadas del tratamiento de las direcciones IP y la utilización de *cookies*.

La propuesta de Reglamento General de Protección de Datos Personales, que ha presentado recientemente la Comisión Europea, contiene una interesante regulación de su ámbito de aplicación territorial, con la finalidad de tratar de resolver la problemática de jurisdicción y de ley aplicable que plantean las corporaciones internacionales que no tienen su sede en la Unión Europea, pero que ofrecen en el territorio de la Unión servicios de tratamiento de datos, como los servicios de redes sociales virtuales –u otros como los motores de búsqueda o los servicios de computación en nube–, y que había dado lugar, recientemente, a una cuestión prejudicial planteada por la Audiencia Nacional²⁸. Hay que destacar que la propuesta de Reglamento no esgrime para el ámbito de aplicación territorial el criterio –presente en el art. 4.1.c) de la Directiva 95/46/CE– relativo al empleo de medios técnicos en los Estados de la Unión –que el responsable que tiene su sede fuera de la Unión Europea recurra para el tratamiento de datos personales a medios, automatizados o no, situados en los Estados de la Unión–, sino que emplea “un factor de conexión más específico”, que tiene en cuenta la necesaria “orientación hacia las personas”. Para ello, se establece que el Reglamento

28.- El Auto de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, de 2 de marzo de 2012, planteó una cuestión prejudicial –también en relación al derecho al olvido en Internet–, en el marco de las Resoluciones de tutela de derechos que la AEPD ha dictado frente a Google. Así, se pregunta si debe interpretarse que existe un establecimiento cuando la empresa proveedora del motor de búsqueda crea en un Estado Miembro una oficina o filial destinada a la promoción y venta de los espacios publicitarios del buscador, que dirige su actividad a los habitantes de ese Estado, o cuando la empresa matriz designa a una filial ubicada en ese Estado miembro como su representante y responsable del tratamiento de dos ficheros concretos, que guardan relación con los datos de los clientes que contrataron publicidad con dicha empresa o cuando la oficina o filial establecida en un Estado miembro traslada a la empresa matriz, radicada fuera de la Unión Europea, las solicitudes y requerimientos que le dirigen, tanto los afectados como las autoridades competentes en relación con el respeto al derecho de protección de datos, aun cuando dicha colaboración se realice de forma voluntaria [aquí debería producirse una respuesta afirmativa a la luz del art. 3.2 de la propuesta de Reglamento]. También se pregunta si debe interpretarse el art. 4.1.c de la Directiva 95/46/CE en el sentido de que existe un “recurso a medios situados en el territorio de dicho Estado miembro” cuando un buscador utilice arañas o robots para localizar e indexar la información contenida en páginas web ubicadas en servidores de ese Estado miembro, o cuando utilice un nombre de dominio propio de un Estado miembro y dirija las búsquedas y los resultados en función del idioma de ese Estado miembro [ambas respuestas serían afirmativas a la luz de los Dictámenes 5/2009 y 8/2010, del Grupo del Art. 29]. También se pregunta si puede considerarse como un recurso a medios, en los términos del art. 4.1.c de la Directiva 95/46/CE, el almacenamiento temporal de la información indexada por los buscadores en internet [existe una responsabilidad del buscador sobre sus propios tratamientos, como hemos señalado en “Transparencia administrativa”, cit., págs. 101-112] y si puede entenderse que este criterio de conexión concurre cuando la empresa se niega a revelar el lugar donde almacena estos índices alegando razones competitivas. Por último, en el caso de que el TJUE señale que no concurren los criterios de conexión previstos en el art. 4 de la Directiva, se pregunta si debe aplicarse la Directiva 95/46/CE en materia de protección de datos, a la luz del art. 8 de la Carta Europea de Derechos Fundamentales, en el país miembro donde se localice el centro de gravedad del conflicto y sea posible una tutela más eficaz de los derechos de los ciudadanos de la Unión Europea.

se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable no establecido en la misma, cuando las actividades de tratamiento estén relacionadas con la oferta de bienes o servicios a dichos interesados en la Unión y con el control de su conducta –art. 3.2–, siguiendo en este punto el Dictamen 8/2010, del Grupo de Trabajo del Artículo 29²⁹. Esta ampliación de la zona de aplicación territorial se complementa con la obligación de los responsables del tratamiento no establecidos en la Unión, de designar un representante en la misma, que actúe en lugar del responsable, al que puede dirigirse cualquier autoridad de control en lo que respecta al cumplimiento de sus obligaciones, y que debe estar establecido en uno de los Estados miembros en que residan los interesados, cuyos datos personales son objeto de tratamiento en el contexto de una oferta de bienes o servicios o cuyo comportamiento esté siendo controlado –arts. 4.14 y 25–³⁰.

La propuesta de Reglamento de la Comisión mejora la posición jurídica y las garantías de los ciudadanos europeos, teniendo en cuenta la naturaleza global de Internet, basado en plataformas digitales que no se circunscriben a un solo territorio. De esta forma, se trata de poner fin a una práctica frecuente de las Corporaciones internacionales, que alegan reiteradamente que no les es de aplicación el derecho europeo, negando con ello a sus usuarios europeos algunos derechos que la normativa les garantiza y, además, obligando a los ciudadanos de esa zona a solicitar la tutela de sus derechos ante Cortes internacionales, principalmente la estadounidense, lo que genera una indudable indefensión. La propuesta de Reglamento –al igual que anteriormente lo hacía la Directiva y los Dictámenes del Grupo de Trabajo del Art. 29– obliga a los proveedores de servicios en Internet, como las redes sociales, a someterse a la legislación europea de protección de datos personales, de forma que se pueda garantizar de manera efectiva los derechos de los ciudadanos europeos frente a las prácticas de estas empresas, sometiéndolas, además, a las competencias de control de las autoridades administrativas de

29.– Cfr. Dictamen 8/2010 sobre Derecho Aplicable elaborado por el Grupo de Trabajo de la Unión Europea del Artículo 29, que está accesible en http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_es.pdf

30.– No es aplicable la obligación de designar representante cuando el responsable esté establecido en un país con nivel adecuado de protección, cuando sea una empresa con menos de doscientos cincuenta trabajadores o un organismo público, o cuando el responsable ofrezca sólo ocasionalmente bienes o servicios a interesados residentes de la Unión. El carácter ocasional se desprende de analizar las actividades generales del responsable para determinar si la oferta de bienes y servicios a los interesados es accesorio a las actividades principales –Considerando 64–. En todo caso, hay que recordar que la Directiva 95/46/CE ya preveía que cuando el responsable no estuviera establecido en el territorio de la Unión Europea y utilice en el tratamiento medios situados en un país de la Unión Europea, deberá designar un representante en ese país –art. 4.2–, lo que no siempre se cumplía.

protección de datos de los Estados de la Unión y de sus órganos jurisdiccionales –y no, por ejemplo, a los de Estados Unidos–³¹.

Los usuarios de redes sociales tienen la consideración de afectados o interesados al ser las personas titulares de los datos que son objeto de tratamiento –art. 3.e) LOPD–³². Los usuarios de redes sociales incluyen en sus páginas personales

31.- Recientemente Google ha presentado una nueva política de privacidad, en la que prevé crear un perfil de datos del usuario utilizando todas las aplicaciones derivadas del buscador como redes sociales o programas de localización geográfica. La Comisaria Europea de Justicia, Viviane Reding, ha pedido a Google que deje en suspenso las nuevas normas de privacidad anunciadas, porque no cumplen la legislación europea de protección de datos, recordando, en línea con la propuesta de Reglamento, que las compañías internacionales que ofrecen sus servicios a los consumidores de la Unión Europea deben respetar las normas europeas de protección de datos. También las autoridades de control de privacidad de Asia-Pacífico –en concreto su Grupo de Trabajo Tecnológico TWG–, han remitido un escrito a Google en el que manifiestan su preocupación por sus cambios en la política de privacidad y, en concreto, si se podrá combinar información suministrada por usuarios registrados en un servicio (como Gmail, YouTube o el motor de búsqueda de Google) con información de otros servicios, señalando también la falta de plazos para la eliminación de la información cuando ha sido solicitada por el interesado.

32.- La protección de los datos personales de los usuarios fallecidos –un problema que surge habitualmente en el ámbito de las redes sociales– ha sido analizado extensamente en otro momento. El art. 2.a) de la Directiva definía dato de carácter personal como toda información sobre una persona física identificada o identificable, sin aclarar si protegía o no la información relativa a fallecidos, algo que tampoco resuelve la propuesta de Reglamento de la Comisión Europea. Hasta ahora, la mayoría de las Leyes se aplican únicamente a las personas naturales o físicas, excluyendo expresamente a los fallecidos –*natural living persons or living individuals*. En España el Reglamento de Protección de Datos Personales establece que no será de aplicación a los datos referidos a personas fallecidas, sin perjuicio de que las personas vinculadas a éste puedan dirigirse a los responsables de los ficheros que contengan datos de éste con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo y solicitar en su caso, la cancelación de los datos –art. 2.4–. En la misma dirección, la Ley 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, prevé las personas que pueden ejercer las acciones de protección del derecho a la intimidad de la persona fallecida y solicitar la cancelación de su perfil personal –la persona designada en testamento a tal efecto, los familiares directos o el Ministerio fiscal –arts. 4 y 5–.

Ha existido una evolución en la posición de las redes sociales sobre el mantenimiento de la publicación del perfil personal de una persona tras su muerte. Algunas redes sociales, desde un planteamiento patrimonialista de la propiedad intelectual de lo publicado en su plataforma, continuaban con la publicación del perfil personal de los fallecidos, lo mismo que ocurriría con los blogs escritos para ser difundidos y leídos por Internet y que siguen publicados en la Red. Inicialmente, Facebook se negaba a cerrar los perfiles en Internet de las personas fallecidas –esto ocurrió con el perfil del periodista William Bemister, a pesar de las reclamaciones de su hermana–. Esta es una cuestión que en España se planteó con la continuidad de la publicación de los datos y conversaciones privadas de Marta del Castillo obtenidas de la red social Tuenti. En ese caso, Tuenti cerró, a petición de la Fiscalía, su perfil y el de alguno de los adolescentes relacionados con el suceso. En la actualidad, las redes sociales cuentan con un protocolo relativo a los datos de personas fallecidas. Facebook establece en su política de privacidad el mantenimiento de las páginas del perfil de los fallecidos “de forma especial y conmemorativa durante un periodo de tiempo determinado, eliminando cierta información sensible” y permitiendo el acceso a la página sólo a los amigos, que ya estaban confirmados por el usuario en el momento de su muerte. Al mismo tiempo, Facebook ofrece también a

datos de otras personas. En la mayoría de los casos, son tratamientos que se encuentran excluidos del régimen de protección de datos personales al ser considerados “ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas” –art. 2.2.a) LOPD, una excepción también prevista en el art. 3.2 de la Directiva 95/46/CE– que va destinada a los datos personales que afecten a la esfera familiar y de amistad, y que cubre aquellos tratamientos que no pretendan otra finalidad que las relaciones propias de estos ámbitos³³. La propuesta del Reglamento General de Protección de Datos también excluye de su ámbito de aplicación material los tratamientos de datos personales que lleve a cabo una persona física en el ejercicio de sus actividades, exclusivamente personales o domésticas, precisando con acierto: “siempre que no tengan un interés lucrativo” –art. 2.2.d)–³⁴. Esta cuestión tiene particular interés en el ámbito de las redes sociales, donde, si bien la mayoría de los tratamientos que llevan a cabo los usuarios afectan a la esfera familiar y de amistad –y se encuentran excluidos, por tanto, del ámbito material de aplicación de la Normativa–, hay otros tratamientos desarrollados por los usuarios en los servicios de redes sociales que no pueden ser considerados de carácter “personal o doméstico” y que, por tanto, no se encuentran excluidas de la Normativa de protección de datos³⁵. Esto ocurriría, por ejemplo, cuando los usuarios utilizan

los familiares cercanos la solicitud para cerrar completamente la cuenta del fallecido. Igualmente, Tuenti ofrece a los familiares y personas vinculadas a éste la posibilidad de notificar el fallecimiento de un usuario y solicitar la cancelación del perfil, con los requisitos de acreditación del fallecimiento y de la relación directa. El cierre de la cuenta supone el borrado automático de todos los datos, imágenes y cualquier tipo de información que apareciera del usuario. Por último, hay que señalar que existen redes sociales para fallecidos como Lifstrand, una especie de cementerio virtual con el fin de expresar las condolencias a los familiares, rendirles un homenaje y compartir recuerdos –fotos y vídeos–, tratando de eternizar su recuerdo a través de Internet. Incluso hay empresas que han desarrollado una aplicación para que, tras el fallecimiento, se publique un mensaje que se grabó con anterioridad.

111

- 33.– La Audiencia Nacional, en su Sentencia de 15 de junio de 2006, ha establecido que se consideren ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas los datos que “afecten a la esfera más íntima de la persona, a sus relaciones familiares y de amistad y que la finalidad del tratamiento no sea otra que surtir efectos en estos ámbitos”.
- 34.– El Considerando 15 de la Propuesta, pone como ejemplo de tratamientos personales o domésticos la correspondencia y la llevanza de un repertorio de direcciones, sin ningún interés lucrativo y, por tanto, sin conexión alguna con una actividad profesional o comercial. Sin embargo, precisa que esta exención no debe aplicarse a los responsables o encargados del tratamiento que proporcionen los medios para tratar los datos personales relacionados con tales actividades personales o domésticas.
- 35.– El Dictamen 5/2009 del Grupo de Trabajo del Artículo 29 precisa en qué circunstancias las actividades de un usuario de servicios de redes sociales no están cubiertas por la «exención doméstica». Una preocupación de este Grupo de Trabajo es la difusión y utilización de la información disponible en los servicios de redes sociales con fines secundarios, no buscados. Así, el Dictamen 5/2009, señala que una tendencia creciente que se evidencia en los servicios de redes sociales es el paso de la Web 2.0 para el ocio a la Web 2.0 para la productividad y los servicios.

el servicio de red social como una plataforma de colaboración con una empresa para una finalidad comercial³⁶ o como un medio para desarrollar un objetivo de carácter político o social, que no son finalidades personales o domésticas³⁷. Igualmente, un número muy elevado de contactos por parte de un usuario implica que no conoce a muchos de ellos –consecuencia de una aceptación indiscriminada de peticiones de amistad sin que exista una relación personal–, por lo que no puede hablarse de datos que afecten a la esfera familiar y de amistad o de tratamientos personales o domésticos. Tampoco puede hablarse de un tratamiento “personal o doméstico” cuando el perfil y los contactos personales se encuentran abiertos para todos los usuarios de la red social, o cuando la información personal puede ser indexada a través de motores de búsqueda fuera de la propia red. En estos supuestos, el usuario debe ser considerado responsable de un tratamiento, aplicándole el mismo régimen que en la publicación de datos personales en otras plataformas tecnológicas de manera abierta en Internet. Así, el Tribunal de Justicia de la Unión Europea ha señalado en la Sentencia Lindqvist, que los tratamientos de datos personales que consistan en la publicación de datos de manera que éstos sean accesibles para una pluralidad de personas, aunque sean personales o domésticos y no tengan un interés lucrativo, estarían dentro del ámbito material de aplicación de la normativa de protección de datos³⁸. De hecho,

36.- Así, muchas redes sociales especializadas son básicamente redes de profesionales, como LinkedIn –que quiere favorecer las relaciones entre profesionales– o Ryze.com –que hace conexiones de empresas para resolver sus necesidades–. Hay que tener en cuenta que la normativa española no protege los datos de personas jurídicas ni los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquellas –cuando constan únicamente nombre y apellidos, funciones o puestos desempeñados, dirección postal o electrónica, teléfono y número de fax profesionales–, ni los ficheros con datos relativos a empresarios individuales, cuando se haga referencia a ellos en su calidad de comerciantes, industriales o navieros –art. 2 del Reglamento de desarrollo de la LOPD–. Así, la información de relaciones profesionales no forma parte nuclear de la privacidad de las personas. En ese sentido, las redes generalistas tienen un mayor nivel de riesgo, ya que no sólo ofrecen información profesional sino también, vivencias o aficiones. No obstante, no están excluidos de la LOPD los tratamientos de datos personales de potenciales clientes. MySpace, si bien es una red generalista, dispone de un grupo formado por artistas que la aprovechan para dar a conocer sus trabajos ante el público en general.

37.- El hecho de que no se aplique al usuario la excepción de los tratamientos con fines personales o domésticos, no significa que no sean de aplicación otras excepciones a los principios y derechos de protección de datos, como son las destinadas a aquellos tratamientos que suponen el ejercicio de otros derechos fundamentales, como la libertad de información y de expresión, que en todo caso se encuentran limitados por el derecho a la intimidad, como ha establecido el art. 9 de la Directiva 95/46/CE y los arts. 21.1.f) y 80 de la propuesta de Reglamento General de Protección de Datos personales. Cfr. sobre esta cuestión la “Introducción y Presentación” a *An Approach to Data Protection in Europe*, Thomson-Civitas, APDCM, 2007, págs. 26-33.

38.- Cfr. la STJUE, de 6 de noviembre de 2003, As. Lindqvist, sobre la catequista sueca que publicó datos personales en Internet. Cfr. E. PÉREZ LUÑO, *La tercera generación de derechos humanos*, Thomson-Aranzadi, Cizur Menor, 2006, págs. 110-114; M. C. GUERRERO PICÓ, *El impacto de Internet en el derecho fundamental a la protección de datos de carácter personal*, Civitas,

la interpretación limitada del concepto de tratamiento personal o doméstico es una consecuencia del principio *pro libertate*, que obliga a una interpretación restrictiva de los límites a un derecho fundamental, especialmente cuando afecta al contenido esencial del derecho y a los intereses jurídicos que le dan vida. Así, excluir estos tratamientos del derecho fundamental a la protección de datos personales afectaría a los intereses jurídicos que dan vida a este derecho –especialmente de terceras personas–, dejándolos sin protección –STC 11/1981–.

Este planteamiento es una exigencia del respeto a los derechos de las personas en las redes sociales. Así, no tendría sentido que no pueda aplicarse la Normativa de protección de datos personales –y, por tanto, no esté vigente el derecho fundamental a la protección de la información personal–, a tratamientos que suponen una cesión indiscriminada de datos –incluso sensibles– de terceras personas a un número muy amplio de usuarios de una red social, a todos los usuarios de la misma sin restricciones de acceso o al público en general –a través de motores de búsqueda–. Esta publicación de datos personales debe suponer que el usuario de la red social asume la responsabilidad del tratamiento –en relación con las personas cuyos datos y fotografías aparecen publicadas en su perfil–, lo que le obliga, en especial, al cumplimiento de los principios de información y consentimiento y al respeto a los derechos de los afectados que establece la Ley Orgánica de Protección de Datos (LOPD), así como a la notificación del tratamiento a la Agencia Española. De hecho, el usuario es responsable no sólo ante la Agencia de Protección de Datos sino también tanto, en el orden jurisdiccional civil como en el penal, por las vulneraciones de los derechos de las personas que se deriven de la información incorporada por éste a la red social.

113

- b) *La información y el consentimiento del interesado para el tratamiento y para las cesiones a la luz de la propuesta de Reglamento General de Protección de Datos personales, el establecimiento de niveles de acceso y la inclusión de datos de otras personas en el propio perfil.*

Cizur Menor, 2006, págs. 356–361. También hemos señalado que la realización de fotografías de grupos de menores en centros educativos por parte de los padres puede considerarse un tratamiento personal o doméstico, pero su publicación en Internet en abierto supone un tratamiento que sale de la esfera personal y se constituye en una cesión indiscriminada de datos personales. La Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, señala que la protección de estos derechos “quedará delimitada por las leyes y por los usos sociales atendiendo al ámbito que, por sus propios actos, mantenga cada persona reservado para sí misma o su familia”. Cfr. nuestra “Introducción y Presentación” a *Protección de datos personales para centros educativos públicos*, Civitas-APDCM, Madrid, 2008, pág. 55.

El art. 6 de la propuesta de Reglamento mantiene las condiciones de licitud de los tratamientos presentes en el art. 7 de la Directiva, especificándolos más en profundidad³⁹. En especial, la propuesta fija las condiciones para que el consentimiento sea válido como fundamento jurídico del tratamiento lícito. El cambio más relevante se encuentra en el Capítulo I –“Disposiciones Generales”–, y más concretamente en las definiciones, donde desaparece la legitimidad del consentimiento tácito. El consentimiento es para la propuesta de Reglamento toda manifestación de voluntad no sólo libre, específica, informada sino también explícita, “mediante la que el interesado acepta, ya sea mediante una declaración, ya sea mediante una clara acción afirmativa, el tratamiento de datos personales que le conciernen”. Se trata, como señala la Exposición de Motivos, de: “dotarse de una definición única y coherente que garantice que el interesado es consciente de que da su consentimiento y a qué lo da”⁴⁰. Por tanto, el consentimiento explícito para el tratamiento de datos personales será plenamente de aplicación a los servicios de redes sociales. Posiblemente, la mejora de las tecnologías de la comunicación ha facilitado la posibilidad de exigir el consentimiento explícito, algo que en el pasado podía ralentizar la relación jurídica en Internet. Se establecen ahora algunos rasgos nuevos en relación con el consentimiento, que ya estaban señalados por la doctrina y la jurisprudencia: que la carga de la prueba del consentimiento la tiene el responsable del tratamiento, que el consentimiento para el tratamiento debe ser distinguido de cualquier otra dación de consentimiento para otro asunto, y que el consentimiento no es una base jurídica válida cuando existe un desequilibrio entre el interesado y el responsable del tratamiento. Como señala la Exposición de Motivos de la propuesta de Reglamento, a juicio de la Comisión, era necesaria una interpretación clara y uniforme del consentimiento válido en toda la Unión Europea, que dé seguridad jurídica a los agentes económicos.

Por tanto, la recogida de datos personales por el proveedor del servicio de red social, así como las posibles cesiones tienen que hacerse mediante el consentimiento libre, inequívoco, específico, e informado del interesado –art. 3.h) LOPD–, así como explícito. Debe ser el usuario el que dé

39.- Así, los tratamientos de datos personales se consideran legítimos si existe consentimiento, relación contractual, obligación jurídica del Derecho de la Unión o de la legislación del Estado, cumplimiento de una misión de interés público o inherente al ejercicio de poder público y satisfacción del interés legítimo del responsable.

40.- De esta forma, la propuesta de Reglamento es más garantista que la Carta de Derechos fundamentales de la Unión Europea, que señala que el consentimiento ha de prestarse de forma inequívoca –art. 8–. Esto estaba en línea con la Directiva que consideraba únicamente como rasgos esenciales del consentimiento que fuera libre, específico e informado –art. 2.h)–, al que la LOPD añadía también que fuera inequívoco –art. 3.h)–. En cambio, el consentimiento expreso o explícito se requería únicamente para el tratamiento de categorías especiales de datos –art. 8.2.a) de la Directiva y art. 7 LOPD–.

su consentimiento, estableciendo el nivel de acceso a su perfil personal –a sus amigos, a los amigos de sus amigos, a toda la red social o fuera de ella, permitiendo la indexación por motores de búsqueda–. Este consentimiento se ejerce habitualmente aceptando la política de privacidad establecida por defecto⁴¹. El interesado, de esta forma, consiente el tratamiento de sus datos personales por el servicio de red social. Sin embargo, el usuario no consiente los tratamientos de sus datos que se llevan a cabo en las páginas personales de otros usuarios. El beneplácito es un derecho del usuario y una obligación del responsable de la red social como responsable del tratamiento; por tanto, no es una obligación legal del usuario, salvo que también sea responsable del tratamiento en los términos antes señalados⁴², o salvo que la información revelada por el usuario afecte al derecho a la intimidad, honor y propia imagen de otras personas, superando los usos admitidos socialmente –art. 2.1 de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen–. Hay que recordar de nuevo la distinción existente entre el proveedor del servicio de red social, que es el responsable del tratamiento, y el usuario, ya que las cesiones que haga éste último en un ámbito restringido pudieran entenderse como un tratamiento para fines personales, familiares o domésticos, que están excluidos de la Directiva 95/46/CE y de la LOPD⁴³. Un modelo ideal sería

-
- 41.– Existen distintas medidas que pueden implantar los servicios de redes sociales para limitar las injerencias en la privacidad de las personas. Así, la 30ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad de Estrasburgo del año 2008 estableció que los servicios de red social deben tomar medidas eficaces para impedir el *spidering* y/ o las descargas en masa de datos de perfil por parte de terceros.
- 42.– La publicación excesiva de información de terceros –fotos– sin consentimiento de éstos ha sido sancionado por la Agencia Española (Procedimiento Sancionador 000117/2008).
- 43.– Los usuarios de redes sociales tratan en muchas ocasiones datos de personas que no son miembros de la red social y que no han dado su consentimiento. Lo esencial es que el propio servicio de red social, como responsable del tratamiento, no lleve a cabo un tratamiento de estos datos personales –por ejemplo, no cree perfiles de no miembros prerrellenados ni invite a no miembros a adherirse a la red–. Éste es el sentido que hay que darle a este apartado del Dictamen 5/2009 del Grupo de Trabajo del Artículo 29: “Muchos servicios de redes sociales permiten a los usuarios proporcionar datos sobre otras personas, como añadir un nombre a una imagen, evaluar a una persona, o poner una lista de «gente que he conocido/quiero conocer» en acontecimientos. Esta información puede identificar también a no miembros. Sin embargo, el tratamiento de este tipo de datos relativos a no miembros por el SRS sólo puede realizarse si se cumple uno de los criterios contemplados en el artículo 7 de la Directiva relativa a la protección de datos. Además, la creación de perfiles de no miembros prerrellenados mediante la agregación de datos proporcionados independientemente por usuarios de SRS, incluidos los datos afines deducidos de las listas de contactos en línea, no tiene ninguna base jurídica. Incluso, aunque el SRS tuviese los medios para ponerse en contacto con el no usuario e informarle de la existencia de datos personales relativos a él, una posible invitación por correo electrónico para adherirse al servicio de red social con el fin de acceder a estos datos personales violaría la prohibición prevista en el artículo 13, apartado 4, de la Directiva sobre la privacidad y las comunicaciones electrónicas, relativa al envío de mensajes electrónicos no solicitados con fines de comercialización directa”.

que los usuarios no cedieran datos de otras personas –por ejemplo, imágenes de grupo– sin su consentimiento. A este criterio tienen que ir encaminados todos los códigos de buenas prácticas y la concienciación de los usuarios. Sin embargo, muchas redes sociales permiten el tratamiento de datos de otras personas –por ejemplo, la fotografía o su etiquetado– sin este consentimiento. Hay que ser conscientes de que no siempre es fácil solicitar y obtener el consentimiento de todas las personas que aparecen en una fotografía. La publicación por parte de los usuarios de redes sociales de datos personales de terceros sin su consentimiento –por ejemplo, fotografías–, aunque sea entre amigos y para un círculo restringido, es una cuestión compleja desde el punto de vista del derecho a la intimidad y a la imagen. Parece razonable que la publicación para un número limitado de amigos y, por tanto, con el máximo grado de privacidad –y no para amigos de amigos, toda la red social y todo Internet–, pueda considerarse un uso admitido socialmente, formando parte en este caso de un tratamiento familiar o doméstico, lo que significa que no se considera una intromisión ilegítima que deba ser perseguida –por otra parte, no sería posible hacerlo– y siempre que la información publicada no afecte a la intimidad de una persona. No obstante, la existencia de una oposición del interesado debería bastar para la supresión de esta información de esta comunidad restringida siendo importante, por ello, que las redes sociales tengan canales de denuncia que lo permitan⁴⁴.

116

El usuario de los servicios de red social que no lleva a cabo tratamientos personales o domésticos –bien porque desarrolla una actividad comercial, empresarial o profesional a través de la red social, bien porque mantiene un número muy elevado de contactos, bien porque establece su perfil personal con datos de otras personas abierto a todos los usuarios de la red social o indexable a través de buscadores fuera de la red social–, es el responsable del tratamiento de los datos de otras personas publicados en su perfil, y está obligado por ello a cumplir los principios y derechos de protección de datos, en especial, el principio de consentimiento.

44.- El Dictamen 5/2009 plantea la implementación de herramientas que mejoren el consentimiento entre los usuarios miembros de la red social. Se habla así de la “introducción de herramientas de gestión de etiquetas de la información en los sitios de redes sociales, en particular, creando espacios en un perfil personal para indicar la presencia de un nombre de usuario en imágenes o vídeos con etiqueta que estén a la espera del consentimiento del usuario en cuestión, o fijando plazos de expiración para las etiquetas que no hayan recibido el consentimiento de la persona señalada”. Así, por ejemplo, Tuenti ofrece a sus usuarios en las “condiciones de uso” mecanismos técnicos para el borrado de una foto, para quitar una “etiqueta” que marca una fotografía identificando a un usuario y para su denuncia. Además, informa que los usuarios no están autorizados a subir imágenes sin haber obtenido el oportuno consentimiento de las personas que en ellas pudieran aparecer. Esta es una cuestión que he tenido la oportunidad de debatir en múltiples foros –Fundación Pfizer, Colegio de Abogados de Madrid, Universidad Politécnica– con el Director de Comunicación de Tuenti Ícaro Moyano, al que agradezco las aclaraciones sobre el funcionamiento de su red social.

Se han analizado las excepciones a algunos principios de protección de datos, especialmente el consentimiento, en los tratamientos de los datos personales efectuados exclusivamente con fines periodísticos o de expresión literario o artística, algo frecuente en el ámbito de las redes sociales, y la necesidad de conciliar el derecho a la protección de los datos personales con la libertad de expresión, una previsión que se encuentra en los arts. 80 y 21.1.f) de la propuesta de Reglamento y en el art. 9 de la Directiva⁴⁵. Además, el art. 7.f) de la Directiva 95/46/CE –que se mantiene en el art. 6.1.f) de la propuesta de Reglamento– permite el tratamiento de datos personales sin consentimiento del interesado cuando concurren dos requisitos acumulativos:

- Que sea necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos
- Que no prevalezcan los derechos y libertades fundamentales del interesado, lo que exige una ponderación que dependerá de las circunstancias concretas en cada caso

Este precepto tiene efecto directo, como ha recordado recientemente el Tribunal de Justicia de la Unión Europea, en la Sentencia de 24 de noviembre de 2011⁴⁶. El tratamiento de datos de otras personas sin consentimiento previsto en el art. 7.f) de la Directiva, podría encontrar su justificación en la satisfacción de un interés legítimo si el número de contactos es reducido o el acceso al perfil personal está restringido –un usuario que lleva a cabo un tratamiento personal o doméstico y no de un responsable de tratamiento–. Sin embargo, cuando el usuario se convierte en responsable del tratamiento por tener un muy elevado número de contactos personales o un perfil abierto, el tratamiento de datos de otras personas sin su consentimiento en su perfil personal difícilmente podría justificarse en la satisfacción de un interés legítimo de éste, y no superaría el *balance test* que obliga a llevar a cabo una ponderación, valorando la posible prevalencia de los derechos y libertades

117

45.– Esta cuestión se ha abordado en “Hacia un nuevo marco jurídico europeo de protección de datos personales”, cit.

46.– Esta Sentencia ha resuelto una cuestión prejudicial presentada por el Tribunal Supremo de España, a través de la Resolución de 15 de julio de 2010, poniendo en evidencia el incumplimiento de nuestro país en la transposición de la Directiva 95/46/CE, lo que ha llevado al Tribunal Supremo, en su reciente Sentencia de 8 de febrero de 2012, a anular el art. 10.2.b) del RPD. Cfr. más ampliamente “Hacia un nuevo marco jurídico europeo de la protección de datos personales”, cit. El Tribunal de Justicia ha recordado que el art. 7.f) es una disposición suficientemente precisa y establece una obligación incondicional, por lo que concurren los requisitos de la jurisprudencia –STJCE *Simmenthal*, 1978– para atribuirle un efecto directo, de forma que puede ser invocado directamente por un particular y aplicado por los órganos jurisdiccionales nacionales, aunque no exista transposición.

de los interesados. La resolución del equilibrio de intereses que prevé el art. 7.f) de la Directiva, puede justificar la ausencia del consentimiento del interesado para los tratamientos de datos personales o la cesión de datos a un concreto cesionario en la actividad económica o de prospección comercial –especialmente, cuando esos datos consten en fuentes accesibles al público, como señalaba la legislación española, porque implica una menor gravedad de la injerencia, sin perjuicio de no poder excluir los tratamientos sin consentimiento de otros datos que no figuren en fuentes accesibles al público-. Sin embargo, la inclusión de datos de otras personas en un perfil personal con un número muy elevado de contactos o abierto a todos los usuarios de red social sin restricciones de acceso o al público en general a través de motores de búsqueda, implica una publicación de datos personales que, en muchas ocasiones, no permite identificar al cesionario y, por tanto, supone una cesión indiscriminada de datos –incluso sensibles– donde el interesado pierde el control de su información personal.

118 Los proveedores de redes sociales no pueden tratar datos de ideología, religión o creencias de los usuarios sin el consentimiento expreso y escrito de éstos y con expresa advertencia del derecho a no prestarlo –arts. 7.1 y 2 LOPD-. Los detalles de raza, salud o vida sexual de los usuarios no pueden ser objeto de tratamiento por el servicio de red social sin el consentimiento expreso del usuario –art. 7.3 LOPD-. Además, los formularios de inscripción en la red social deben señalar, expresamente, que esta información es voluntaria.

La LOPD prohíbe expresamente los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico o vida sexual –art. 7.4-, lo que debe ser tenido en cuenta por las empresas proveedoras de estos servicios a la hora de favorecer la organización de grupos. Se está hablando, de nuevo, de las obligaciones del responsable del tratamiento y, por tanto, de los derechos del usuario. Lógicamente, estos criterios son de aplicación a la persona que es, al mismo tiempo responsable, del tratamiento –en los supuestos antes señalados-, de forma que éste, por ejemplo, no puede publicar datos sensibles de otras personas en abierto en Internet sin los mismos requisitos de consentimiento antes señalados. Si bien, la legislación de protección de datos personales no se aplica a los tratamientos personales, familiares o doméstico, la obligación que tiene toda persona –no sólo el responsable del tratamiento– de respetar el derecho a la intimidad de los demás y las eventuales responsabilidades penales o civiles al margen del derecho fundamental a la protección de datos personales que pueden derivarse de su incumplimiento, obligan a los usuarios a ser especialmente cautos, respetando en este caso el principio de consentimiento. Así, hay que recordar que los datos de ideología, afiliación sindical, religión o creencias, raza, salud o vida

sexual afectan a la esfera más íntima de una persona, por lo que su revelación en una red social –aunque sea a un círculo restringido que no hagan del usuario un responsable del tratamiento– puede suponer igualmente la vulneración del derecho a la intimidad de la persona. Por tanto, si como criterio general un usuario no debería revelar información de otras personas sin su consentimiento, esto dispone de un especial refrendo normativo cuando hablamos de datos especialmente protegidos. En todo caso, hay que recordar que una excepción a la prohibición de tratamiento de categorías especiales de datos es que el interesado los haya hecho manifiestamente públicos –art. 9.2.e) de la propuesta de Reglamento, que también se encuentra en el art. 8.2.e) de la Directiva 95/46/CE–.

La mayoría de las redes sociales anima a los usuarios a que inviten a sumarse a la red social a sus contactos personales. Así, en el momento de la inscripción, los éstos son invitados a enviar un correo electrónico a sus contactos en su agenda de direcciones electrónicas. La Directiva 2002/58/CE, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, exige, como regla general, el consentimiento del interesado para la recepción de comunicaciones comerciales no solicitadas. Si bien existe una invitación por parte de la red social que es la responsable del tratamiento, estamos hablando en este caso de una comunicación personal por lo que no es de aplicación la prohibición de utilizar el correo electrónico con fines de comercialización directa, siempre que se cumplan una serie de requisitos⁴⁷. En todo caso, la inclusión de estos contactos sólo puede hacerse con su consentimiento.

119

Igualmente, las redes sociales tienen un servicio de notificación de novedades en el propio perfil o en el de sus contactos cuando, por ejemplo, alguien ha agregado su perfil a la lista de contactos de otra persona, se le invita a participar en un grupo o alguien ha etiquetado su foto. La incorporación a este servicio de notificación debe hacerse también con el consentimiento del interesado.

Es especialmente importante el cumplimiento del principio de información –art. 5 LOPD⁴⁸–, de forma que el titular de los datos debe ser previamente informado:

47.- Para que estas invitaciones que hacen los usuarios cumplan la excepción de las comunicaciones personales, el Dictamen 5/2009 del Grupo de Trabajo del Artículo 29 señala que el servicio de red social debe cumplir los siguientes criterios: no incentivar al remitente ni al destinatario; el proveedor no debe seleccionar a los destinatarios; la identidad del remitente debe mencionarse claramente; y el remitente debe conocer todo el contenido del mensaje que se enviará en su nombre.

48.- Estas exigencias son aplicables para las redes sociales sometidas a la LOPD ya que las obligaciones de información de la Directiva son más flexibles.

1º- De la existencia de un fichero y de un tratamiento con sus datos personales –hay que informar, por tanto, de la recogida de *cookies*–.

- Todas las finalidades del tratamiento –debe informarse si los datos de los perfiles van a ser empleados con fines distintos a la participación en la red, como, por ejemplo, para fines publicitarios o de marketing–
- De los cesionarios o destinatarios de la información debe informarse de los niveles de acceso y de las categorías, qué tipo de datos van a ser cedidos y la finalidad, si se va a hacer publicidad de los distintos perfiles, si la información puede ser indexada por cualquier buscador o si se prevén transferencias a países no miembros de la Unión Europea que no ofrecen el mismo nivel de protección⁴⁹

2º- Del carácter obligatorio o facultativo de la respuesta –las redes sociales incentivan a través de impresos la incorporación del mayor número de datos posibles, pero no informan de qué casillas son necesarias para la incorporación a la red social y cuáles son opcionales–.

120 3º- De las consecuencias de la obtención de los datos y de la negativa a suministrarlos.

4º- De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

5º- De la identidad y dirección postal y electrónica del responsable del fichero y del servicio para el ejercicio de los derechos antes señalados –es muy importante que los proveedores de servicios de redes sociales informen a los usuarios de su identidad–⁵⁰.

Es necesario que se lea y se acepte expresamente la política de privacidad antes de la publicación del perfil con datos personales en la red social.

49.- El Dictamen 5/2009 del Grupo de Trabajo del Artículo 29 incide en la importancia de que se informe de la utilización de los datos con fines de comercialización directa; de la posible distribución de datos a categorías específicas de terceros; de una reseña de los perfiles –su creación y sus principales fuentes de datos– y de la utilización de datos sensibles.

50.- Cfr. el documento del Grupo de Trabajo del Artículo 29 “Recomendación sobre determinados requisitos mínimos para la recogida en línea de datos personales en la Unión Europea”, aprobado el 17 de mayo de 2001. Este documento señala que la no mención de los destinatarios equivale al compromiso de no comunicar información personal. Cfr. también el documento del Grupo de Trabajo del Artículo 29: “Privacidad en Internet: enfoque comunitario integrado de la protección de datos en línea”, adoptado el 21 de noviembre de 2000.

Así, no debe ser posible la introducción de ningún dato sin que el afectado haya dado su consentimiento expreso, aceptando los términos y condiciones de la política de privacidad de la red social. Sin embargo, no todas las redes cumplen la normativa de protección de datos personales en este punto. La política de privacidad no está destacada suficientemente en las páginas de inicio y en las fases de registro⁵¹. No existe un conocimiento de quién posee los datos, para qué finalidad; tampoco se informa de los derechos del afectado ni se conoce de manera completa las posibles cesiones y el almacenamiento de *cookies*⁵². Existe una apariencia de consentimiento, pero el incumplimiento del principio de información implica que no existe un consentimiento informado⁵³.

La propuesta de Reglamento general de protección de datos personales introduce el principio de transparencia –que los datos serán tratados de manera transparente en relación con el interesado del art. 5.a)–, lo que tiene consecuencias para los servicios de redes sociales en relación con la información al interesado y con el derecho de acceso. Así, la información al interesado debe incluir no sólo los fines del tratamiento sino también el interés legítimo del responsable; debe contener, además, información sobre el plazo dentro del cual se conservarán los datos personales, la fuente de la que proceden los datos –esto ya estaba en la LOPD–, el derecho a presentar una reclamación ante la autoridad de control y, en su caso, la intención del responsable de efectuar una transferencia internacional y el nivel de protección del tercer país.

121

- c) *El principio de calidad en el servicio de red social, la conservación de la información y las medidas de seguridad.* Las obligaciones que la propuesta de Reglamento general de protección de datos personales fija al responsable del tratamiento: los *Privacy Impact Assessment* (PIA).

Las redes sociales deben cumplir el principio de calidad como principio de finalidad –art. 4 LOPD–. Éstas plantean riesgos potenciales de utilización de la información para otras finalidades –por ejemplo, para el *marketing* personalizado– lo que no puede hacerse sin la información y el consentimiento

51.– Muy pocas personas leen la política de privacidad –donde se señala la explotación de la información por intereses económicos–, especialmente los jóvenes. Hay que destacar que los *digital natives* son objeto de un interés específico por las compañías de publicidad.

52.– Cfr. el Informe de la Agencia Española de Protección de Datos sobre buscadores de Internet, de 1 de diciembre de 2007, accesible en la web de la Agencia.

53.– Algunos de los criterios relativos a la protección de datos personales en la Administración electrónica son también trasladables a las redes sociales. Cfr. nuestro trabajo “La Administración electrónica y la protección de datos personales”, cit.

del interesado. No siempre es fácil evitar los tratamientos de datos personales excesivos, sobre todo cuando el interesado es el que quiere y decide que aparezcan en su perfil personal. En todo caso, el servicio de red social no debe exigir ningún dato personal excesivo en la solicitud de inscripción en la red social, debiendo indicar claramente qué datos son obligatorios y cuáles facultativos.

La información en la red social frecuentemente no se encuentra actualizada -porque el usuario no lo hace-. Es importante que los datos personales sean cancelados cuando hayan dejado de ser necesarios, lo que impone un conjunto de obligaciones al proveedor del servicio en relación con la conservación de la información. El mantenimiento de las copias por un tiempo indeterminado no es aceptable⁵⁴. Como regla general, el responsable de la red social no puede conservar copias archivadas de los perfiles de los usuarios que han abandonado la red social para sus propias finalidades, y mucho menos por un tiempo indeterminado. Igualmente, la información suprimida por el usuario al actualizar su página personal no debe almacenar por el proveedor de servicio de red social para sus propios fines. En esta dirección, algunas exigencias incluidas en el Dictamen 5/2009 del Grupo de Trabajo del Artículo 29 que establecen límites a la conservación de la información por las redes sociales en supuestos de no utilización del servicio por el usuario van encaminadas a facilitar el control de la propia información personal⁵⁵. Por ello, los responsables de las redes sociales sólo están facultados para conservar esta información bloqueada durante el tiempo necesario para la persecución de infracciones penales o administrativas; más allá de este plazo, esos datos deben ser suprimidos.

Existen supuestos donde el responsable de la red social conserva alguna información de los usuarios que han abandonado la red social como instrumento de autorregulación. Así, el Dictamen 5/2009 antes citado señala que algunos servicios de red social conservan los datos de identificación de los usuarios suspendidos del servicio, con el fin de garantizar que ya no podrán

54.- El Grupo de Trabajo del Artículo 29, en su Dictamen 1/2008 sobre cuestiones de protección de datos relacionadas con motores de búsqueda, emitido el 4 de abril de 2008, señala que la retención de datos personales por éstos no debía superar los seis meses. Esta es una cuestión que hemos analizado en “Transparencia administrativa y protección de datos personales” cit. págs. 67-75.

55.- Así, se señala que cuando un usuario no utiliza el servicio durante un período determinado, el perfil debería desactivarse, dejando de ser visible para otros usuarios o para el exterior, y, después de otro periodo, los datos de la cuenta abandonada deberían suprimirse. En todo caso, los servicios de redes sociales antes de proceder a esta cancelación deben informar a los usuarios a través de los medios de que dispongan. Otro caso distinto es que los datos personales comunicados por un usuario cuando se registra en un servicio de red social deban suprimirse en cuanto el usuario o el proveedor de servicios de red social decidan suprimir la cuenta.

registrarse de nuevo, debiendo informarse al interesado de que se realiza este tratamiento. Para el Grupo de Trabajo del Artículo 29, la única información que puede conservarse es la de identificación, y no las razones por las que se suspendió a estas personas, y no deberá conservarse durante más de un año. Sin embargo, este planteamiento supone un límite a las facultades de autorregulación –que también pueden garantizar el derecho fundamental a la protección de datos personales–, además de no dejar de ser un supuesto de conservación de la información “para los fines para los que fueron recogidos” –art. 6.1 de la Directiva 95/46/CE– entre los que estaría la propia autorregulación. No parece razonable exigir unas obligaciones de mantener limpia la red social al proveedor del servicio al mismo tiempo que se dificulta la penalización de las conductas infractoras o su persecución en el futuro.

La regulación que la propuesta de Reglamento General de Protección de Datos personales hace de los principios relativos al tratamiento de datos personales y que se desarrolla en el Capítulo II –arts. 5-10– no aporta una especial novedad⁵⁶, tampoco en lo que respecta al principio de calidad y de finalidad. En todo caso, precisa el principio de prohibición de exceso –un principio de minimización de datos, en términos de la Comisión–, que obliga a: “los datos sean limitados al mínimo necesario en relación a los fines para los que se traten” y “sólo se tratarán si y siempre que estos fines no pudiesen alcanzarse mediante el tratamiento de información que no implique datos personales” en el art. 5.c)⁵⁷. De esta forma, los prestadores de servicios de internet como las redes sociales tienen la obligación de limitar la recogida de datos al mínimo necesario⁵⁸.

123

La propuesta de Reglamento sí fija un conjunto de obligaciones al responsable del tratamiento –Capítulo IV, arts. 22 al 37–, que no estaban en la Directiva 95/46/CE y que son aplicables a los servicios de red social, como la documentación del respeto a los principios y derechos en el tratamiento de datos personales⁵⁹; el cumplimiento de requisitos en materia de autoriza-

56.- De hecho, el considerando 7 de la Propuesta de Reglamento, recogiendo el parecer de las consultas previas a las partes interesadas, señala que los principios generales de la Directiva 95/46/CE “siguen siendo válidos y actuales”.

57.- El principio de calidad como principio de prohibición de exceso se ha analizado en “El principio de calidad de los datos”, A. TRONCOSO REIGADA (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, cit. págs. 344-360.

58.- De hecho, dentro de los principios se establece como novedad que el responsable del tratamiento no está obligado a obtener información adicional para identificar al interesado con la única finalidad de cumplir las disposiciones del Reglamento –art. 10–.

59.- Establece que el responsable del tratamiento de datos “para cada operación de tratamiento, garantizará y demostrará el cumplimiento de las disposiciones del presente Reglamento” –art. 5.f)–, lo que transforma las obligaciones del responsable del Capítulo IV en un principio general de responsabilidad.

ción o consultas previas con la autoridad de control o la realización de una auditoría independiente externa o interna de la observancia de la normativa y no limitada a las medidas de seguridad. La propuesta de Reglamento introduce como obligación del responsable la realización con carácter previo de una evaluación de impacto relativa a la protección de datos –los *Privacy Impact Assessment* (PIA)–, cuando los tratamientos entrañen riesgos específicos para los derechos y libertades de los interesados en razón de su naturaleza, alcance o fines –art. 33–, estableciéndose incluso en estos supuestos la necesidad de que el responsable o el encargado obtenga con carácter previo al tratamiento de estos datos una autorización o lleve a cabo una consulta a la autoridad de control –art. 34–.

124

La evaluación de impacto sería necesaria porque los servicios de red social llevan a cabo un tratamiento a gran escala de datos de aficiones, de datos especialmente protegidos –de vida sexual o de salud cuando los incluye el usuario–, de menores y suponen una evaluación indirecta de aspectos personales o de las preferencias personales de los usuarios, sin perjuicio de que los servicios de red social no vayan a tomar medidas que produzcan efectos jurídicos o le afecten significativamente⁶⁰. La propuesta de Reglamento incluye también la obligación de designar un delegado de protección de datos personales –Data Protection Officer–, con la función de velar por el cumplimiento de la normativa de protección de datos personales en el ámbito interno del responsable, cuando la actividad principal del responsable consista en operaciones de tratamiento que, en razón de su naturaleza, alcance o fines, requieran un seguimiento periódico y sistemático de los interesados –art. 35.1.c)–, algo que se aplica a las empresa que prestan servicios de red social.

La Directiva 95/46/CE dejaba un amplio margen de maniobra a los Estados a la hora de implementar la seguridad de los tratamientos de datos personales. La propuesta de Reglamento regula la seguridad entre las obligaciones del responsable y del encargado del tratamiento. Una de las novedades que presenta la regulación de la seguridad de los datos en la propuesta de Reglamento es la necesidad de realizar una evaluación de riesgos, que permita adoptar las medidas para proteger los datos contra su destrucción accidental o ilícita, pérdida accidental o cualquier tratamiento ilícito, como

60.- La Exposición de Motivos de la Propuesta de Reglamento, prevé que la evaluación de impacto abarque aplicaciones o plataformas comunes de tratamiento o cuando se plantee introducir una aplicación o un entorno de tratamiento común en un sector para una actividad horizontal de uso generalizado –Considerando 72–. Este informe de evaluación de impacto en la privacidad debe contener la descripción general del tratamiento, los riesgos para los derechos, las libertades de los interesados y las medidas contempladas para hacer frente a los riesgos, y para garantizar el cumplimiento de la normativa y el respeto de los derechos e intereses legítimos de las personas afectadas.

la comunicación, difusión, el acceso no autorizado o la alteración de los datos personales. Existe una preocupación específica, no sólo por impedir cualquier acceso no autorizado sino también por evitar cualquier forma no autorizada de comunicación, lectura o copia. Además, se establece la obligación de notificación de la violación de los datos personales a la autoridad de control y su comunicación al interesado –arts. 31-32–, más conocida por brechas de seguridad –las llamadas “BCR`s–”. La propuesta de Reglamento no incluye una referencia a niveles de seguridad ni tampoco un conjunto de medidas de seguridad a implementar sino que, al igual que el art. 9 LOPD que prevé su desarrollo reglamentario, y a diferencia de la Directiva, faculta a la Comisión para realizar los actos normativos necesarios para especificar las medidas técnicas y organizativas, lo que incluye la referencia a sectores específicos y situaciones de tratamiento de datos específicas –entre los que están, sin duda, los servicios de red social–, teniendo en cuenta no sólo la evolución de la tecnología, sino también las soluciones de privacidad desde el diseño y la protección de datos por defecto.

Hasta que entre en vigor la propuesta de Reglamento y su desarrollo normativo, las redes sociales tienen que implantar las medidas de seguridad establecidas en las legislaciones nacionales, en virtud de la tipología de datos personales sometidos a tratamiento, algo especialmente importante en España ya que desde el año 1999 la normativa obliga a establecer unas concretas medidas de seguridad –art. 9 LOPD, desarrollado primero por el Real Decreto 994/1999, de 11 de junio, ya derogado, y ahora por el Real Decreto 1720/2007, de 21 de diciembre–. Inicialmente, puede parecer que las redes sociales deben adoptar medidas de seguridad de nivel medio ya que son tratamientos que ofrecen un perfil de las personas y permiten evaluar aspectos de su personalidad. Sin embargo, es necesario implantar medidas de seguridad de nivel alto ya que, en muchas ocasiones, se tratan datos de origen racial, ideología, orientación sexual, lo que implicaría, entre otras cosas, la existencia de un registro de accesos y la encriptación de las comunicaciones. Hay que señalar que la voluntad del titular de los datos de compartir una determinada información con un círculo de personas, significa la determinación de excluir al resto de los miembros de la red social del conocimiento de esta información, lo que obliga a establecer herramientas que garanticen esta confidencialidad. Evitar los accesos indebidos a la información de los perfiles debe constituir una de las principales preocupaciones de las redes sociales. En todos los ámbitos de la sociedad de la información –comercio electrónico, administración electrónica, redes sociales virtuales–, la seguridad de la información es un elemento esencial para la confianza de los usuarios y para el desarrollo de la economía digital.

- d) *Los derechos de las personas y las vías de reclamación. El derecho al olvido en Internet y a la portabilidad de los datos en la propuesta de Reglamento General de Protección de Datos personales. La protección de los menores.*

126

El derecho de acceso permite al interesado conocer sus datos personales sometidos a tratamiento, el origen de los mismos y las comunicaciones realizadas o que se prevén hacer a terceras personas –art. 15 LOPD–. Igualmente, el interesado tiene derecho a rectificar sus datos si son inexactos o incompletos y a cancelarlos –art. 16 LOPD–. El titular de los datos también puede revocar el consentimiento para el tratamiento, así como ejercer el derecho de oposición –art. 6 LOPD–, notificándoselo al responsable. En especial, los responsables de los servicios de red social tienen que respetar el ejercicio del derecho de cancelación cuando los usuarios desean hacer desaparecer parte de la información que han publicado en su perfil personal, o darse de baja de la propia red social⁶¹, sin perjuicio de las obligaciones de bloqueo que tiene el responsable o de la necesidad de conservar determinada información a efectos de autorregulación. También, el responsable del servicio de red social tiene que respetar el derecho de oposición del usuario a determinados tratamientos de datos personales –por ejemplo, para finalidades comerciales, o cuando desea modificar el nivel de acceso a su perfil personal para restringirlo o para impedir la indexación por los buscadores–. Lógicamente, el ejercicio de estos derechos no se limita a los usuarios de la red social, sino también a todas las personas cuyos datos personales son sometidos a tratamiento, entre los que pueden estar personas que no son miembros de la red social. Los responsables de los servicios de red social deben facilitar el ejercicio de esos derechos, aunque no sea a través del procedimiento previsto expresamente por el responsable –incluso a través de los servicios de atención al público y de reclamaciones–, adoptando las medidas oportunas para que todas las personas de su organización informen al interesado del procedimiento a seguir para ejercer sus derechos –art. 24 del Reglamento de desarrollo de la LOPD–. Así, como señala el Dictamen 5/2009, del Grupo de Trabajo del Artículo 29: “como mínimo, en la página inicial de los SRS debería figurar un enlace hacia una oficina de reclamaciones, tanto para miembros como para no miembros, que cubra cuestiones de protección de datos”.

Lógicamente, el ejercicio de estos derechos de acceso, rectificación, cancelación y oposición se realiza ante el responsable del tratamiento, que serán

61.- El responsable del servicio de red social debe resolver la solicitud de cancelación y hacerla efectiva en un plazo máximo de diez días a contar desde la recepción de la misma. Transcurrido este plazo sin que se responda a la petición de manera expresa, ésta puede entenderse desestimada. En el caso de que el responsable no disponga de datos de carácter personal del afectado deberá igualmente comunicárselo en el mismo plazo –art. 32 del Reglamento de desarrollo de la LOPD–.

las empresas proveedoras del servicio de red social⁶², no ante el resto de usuarios de la red social, salvo que éstos tengan también el carácter de responsables del tratamiento. Sin embargo, en muchas ocasiones el interesado detecta el tratamiento de sus datos personales –por ejemplo, su fotografía– por parte de otros usuarios sin su consentimiento.

Las redes sociales tienen procedimientos de denuncia para oponerse al tratamiento de datos personales por parte de otras personas⁶³. Si bien estos tratamientos se encuentran excluidos del ámbito de aplicación de la LOPD al tratarse de ficheros personales o domésticos, los usuarios deben respetar en todo caso los derechos a la intimidad, al honor o a la propia imagen de otras personas. Comentarios de naturaleza injuriosa o calumniosa sobre la vida profesional, publicación de fotografías íntimas, creación de perfiles falsos, por poner sólo algunos ejemplos, pueden ser delitos o faltas tipificados en el Código Penal –arts. 205 y 208–⁶⁴ o dar lugar a una responsabilidad civil por vulneración del derecho al honor, a la intimidad personal y familiar y a la propia imagen, desarrollados en la Ley Orgánica 1/1982, de 5 de mayo. En todo caso, hay que señalar que los titulares de redes sociales tienen una gran dificultad técnica para llevar a cabo una cancelación efectiva de los datos personales. Así, si bien las redes permiten dar de baja el perfil o borrar parte de la información, sin embargo, los comentarios, mensajes cruzados o los etiquetados de fotografías persisten en los perfiles de los demás usuarios, por lo que la cancelación de datos personales es difícil de implementar.

127

El principio de transparencia que introduce la propuesta de Reglamento General de Protección de Datos personales –la obligación del responsable de ofrecer una información transparente y de fácil acceso y comprensión– tiene consecuencias en el ejercicio del derecho de acceso, también en el ámbito de las redes sociales. Cuando el interesado solicite el ejercicio del derecho de acceso, el responsable tendrá ahora que facilitar información sobre el plazo durante el cual se conservarán los datos personales –plazo para la supresión que también está sometido a una obligación de documentación en virtud del art. 28.2.g)– y el derecho a presentar una reclamación ante la autoridad de control. La propuesta de Reglamento también mejora el ejercicio de los

62.– También puede ejercerse el derecho de cancelación frente a los buscadores más relevantes en relación con la información que aparece en la memoria caché. Las dificultades que plantea la cancelación de la información personal en Internet ha sido analizado en “*Transparencia administrativa y protección de datos personales*”, cit. págs. 67-75.

63.– Basta que el afectado se oponga a la publicación de su dato personal para que ésta deba ser cancelada.

64.– La Policía dispone de una unidad de delitos tecnológicos que sigue los rastros que estas conductas dejan en Internet. Cfr. *Presente y futuro de la seguridad en la sociedad de la información*, Fundación Policía Española 2004, págs. 101-159.

derechos de acceso, rectificación y cancelación de datos personales a nivel europeo, fijando plazos de respuesta a las peticiones de las personas afectadas, autorizando el ejercicio de estos derechos por vía electrónica y obligando a motivar las denegaciones –arts. 11-15–⁶⁵.

128 La propuesta de Reglamento General de Protección de Datos personales se preocupa específicamente de dar respuesta a algunos problemas que tienen los interesados para el control de sus datos personales, frente a los tratamientos que llevan a cabo empresas que prestan servicios en Internet, como los servicios de redes sociales. Así, ante las dificultades que tienen los interesados para suprimir o para recuperar sus datos personales, se reconoce expresamente el derecho al olvido en Internet y el derecho a la portabilidad de los datos –arts. 17 y 18–⁶⁶. Se atribuye al interesado el derecho a que el responsable suprima los datos personales que le conciernan y se abstenga de utilizarlos cuando el interesado retira el consentimiento o se oponga al tratamiento. De esta manera, se reconoce el derecho de los usuarios de redes sociales a exigir a los proveedores de estos servicios de Internet que borren completamente sus datos personales cuando el cliente se dé de baja en el servicio o cuando dejen de ser necesarios para los fines para los que se recabaron. Además, se establece expresamente que cuando el responsable haya hecho públicos los datos personales, éste esté obligado a adoptar las medidas razonables –incluidas las técnicas– en lo que respecta a los datos de cuya publicación sea responsable, con miras a informar a los terceros que están tratando dichos datos de que un interesado les solicita que supriman cualquier enlace a estos datos personales, o cualquier copia o réplica de los mismos. Así, la propuesta de Reglamento establece una obligación del responsable, no sólo de suprimir los datos personales, sino de comunicar a terceros que el interesado solicita que se suprima cualquier enlace, copia o réplica de los mismos, relacionando una cosa con la otra ⁶⁷. También merece destacarse en la propuesta de Reglamento el reconocimiento del derecho a la portabilidad de la información, de manera que cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado –también cuando el interesado los haya facilitado con su consenti-

65.- Tanto la información como el ejercicio de los derechos son gratuitos, salvo que la solicitud sea claramente excesiva por su carácter repetitivo, que justifique, en su caso, la aplicación de una tasa, asumiendo el responsable la carga de la prueba de la demostración del carácter excesivo de la solicitud.

66.- El derecho al olvido en Internet es una cuestión que hemos analizado recientemente en *“Hacia un nuevo marco jurídico europeo de protección de datos personales”*, cit.

67.- El art. 13 de la propuesta de Reglamento establece también unos derechos en relación con el destinatario, que consiste en la obligación del responsable del tratamiento de informar a los destinatarios a los que haya comunicado sus datos –incluyendo al encargado del tratamiento–, de cualquier rectificación o supresión de datos en virtud del ejercicio de los derechos de los interesados, lo que tiene gran importancia en relación con el derecho al olvido en Internet.

miento y en virtud de un contrato-, la persona tenga derecho a obtener del responsable una copia de los datos en un formato electrónico que le permita seguir utilizándolos. De esta forma, el reconocimiento que hace la propuesta del Reglamento de la portabilidad de los datos supone el derecho de los usuarios a retirar sus datos -fotos o una lista de amigos- de una aplicación o un servicio y transferirlos a otra aplicación sin que los responsables del tratamiento inicial puedan bloquearlo.

El interesado al que se le deniegue total o parcialmente el ejercicio de estos derechos, tiene una acción de tutela ante la Agencia Española de Protección de Datos -art. 18 LOPD-. Hay que recordar que cualquier vulneración de la legislación de protección de datos personales debe ser denunciada ante la Agencia Española de Protección de Datos, estando tipificadas un conjunto de infracciones en el art. 44 de la LOPD, a las que se les aplica las sanciones establecidas en el art. 45 de la LOPD⁶⁸. La propuesta de Reglamento General de Protección de Datos personales refuerza tanto la independencia como la capacidad coercitiva de las autoridades administrativas de protección de datos personales, mejorando los poderes de investigación y de sanción, lo que incluye importantes sanciones económicas. Además, la propuesta de Reglamento es más exigente con quien, como las empresas que prestan servicio de redes sociales, tiene los tratamientos de datos personales como actividad principal de carácter comercial -valorando también su volumen de negocios a nivel mundial, como hacía la LOPD- siendo, en cambio, más flexible con la mayoría de las pequeñas y medianas empresas que no llevan a cabo tratamientos de datos personales como actividad principal.

129

La propuesta de Reglamento refuerza a las autoridades de protección de datos y equipara sus poderes. De esta forma, elimina las diferencias normativas existentes entre las distintas leyes nacionales que indudablemente perjudicaban a las empresas sometidas en algunos Estados a un mayor control y régimen sancionador, suprimiendo así una de las disfunciones principales que existían para un correcto funcionamiento del mercado interior.

68.- C. VELA SÁNCHEZ-MERLO, abogada del Departamento de Nuevas Tecnologías de Ernst & Young, recuerda: “para poder efectuar correctamente la denuncia y aportar pruebas suficientes, es importante recoger toda la información y todas las evidencias del tratamiento de nuestros datos. Por ejemplo, una impresión de las pantallas del sitio web donde se publica nuestra información personal, los e-mails de comunicación que este portal o página web tenga con nosotros, desde la confirmación de haber creado una cuenta, los e-mails recibidos publicitarios recibidos o cualquiera de nuestras interacciones con el portal web, así como otros e-mails, comunicaciones, etc. que se consideren pueden estar relacionados y contengan datos personales nuestros o indicios de que conocen nuestra información personal, y que no hayan sido directamente recibidos del propio portal web. De esta manera, se tiene gran parte de la información del tratamiento y podremos demostrar las presuntas finalidades con las que se están usando nuestros datos, y con ello disponer de las pruebas suficientes para poder iniciar una acción contra el vulnerador que está infringiendo los datos personales” -*loc. cit.* págs. 266-267-.

Los tratamientos de datos personales en los servicios de redes sociales tienen un carácter transnacional. Se ha analizado anteriormente como la propuesta de Reglamento aborda el ámbito de aplicación territorial y, en especial, la problemática de ley aplicable que plantean las corporaciones internacionales que ofrecen servicios de red social y tienen su sede fuera de la Unión Europea –Facebook, MySpace–. La propuesta de Reglamento aclara también cuestiones de competencia y jurisdicción de autoridades de control cuando el tratamiento de datos personales sea llevado a cabo por un responsable o encargado en varios Estados miembros, señalando como competente la autoridad donde esté situado el establecimiento principal⁶⁹. Además, trata de fortalecer la cooperación y la coherencia entre autoridades de control de la Unión Europea entre sí y con la Comisión, una cuestión a la que dedica todo el Capítulo VII –arts. 55-72–, que contiene una regulación muy novedosa que no se existía en la Directiva⁷⁰. La propuesta materializa la cooperación entre autoridades de control en un conjunto de deberes de asistencia mutua –como facilitarse información útil– y medidas de control como solicitudes de autorización y consulta previa, inspecciones, comunicación rápida de información sobre la apertura de expedientes, lo que incluye medidas represivas para que se proceda al cese o a la prohibición de las operaciones de tratamiento, todo ello dentro de plazos concretos y prohibiendo la negativa a las solicitudes de asistencia. De esta forma, se introducen normas explícitas sobre asistencia recíproca obligatoria, que incluyen las consecuencias del incumplimiento de la solicitud de otra autoridad de control –art. 55–. También se prevén operaciones conjuntas –investigaciones, medidas represivas– en las que participen autoridades de control de distintos Estados miembros, estableciendo una interesante regulación sobre la relación entre las autoridades de control del país de origen y del país de acogida, especialmente en relación con la presencia del personal de la primera autoridad, sus inspecciones y la responsabilidad sobre sus actos –art. 56–.

69.- Esta solución es calificada por la Exposición de Motivos de la Propuesta de Reglamento como “principio de ventanilla única”, con la finalidad de velar por una aplicación uniforme.

70.- Buena muestra las discrepancias en la aplicación de las normas de protección de datos personales en los diferentes Estados miembros ante el mismo supuesto de hecho, y la necesidad de actuar de manera coordinada ha sido el caso de Google Street View, que ha sido sometido a exigencias de privacidad más duras en Alemania que en otros Estados miembros. Como es sabido, entre mayo de 2007 y mayo de 2010 Google recopiló los datos de redes Wifi en muchos países como parte de su proyecto Street View, que ofrece a los usuarios de Google Maps y Google Earth la posibilidad de ver a nivel de calle las imágenes de las estructuras y los terrenos adyacentes a las carreteras y autopistas. Sin embargo, Google también recogió las contraseñas, historial de uso de Internet y otros datos personales sensibles, que no eran necesarios para su proyecto, según advirtió la Comisión Federal de Comunicaciones de los Estados Unidos de América. Google reconoció públicamente en mayo de 2010 que los coches que utilizaban para tomar las fotos para Street View habían recogido datos privados, la mayoría de ellos fragmentados. Ello dio lugar a una investigación de la FCC acerca de si se había violado la Ley de Comunicaciones.

La propuesta de Reglamento no se queda en la cooperación, sino que fija un marco de mecanismos de coherencia, que tratan de facilitar la libre circulación de datos personales en el territorio de la Unión, al mismo tiempo que se respeta la protección de datos personales, estableciendo herramientas que aproximen las divergencias entre autoridades de control. La propuesta de Reglamento incluye también mecanismos de coordinación entre órganos jurisdiccionales, de manera que si un órgano jurisdiccional competente de un Estado miembro tenga motivos razonables para creer que se están llevando procedimientos judiciales paralelos en otro país miembro, se ponga en contacto con el órgano jurisdiccional competente y pueda suspender el procedimiento -art. 75-.

Muchos de los usuarios de las redes sociales son menores, por lo que estos servicios deben respetar especialmente la legislación de protección jurídica de éstos. El Reglamento de desarrollo de la LOPD señala: “podrá procederse al tratamiento de los datos de los mayores de 14 años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de 14 años se requerirá el consentimiento de los padres o tutores”⁷¹. No tiene sentido elevar la edad para permitir a los jóvenes integrarse en una red social porque a partir de los 14 años el menor tiene capacidad de obrar para muchas cosas, incluso para emanciparse, si bien es a partir de los 16 años cuando los jóvenes tienen una mayor capacidad de decisión en ámbitos como el educativo, el sanitario o los servicios sociales. No se puede caer en un exceso de paternalismo que suprima la autonomía de los menores, algo necesario para el libre desarrollo de la personalidad.

131

No obstante, parece razonable obligar a las redes sociales a restringir al máximo grado de privacidad el acceso a los perfiles de los menores, limitando, además, el número de “amigos”. Hay que tener en cuenta que el 95 por ciento de los pederastas conocen a sus víctimas a través de los chat o de redes sociales⁷². Además, cuando las redes sociales vayan a registrar datos

71.- La redacción de este precepto, obra de Piñar Mañas, ha sido especialmente feliz. Igualmente, los derechos de acceso, rectificación, cancelación y oposición son personalísimos y deben ser ejercidos por el afectado, salvo que se encuentre en una situación de minoría de edad que le imposibilite el ejercicio personal de los mismos, en cuyo caso podrán ejercitarse a través de su representante legal. La problemática del consentimiento para el tratamiento otorgado por los menores y el ejercicio de los derechos por estos y por sus padres han sido analizados en A. TRONCOSO REIGADA, “Introducción y Presentación” a *Protección de datos personales en centros educativos públicos*, cit. págs. 61-67 y 81-85; y “La confidencialidad de la historia clínica”, *Cuadernos de Derecho Público*, núm. 27, 2006, págs. 119-130.

72.- Cfr. el informe sobre “*Protección legal de los menores en el uso de Internet*”, del Instituto Nacional de Tecnologías de la Información, cit.

de menores de edad deben expresar la información prevista en el art. 5 de la LOPD en un lenguaje fácilmente comprensible –art. 13.3 Reglamento-. Tradicionalmente, las redes sociales, si bien requerían el dato de la edad, no establecían ninguna medida para la verificación de ésta o de la autenticidad del consentimiento prestado por los padres o tutores. El art. 13.4 del Reglamento obliga al responsable del tratamiento a: “articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales”. Es, por ello, necesario que se establezcan medidas que permitan el control de la edad o del consentimiento de los padres o tutores, si bien hay que evitar un tratamiento masivo de datos identificativos por los servicios de redes sociales, que puede ocasionar un problema mayor⁷³. El Dictamen 5/2009, del Grupo de Trabajo del Artículo 29 establece un conjunto de directrices relativas a los tratamientos de datos personales de menores por parte de las redes sociales: no pedir datos sensibles en el formulario de registro, no realizar comercialización directa destinada específicamente a los menores, establecimiento de grados adecuados de separación lógica entre las comunidades de niños y de adultos, etc.

132 La propuesta de Reglamento General de Protección de Datos personales que ha presentado recientemente la Comisión, incluye una regulación relativa a los tratamientos de datos personales de los niños. Así, en el apartado de definiciones, considera niño a toda persona menor de 18 años, lo que está en contradicción, como acabamos de señalar, con el art. 13 del RPDP, que acertadamente permitía el tratamiento de los datos de los mayores de 14 años con su consentimiento, sin perjuicio de los casos en los que la Ley exija la asistencia de los titulares de la patria potestad o tutela, y con la legislación que reconoce el ejercicio de los derechos y la autonomía de la voluntad del menor maduro, también en el ámbito sanitario.

No obstante, la propuesta de Reglamento incluye también una regulación específica de los tratamientos de los datos personales relativos a los niños –art. 8-, que contiene una excepción a esta mayoría de edad de 18 años en relación con la oferta directa de servicios de la sociedad de la información, permitiendo que el consentimiento o la autorización del padre o tutor sólo sea necesaria en los tratamientos de datos personales relativos a niños menores

73.- El art. 13.4 del Reglamento de desarrollo de la LOPD ha sido analizado en la Sentencia de la Sala de lo Contencioso-Administrativo del Tribunal Supremo, de 15 de julio de 2010 –Sección Sexta-, confirmandose su legalidad. La AEPD tiene un acuerdo con Tuenti para que solicite el DNI a los usuarios respecto de los que sospeche o tenga indicios de que su edad es menor de 14 años. También ha acordado con Facebook que no inscribirá a menores de 14 años. Cfr. las notas de prensa sobre las reuniones que la Agencia Española de Protección de Datos ha mantenido con representantes de Facebook –el 26 de marzo de 2009- y de Tuenti –2 de abril de 2009- en www.aepd.es-.

de 13 años, lo que facilita el funcionamiento de las redes sociales virtuales, que tienen fijada la edad en 14 años –Tuenti– o 13 años –Facebook–⁷⁴.

Existen otras previsiones en la propuesta de Reglamento de la Comisión que tratan de proteger a los menores: la necesidad de que el responsable facilite especialmente cualquier información dirigida a niños de manera inteligible, sencilla, clara y adaptada al interesado –art. 11–⁷⁵; el reconocimiento especial del derecho al olvido en Internet y a la supresión de los datos proporcionados siendo niño –art. 17–; la toma en consideración de que el interesado sea un niño en la ponderación entre la satisfacción del interés legítimo del responsable del tratamiento y los derechos y libertades fundamentales que requieran la protección de los datos personales –art. 6–; o la exigencia de que el responsable de tratamientos de datos personales en ficheros a gran escala relativos a niños, al igual que en el caso de los datos biométricos o genéticos, lleve a cabo una evaluación de impacto en la protección de datos personales –art. 33–.

4. LAS POSIBILIDADES QUE BRINDA LA AUTORREGULACIÓN Y LA IMPORTANCIA DE LA CONCIENCIACIÓN DE LOS USUARIOS

Las redes sociales, salvo la española Tuenti, radican –o se extienden– en Estados Unidos o en otros países donde no es fácil la aplicación de la normativa europea de protección de datos personales. Por ello, cobra especial relieve tanto la autorregulación de las propias empresas como la concienciación de los usuarios.

a) *La autorregulación: canales de denuncia, privacidad por defecto, privacy by design y códigos de conducta.*

Ya se han analizado las posibilidades que brinda la autorregulación para la protección de datos personales, especialmente mientras no estén aprobados unos estándares internacionales sobre protección de datos personales⁷⁶.

74.- Téngase en cuenta que la Children's Online Privacy Protection Act (COPPA) de Estados Unidos considera menores únicamente a aquellos que no han cumplido todavía 13 años.

75.- La propuesta de Reglamento de la Comisión introduce un conjunto de garantías para la protección de los datos de menores de edad, que ya se encuentran en el art. 13 del Reglamento de desarrollo de la LOPD, en especial, que la información sea comprensible y que existan procedimientos que garanticen que se ha comprobado de manera efectiva la edad del menor y la autenticidad del consentimiento de los padres o tutores.

76.- Esta es una cuestión que se ha abordado en la ponencia “La necesidad de unos estándares internacionales de protección de datos personales y las posibilidades que brinda la autorregulación a este respecto” en la Conferencia Internacional de Privacidad y Protección de Datos Personales, celebrada en Madrid en noviembre de 2009 y, más recientemente, en “Hacia un nuevo marco jurídico europeo de protección de datos personales”, cit.

Así, en muchas ocasiones, dadas las dificultades existentes para aplicar la normativa de protección de datos personales o la demora de una resolución estimatoria en un procedimiento administrativo o jurisdiccional –consecuencia de la necesidad de respetar unos plazos para hacer efectivo el principio de contradicción o la práctica de la prueba–, lo más efectivo para hacer desaparecer una intromisión ilegítima en los derechos de las personas es acudir a los propios canales de denuncia de las redes sociales o de los sitios web. Éstos, frecuentemente, suprimen un comentario si se trata de un insulto, si hay sexo explícito o si tiene un contenido xenófobo o cancelan una fotografía si no existe consentimiento por el interesado.

A las propias empresas privadas le supone una ventaja competitiva el buen funcionamiento de los canales de denuncia. Por ello, las redes sociales deben facilitar estos canales de denuncias, garantizando la respuesta a las solicitudes en un plazo breve de tiempo y eliminando el comentario o la fotografía lesiva con la intimidad de las personas o sobre la que se ha ejercido un derecho de oposición. Las redes sociales deben también sancionar en el ámbito de su comunidad virtual a aquellos usuarios que vulneren la intimidad o la protección de datos personales de terceros, publicando fotografías o vídeos de otras personas con su oposición o realizando comentarios que sean poco respetuosos con terceras personas. Es imprescindible facilitar medios de control de comentarios y sistema de bloqueo de cuentas de forma que se puedan evitar insultos o comentarios inadecuados. Si bien, la responsabilidad civil les correspondería a los autores de la vulneración del derecho a la intimidad y a la protección de datos personales de terceras personas, las redes sociales también tendrían una responsabilidad al ser titulares del medio donde se publica la información, especialmente cuando no son diligentes en la cancelación de la misma si ha sido solicitado previamente por el perjudicado⁷⁷.

Las redes sociales deben tener en cuenta las exigencias de privacidad en el diseño de sus servicios y sistemas de información, estableciendo también políticas de privacidad que incluyan, por defecto, parámetros que sean más respetuosos con ésta. Hay que tener en cuenta que la propuesta de Reglamento General de Protección de Datos que ha presentado la Comisión, ha convertido en obligaciones para el responsable del tratamiento algunas medidas que hasta ahora estaban en el ámbito de la autorregulación, como es el caso de la privacidad por defecto y de la privacidad en el diseño. Así,

77.- Las fotografías suelen ser una fuente de conflictos, no sólo por la publicación de las mismas sin consentimiento de los usuarios, sino también por la revocación del consentimiento prestado en su momento. Si bien la red social no deja de ser un canal neutral al que no corresponde la resolución de disputas entre los usuarios de la misma, basta que exista una oposición de un interesado a la publicación de una fotografía para que ésta deba ser cancelada por la empresa proveedora del servicio de red social de manera automática.

la propuesta de Reglamento establece la obligación del responsable del tratamiento de establecer mecanismos que permitan que, por configuración inicial, sólo sean objeto de tratamiento los datos necesarios para cada fin específico, de manera que no se recojan ni se conserven datos más allá del mínimo necesario para los fines, tanto en lo que respecta a la cantidad de los datos como a la duración de su conservación, estableciéndose, asimismo, mecanismos que garanticen que, por defecto, los datos personales no sean accesibles a un número indeterminado de personas –art. 23–.

La propuesta de Reglamento también establece la privacidad en el diseño o *privacy by design*, señalando la obligación de que la protección de datos personales sea tenida en cuenta en el momento del diseño del sistema de información; es decir, que las exigencias en materia de privacidad –especialmente frente a las amenazas más frecuentes– sean un elemento a tener en cuenta en el diseño de los servicios en Internet, también en los servicios de redes sociales. Por ello, las redes sociales deben avanzar en la privacidad en el diseño y por defecto en cuestiones como, por ejemplo, los niveles de acceso a los datos personales publicados en el perfil –uno de los principales parámetros de confidencialidad– o el establecimiento de canales de denuncia.

Es necesario que las redes sociales modifiquen sus configuraciones por defecto relativas al nivel de acceso a las páginas personales, evitando que la configuración inicial prevea que toda la información esté en abierto, limitando el nivel de publicidad para que la información sea accesible únicamente para los amigos y no para los amigos de éstos. Téngase en cuenta que muy pocos usuarios modifican los parámetros establecidos por defecto. Si no se establecen restricciones al acceso, cualquier tercero puede acceder a los datos personales de los usuarios, no sólo los miembros de la red social sino también no miembros a través de los motores de búsqueda –cuando el servicio de red social así lo prevea–. Con esta medida de privacidad por defecto, las personas se ven obligadas a aceptar expresamente que personas distintas de sus contactos van a acceder al perfil, lo que reduce el riesgo para su privacidad⁷⁸. Sin embargo, en la actualidad, la mayoría de las redes sociales establecen por defecto la accesibilidad del perfil no sólo para los amigos sino también para los amigos de los amigos –la lista de contactos de los amigos–. Hay que tener en cuenta que en las redes sociales el consentimiento se ejerce habitualmente aceptando la política de privacidad establecida por defecto.

135

78.– Recientemente, Google+ ha lanzado una nueva función para los usuarios de la red social, de forma que todos los usuarios que tengan una cuenta y utilicen el servicio de Google Contact para gestionar su libreta de direcciones, puedan ver la información de sus contactos desde su perfil de la red social, integrándola dentro de la misma. No obstante, en este caso esta información sólo puede ser vista de forma privada por el usuario y no será un dato al que tengan acceso sus contactos de Google+.

La propuesta de Reglamento incide también en la importancia de los Códigos de conducta, dirigidos a contribuir a la vigencia de este derecho fundamental en sectores de tratamiento específicos –art. 38-. Sería, pues, conveniente que las redes sociales aprobaran también un Código de conducta que incluyera que los usuarios no pueden ceder datos de otras personas en la página personal –por ejemplo, fotografías o su etiquetado- sin su consentimiento, la protección de los niños, la transparencia de la información al interesado o la inclusión de los mecanismos de supervisión y garantía, como procedimientos extrajudiciales y de resolución de conflictos, que permitan resolver las controversias entre los responsables y los interesados, sin perjuicio de la posibilidad de acudir a las autoridades de control y a los Tribunales. De hecho, el propio Grupo de Trabajo del Artículo 29, en su Dictamen 5/2009, aconsejaba también la aprobación de códigos de buenas prácticas de los proveedores de servicios de redes sociales que incluyeran medidas de ejecución eficaces y sanciones disciplinarias⁷⁹.

136

Por último, hay que tener en cuenta que, en el caso de que sea difícil aplicar la normativa europea de protección de datos a una empresa que presta un servicio de red social, el incumplimiento de la política de su privacidad o del código de conducta al que está adherido representa la violación de un compromiso con el usuario que puede tener consecuencias legales graves para el responsable en muchos países –por ejemplo, en Estados Unidos–⁸⁰.

El Grupo de Trabajo del Artículo 29, en el Dictamen 5/2009, incluye otras recomendaciones dirigidas a las empresas proveedoras de servicios de red social. Entre éstas destaca la implantación de tecnologías en defensa de la privacidad –PET- como los programas informáticos de verificación de la edad o que establezcan instrumentos de control de los padres sobre el acceso de los menores a Internet o la aparición de ventanas emergentes de advertencia en fases sensibles. Llama la atención, especialmente, la recomendación relativa a un mejor cumplimiento del principio de adecuación, pertinencia y prohibición de exceso previsto en el art. 6.1.c) de la Directiva 95/46/CE en relación con la posibilidad de permitir a los usuarios de redes sociales actuar bajo un seudónimo, una medida que se ha aconsejado tradicionalmente para preservar la privacidad en Internet⁸¹.

79.- El Reglamento de desarrollo de la LOPD al regular los Códigos Tipo también incluye como garantía de su cumplimiento, la existencia de procedimientos de supervisión y el establecimiento de un régimen sancionador adecuado, eficaz y disuasorio –art. 75-.

80.- Hemos analizado recientemente la comparación entre los distintos modelos de protección de datos a nivel internacional y la importancia que tiene en Estados Unidos la autorregulación. Cfr. “El desarrollo de la protección de los datos personales en Iberoamérica desde una perspectiva comparada”, y “Presentación” en *Revista Internacional de Protección de Datos*, núm. 1 en prensa.

81.- “En este contexto, cabe señalar que el SRS puede tener necesidad de registrar algunos datos

En general, se echa en falta un adecuado diseño de las plataformas de las redes sociales para reducir los problemas relacionados con la privacidad. Por ello, es imprescindible que las autoridades de control eviten las posiciones frentistas en relación con las redes sociales, y sean capaces de generar entornos de colaboración, lo que no significa ceder ante la industria –que no deja de ser un *stakeholder*– sino de alcanzar un diálogo que permita la *privacy by design*. Esto no implica el abandono de la regulación y de los instrumentos heterónomos. De hecho, si no fuera por la presión de los poderes públicos no se movería la industria que busca el beneficio económico, y que no siempre está dispuesta a limitar los tratamientos de datos personales desleales en los servicios de redes sociales que aporten beneficio económico, si no es por la existencia de una normativa y el funcionamiento efectivo de las autoridades de control⁸².

b) La concienciación de los usuarios.

Es importante concienciar a los usuarios, especialmente a los jóvenes, acerca de la información que publican en estas redes sociales, para que valoren la importancia de su intimidad y la protección de sus datos personales, también de los de otras personas⁸³. La sensibilización hacia la privacidad personal debe estar presente tanto en el momento de registrarse como durante el desarrollo de la actividad dentro de la red social.

137

Así, todas las personas antes de incorporarse a una red social deben leer atentamente la política de privacidad para conocer especialmente el nivel de acceso a los perfiles personales. Lo más adecuado es restringir el acceso

de identificación de sus miembros, pero no es preciso que publique su verdadero nombre en Internet. Por tanto, los SRS deberían considerar si pueden justificar el hecho de obligar a sus usuarios a actuar bajo su verdadera identidad en vez de bajo un seudónimo. Son argumentos de peso para que los SRS dejen la elección a este respecto a los usuarios, y es una exigencia legal al menos en un Estado miembro. Estos argumentos son especialmente sólidos cuando el SRS en cuestión tiene miembros en todo el mundo. El artículo 17 de la Directiva relativa a la protección de datos exige que el responsable del tratamiento aplique las medidas técnicas y de organización adecuadas para la protección de los datos personales. Tales medidas de seguridad incluyen, en particular, el control del acceso y mecanismos de autenticación que pueden aplicarse aunque se utilicen seudónimos”.

82.– Además, no siempre funcionan los canales de denuncia, ya que en muchas ocasiones las redes sociales no dan de baja comentarios, alegando su neutralidad –que no tienen línea editorial– y la prohibición de la censura.

83.– Todos los documentos nacionales e internacionales relativos a redes sociales hacen hincapié en la importancia de la concienciación de los usuarios. Este es el motivo por el que se incluye este apartado en el trabajo. Cfr. el Dictamen 5/2009 del Grupo de Trabajo del Artículo 29. Cfr. los distintos Informes elaborados por el Área Jurídica del Observatorio de la Seguridad de la Información del Instituto Nacional de Tecnologías de la Comunicación “*Protección del Derecho al honor, a la intimidad y a la propia imagen en Internet*”, “*La privacidad en Internet*”, “*Protección de los menores en el uso de Internet*”, “*Redes sociales, menores de edad y privacidad en la red*”, que se encuentran accesibles en su web.

al perfil personal únicamente a nuestras las contacto –a los amigos– y no abriéndolo a los amigos de éstos⁸⁴. Para ello, es necesario modificar las configuraciones por defecto ya que a las redes sociales le interesan los perfiles abiertos, no porque sean ONGs que quieran favorecer la sociabilidad sino porque se financian con la publicidad. Las redes sociales no son redes de amigos; son redes de algunos conocidos y múltiples desconocidos; existe un desconocimiento de quién está al otro lado y si hay una posible suplantación de la personalidad. De esta forma, las redes deben emplearse preferentemente para compartir información con los amigos, no para invitar a extraños, aceptando compulsivamente solicitudes de amistad⁸⁵. Además, hay que leer la política de privacidad de las redes sociales –muchas no cumplen la legislación española– para conocer, por ejemplo, si la información personal es indexada a través de los buscadores o si se contextualiza la publicidad a través del examen de los datos del usuario y de sus preferencias; además, es bueno saber que es posible incorporarse a las redes sociales proporcionando pocos datos –muchos menos de los que se piden inicialmente–.

138 Cuando se hace la vida dentro de la red social hay que ser conscientes de que lo que se publica en Internet permanece para siempre, porque la cancelación efectiva de la información es prácticamente imposible. A veces, los jóvenes demuestran un desconocimiento profundo de la naturaleza de las nuevas tecnologías cuando piensan que mantienen el control de los datos incluidos en una red social o que esto no les va a perjudicar en un futuro a sus relaciones personales o profesionales. Sin embargo, la información que se incluye en una red social será leída y no desaparece. Lo que se publica en Internet persigue toda la vida, el pasado siempre permanece en el presente y será accesible en el futuro, ya que en Internet la información se propaga de manera viral. Como señala el estudio de la Agencia Europea de Seguridad de las Redes y de la Información, los usuarios de redes sociales afrontan el riesgo del efecto “Hotel California”: *you may enter, but you may never leave*. Una vez que un usuario se suscribe a una red social, la cancelación de la información es prácticamente imposible ⁸⁶. Esta realidad, de pérdida del

84.- Los amigos de mis amigos, a diferencia de lo que dice la canción, son gente desconocida y entre los que se encuentran, sin duda, personas entrañables y otras que no lo son tanto. Hay que destacar que Tuenti tiene un sistema de invitación, de manera que sólo se puede entrar en esta red social previa invitación de un usuario, teniendo cada uno de ellos un número limitado de invitaciones –30–. Además, esta red social no admite la indexación de la información a través de motores de búsqueda. Frierster.com fue diseñada para que los usuarios se hicieran amigos de sus amigos, permitiendo la navegación por la lista de contactos de amigos con cuatro grados de cercanía –amigos de amigos de amigos de amigos–. Pero la creación de perfiles falsos permitió vencer la restricción.

85.- Por eso, el lema de la Campaña de la Agencia de Protección de Datos de la Comunidad de Madrid, que ha llegado en enero de 2010 a más de 400 centros educativos públicos y a 80.000 jóvenes ha sido “Hay cosas que no contarías a un extraño, por qué hacerlo en Internet”.

86.- Las personas queremos ser valoradas por lo que somos ahora, pero no por lo que fuimos o

control tiene que llevar al usuario a que la publicación de información en la Red no sea un automatismo sino un acto consciente –ese *think before you post*–. Hay que pensar previamente la información que se va a incorporar, siendo conscientes de que lo que se publica en Internet se escapa del control personal para siempre. La información que se publicó hace años en la Web –determinadas actitudes, expresiones, fotografías– podrá influir en decisiones futuras que se tomen sobre nosotros en el ámbito laboral. Hay comentarios que, si bien en un momento pudieron parecer simpáticos, en el futuro pueden resultar extraños al propio autor y proyectar una imagen desfigurada de lo que es⁸⁷. Muchas decisiones en la era de Internet –publicar una fotografía en una red social, insertar un comentario en Twitter o contestar un correo electrónico– se toman en lo que Daniel Kahneman ha definido el sistema 1 –el pensamiento más intuitivo y rápido, que requiere un menor esfuerzo mental–, un comportamiento que generalmente incrementa la posibilidad de error y crea problemas a los usuarios⁸⁸.

hicimos en un pasado que tal vez queramos olvidar. Sin embargo, la publicación de información en Internet supone una pérdida de control ya que la difusión es inmediata y alcanza a mucha gente no sólo en el presente sino también en el futuro. Así, por ejemplo, la difusión de una foto impresa se limita a un círculo reducido. La captación de una imagen por un dispositivo electrónico –cámara digital, teléfono móvil, webcam– hace que esta información sea grabada y pueda ser distribuida a través de múltiples terminales.

- 87.– El Dictamen 5/2009 del Grupo de Trabajo del Artículo 29 señala que los datos personales publicados en los sitios de redes sociales “pueden representar grandes riesgos, como la usurpación de identidad, pérdidas económicas, pérdida de actividad económica o posibilidades de empleo, o ataque a la integridad física”. Por ello, el Grupo de Trabajo recomienda que “los proveedores de SRS adviertan adecuadamente a los usuarios sobre los riesgos de ataque a su intimidad y a la de otros cuando ponen información en línea en los SRS”.
- 88.– D. KAHNEMAN, Premio Nobel en Ciencias Económicas por sus trabajos sobre psicología económica, ha publicado “*Thinking, Fast and Slow*” –Farrar, Straus and Giroux, New York, 2011, esp. págs. 19-107 y 408-419–, un estudio que cuestiona el modelo racional del juicio y la toma de decisiones. Kahneman ha explicado que existen dos sistemas que conducen a la manera en que pensamos. El sistema Uno, que es rápido, intuitivo y emocional, y concluye rápidamente sin esperar a la conciencia racional; y el sistema Dos, que es más lento, deliberativo y lógico. El Sistema Uno tiene un acceso casi instantáneo a un vasto almacén de memoria, que es el que se utiliza de referencia y patrón para adelantar conclusiones rápidas. Y en ese almacén de la memoria, los recuerdos más impactantes e influyentes son aquellos asociados con emociones muy intensas: el miedo, el dolor, el odio. Este Sistema Uno presenta un importante margen de error. Es, más bien, la herencia del mundo de la selva, donde mejor le va al rápido, incluso si se equivoca, que a uno muy acertado, pero lento al decidir. En cambio, el Sistema Dos, a través del proceso lento de análisis y examen crítico de la evidencia disponible, llega a juicios más conscientes. Para ello, toma en cuenta los insumos del Sistema Uno, pero da la opción de revisar las opciones y corregir los errores. Probablemente, esa parte del cerebro se desarrolló más recientemente, cuando existía más tiempo para pensar, planear y coordinar actividades y de ahí nació luego la cultura y el arte. Si bien los dos sistemas trabajan juntos, Kahneman señala cuando se debe confiar en las intuiciones y cuando, en cambio, se deben aprovechar los beneficios del pensamiento lento. Kahneman expone las capacidades extraordinarias y también las fallas y los sesgos de pensamiento rápido, y pone de manifiesto la profunda influencia de las impresiones intuitivas en los pensamientos y conducta.

Además, no se debe dar información personal a extraños. En Internet nunca se sabe con certeza quién está al otro lado y la persona se puede llevar grandes sorpresas⁸⁹. Ya se ha señalado anteriormente la conveniencia de restringir el nivel de acceso al perfil personal sólo a los amigos. O al menos, si se aprovecha las redes como instrumentos de exploración social, es necesario ser prudente, distinguiendo la información que ofrecemos a éstos de aquella que se proporciona a desconocidos. Es necesario tratar de limitar la información que se incluye en el perfil personal abierto. En general, hay que tener cuidado con dar información como la dirección, el número de teléfono o enviar fotos a personas desconocidas a través de la red social⁹⁰. A veces, en la redes se ofrecen determinados datos o se introducen imágenes comprometidas que no se darían en la vida off-line. Si habitualmente no se cuenta la intimidad a personas que no se conocen, tampoco se debe hacer en la Red. Hay una falta de conciencia acerca de las consecuencias de que los datos personales sean accesibles por cualquier persona.

La privacidad no trata solo del respeto a los datos personales propios, sino también a los de los demás. Una característica de las redes sociales -y, más en general, de las web 2.0- es que son los usuarios los que incorporan la información personal. Estos tienen que respetar los derechos de los demás y no publicar información de otros -por ejemplo, fotografías- sin su autorización⁹¹. A veces son simples bromas, que pueden causar un perjuicio enorme e irreparable⁹²; en otras ocasiones existe una voluntad deliberada y consciente de hacer daño. La falta de respeto a la intimidad y a la privacidad de los demás puede llegar a ser humillante, afectando a la autoestima y causando un problema psicológico⁹³.

89.- En la campaña de la Agencia de Protección de Datos de la Comunidad de Madrid para concienciar a los jóvenes sobre el uso de redes sociales en enero de 2009, se utilizaba la expresión “en Internet, nadie sabe que tú eres un perro”, para poner el énfasis en las dificultades que presenta este canal a la hora de identificar a los interlocutores. También se ha indicado anteriormente la conveniencia de utilizar en algunos casos seudónimos o *nicks* dentro de las redes sociales para preservar la propia privacidad.

90.- Hay que insistir a los menores en que no deben quedar con extraños que hayan conocido en Internet y, en el caso de que lo hagan, deben ir acompañados por otras personas mayores.

91.- El Dictamen 5/2009 del Grupo de Trabajo del Artículo 29 señala que los proveedores de SRS tienen la obligación de asesorar a sus usuarios en lo que se refiere al derecho a la intimidad de los demás. Así, estos deben recordar a sus usuarios que “poner en línea información relativa a otras personas puede perjudicar su derecho a la intimidad y a la protección de datos; los SRS deben aconsejar a sus usuarios que no suban fotografías o información relativa a otras personas sin el consentimiento de éstas”.

92.- De hecho, lo que puede parecer una broma para quien la hace se convierte frecuentemente en un drama para quien la padece.

93.- Esto ocurre, por ejemplo, cuando determinadas fotos hechas dentro de una relación de pareja son publicadas en Internet cuando la relación termina de manera no amistosa; o cuando se

Si bien la Directiva 95/46/CE y la LOPD excluye de su ámbito de aplicación los tratamientos efectuados por una persona física en el ejercicio de actividades exclusivamente personales o domésticas –lo que alcanza a los usuarios de redes sociales cuando no tengan el carácter de responsables del tratamiento–, sí están obligados a respetar el derecho a la intimidad, al honor y a la imagen de otros seres. Es especialmente grave la posibilidad que ofrecen las redes sociales para llevar a cabo el *cyberbullying* –acoso a través de las tecnologías de la información–, que convierte la vida de algunos jóvenes o de profesores en una auténtica pesadilla. Estas permiten desarrollar conductas hostiles, atacar la reputación, dañar la intimidad de otras personas a través de comentarios, invención de historias, creación de perfiles falsos, suplantación de la personalidad, etiquetado de fotos, etc. Se humilla, se insulta, se amenaza, se chantajea –por ejemplo, con colgar fotos–, se trata de desprestigiar a una persona en Internet y, especialmente, a través de las redes. Si bien los supuestos de acoso existían con anterioridad a la aparición de Internet y de las redes sociales, éstas han favorecido que se den a conocer estas conductas hostiles, generando efectos miméticos y multiplicando sus efectos nocivos, lo que ha incrementado exponencialmente el daño. Hace falta menos valor para criticar a alguien en Internet que para hacerlo de manera presencial. Además, un insulto en la vida real se olvida; en cambio, un comentario en Internet se multiplica, genera una cadena que no pretende el que lo emitió y se transmite de manera viral a través de la Red, que tiene una gran velocidad e inmediatez en la difusión⁹⁴. Existe una cierta imagen de irresponsabilidad en lo que ocurre en el mundo virtual. Sin embargo, no existen espacios de impunidad. Cuando un usuario considere que sus derechos se han vulnerado, debe denunciar los hechos a los administradores de la red social para solicitar la retirada del comentario o de la fotografía, además de bloquear a la persona. Hay que recordar que los usuarios pueden ejercer el derecho de cancelación y oposición sobre su información personal sometida a tratamiento que aparece en la red social. Los hechos pueden ser denunciados ante la Agencia Española de Protección de Datos; además la Administración dispone de una potestad sancionadora en el ámbito educativo. También existe una responsabilidad personal tanto civil como penal por vulnerar el derecho al honor o a la intimidad.

141

suplanta la personalidad de otro, elaborando un perfil falso dentro de una red social donde se incluye el ofrecimiento para mantener relaciones sexuales.

94.- Hay que decirle a los jóvenes, no sólo que no reenvíen las cadenas de ciberacoso, sino que las denuncien, afeando la conducta de quienes lo llevan a cabo. Además, hay que concienciar a los jóvenes sobre la importancia del respeto a los demás en el lenguaje y en las actitudes que emplean en Internet –por ejemplo, no insultando a nadie como tampoco se hace en la relación presencial–.

Por lo expuesto, son necesarias las iniciativas de sensibilización en relación con los riesgos que presentan las redes sociales, especialmente en el ámbito educativo⁹⁵. Hay que destacar que la Agencia de Protección de Datos de la Comunidad elaboró un “Plan de Comunicación en Protección de Datos Personales para Escolares”, dirigido especialmente a aquellos alumnos que se encuentren cursando Enseñanza Secundaria⁹⁶. La finalidad de este Plan es dar a conocer entre los alumnos el derecho fundamental a la protección de datos personales, exponiendo los riesgos a su privacidad que provienen de las modernas tecnologías de la información y las comunicaciones, tratando de que los menores se conciencien acerca de la necesidad de un uso responsable de éstas. Este Plan se centra en tres acciones:

95.- El Dictamen 5/2009, del Grupo de Trabajo del Artículo 29 ha resaltado las iniciativas que han desplegado en este ámbito las autoridades de protección de datos, “fundamentales para garantizar el compromiso activo de los niños (mediante las escuelas, la inclusión en el programa escolar de elementos de protección de datos, la creación de herramientas educativas ad hoc y la colaboración de organismos nacionales competentes)”.

96.- La Agencia de Protección de Datos de la Comunidad de Madrid elaboró este Plan inspirándose en el proyecto realizado por la Oficina de Protección de Datos de la República Checa y la ONG Iuridicum Remedium, titulado “*My privacy. Don't look, don't poke about*” –“¡Mi privacidad! No mires, no curioses”–, que recibió el Primer Premio a las Mejores Prácticas de las Administraciones Públicas Europeas en materia de Protección de Datos Personales correspondiente al año 2007 –cfr. la *Memoria de la IV Edición del Premio a las Mejores Prácticas de las Administraciones Públicas Europeas en materia de Protección de Datos*–. Se trata de un concurso de ensayos, ilustraciones, collages y esculturas sobre privacidad en el que participaron niños y jóvenes entre 12 y 20 años que se anunció el día 28 de enero de 2007 coincidiendo con el primer día de la Protección de Datos. Este proyecto, apoyado por diferentes medios de comunicación, se inscribió dentro del programa educativo “los datos personales en la Educación”, que tenía como objetivo coordinar las direcciones de los centros, la inspección escolar y los profesores para introducir la materia de protección de datos en el sistema educativo checo, a través de la formación de los profesores y el estudio de la materia en las diferentes asignaturas de su plan de estudios. La Segunda Mención Especial recayó en el Inspectorado de Protección de Datos de Noruega por el proyecto “*Tú decides. Campaña educativa sobre protección de datos personales*”, una campaña de sensibilización a los jóvenes sobre el tratamiento de sus datos por las nuevas tecnologías (especialmente Internet). La Agencia empleó estos videos noruegos para la campaña en la Comunidad de Madrid. Además, como herramientas para la realización de esta iniciativa, se tuvo en cuenta los folletos de protección de datos para jóvenes, elaborados por la Comisión de Libertades e Informática en colaboración con todas las Agencias de Protección de Datos de España, que tratan de exponer los aspectos fundamentales del derecho a la autodeterminación informativa de una manera sencilla, huyendo de tecnicismos y con un lenguaje claro y comprensible. Para ello, incluyen ejemplos que puedan ser ilustrativos para el público más joven. Destacar también que la Agencia de Protección de Datos de la Comunidad de Madrid elaboró en el año 2002 un *Cuaderno Informativo sobre Protección de Datos para Escolares* que trataba de ser una aproximación a esta materia orientada y dirigida a menores, que, en muchas ocasiones, ceden sus datos personales y deben ser conscientes de su valor y de que un uso o cesión abusiva puede afectar a su intimidad personal y familiar. Este Cuaderno exponía, de manera sencilla, los aspectos fundamentales del derecho a la autodeterminación informativa, de forma que se pueda facilitar que los profesores puedan impartir alguna unidad formativa en protección de datos a los estudiantes. Durante los años 2002 a 2004 la Agencia editó 7.000 ejemplares de estos cuadernos que fueron enviados a los centros educativos.

- 1) Formar al profesorado en la legislación de protección de datos personales, desde una perspectiva práctica vinculada a su actividad docente.
- 2) Transmitir a los alumnos la importancia del respeto a la privacidad personal de manera transversal en las distintas materias -Literatura, Historia, Ciencias Sociales, Matemáticas y Tecnología, etc.-, así como en la asignatura de Educación para la Ciudadanía.
- 3) Acciones específicas, como breves sesiones informativas en los centros educativos, que se hacen coincidir con el Día Europeo de la Protección de Datos Personales, que se conmemora el 28 de enero. Se trata de suscitar un debate acerca de los tratamientos de datos personales que los jóvenes realizan cotidianamente a través del uso de redes sociales, mensajerías instantáneas, chats, telefonía móvil, etc., y de sus consecuencias presentes y futuras, teniendo en cuenta que ninguna información desaparece.

Por ello, la Agencia de Protección de Datos de la Comunidad de Madrid realizó el 28 de enero de 2009, con motivo del Día Europeo de la Protección de Datos Personales, sesiones informativas en los centros escolares, con el objetivo de dar a conocer entre los alumnos el derecho fundamental a la protección de datos personales, exponiendo los riesgos a su privacidad que provienen de las modernas tecnologías de la información y la comunicación, tratando de que los menores se conciencien acerca de la necesidad de un uso responsable de éstas. Estas sesiones informativas se celebraron en los 404 Institutos de Educación Secundaria para 2º y 3º de ESO, a las que asistieron un total de 80.000 alumnos de la Comunidad de Madrid. En esta campaña participaron expertos de reconocido prestigio en materia de protección de datos, entre los que se incluyen magistrados, fiscales, profesores, abogados, consultores, así como orientadores del ámbito educativo, inspectores de educación, tutores, directores de centros, etc⁹⁷.

Dado el éxito de la campaña del año anterior, la Agencia de Protección de Datos de la Comunidad de Madrid organizó una iniciativa semejante el día 28 de enero de 2010 en los 404 Institutos de Educación Secundaria de la Comunidad de Madrid, que en esa ocasión fue dirigida a los alumnos de 1º y 2º de la ESO⁹⁸. La novedad de la campaña de ese año fue la utilización de la red social Tuenti y de YouTube -los dos canales más utilizados por los jóvenes con edades comprendidas entre los 11 y los 20 años-, para mentali-

97.- Esta campaña fue recogida por distintos medios de comunicación -Telecinco, CNN+, Cuatro, haciendo un seguimiento especial Telemadrid-.

98.- Esta ha sido la última iniciativa que desarrollé como Director de la APDCM, cargo en el que cesé por expiración del mandato el 2 de febrero de 2010.

zarles de la necesidad de proteger sus datos personales cuando se conecten a Internet y a redes sociales. Así, bajo el lema “Hay cosas que no contarías a un extraño, ¿por qué hacerlo en Internet?”, la Agencia de Protección de Datos de la Comunidad de Madrid realizó dos vídeos destinados a los menores y que pueden descargarse en Tuenti y en YouTube⁹⁹, que colaboraron con esta campaña, estableciendo un enlace patrocinado o situándolos como vídeos destacados durante los días 25 a 29 de enero de 2010¹⁰⁰. Además, los audiovisuales fueron emitidos desde el 28 de enero hasta el 3 de febrero de 2010 con cuatro pases diarios en los canales de televisión: Telemadrid SAT y en LaOtra, y con dos pases diarios en Telemadrid, habiéndose obtenido previamente la exención de publicidad. La iniciativa tuvo un seguimiento por los servicios informativos de Telemadrid –en el Programa Buenos Días– y de Antena 3 –en el programa Espejo Público–¹⁰¹.

99.- Estos dos vídeos, que se difundieron durante la Semana Europea de Privacidad, fueron hechos por la productora Wakeup Pictures, que prácticamente no cobró por su aportación –equipo de rodaje, realización, actores, directora de arte, *atrezzo* de rodaje, postproducción de imagen, música y sonido, exportación para Internet, etc–, en aras de la realización de un proyecto que consideraba de interés general. También agradecer a Tuenti y a YouTube que pusieran los videos como eventos patrocinados y destacados sin coste alguno.

100.- Están en el canal “Agencia datos Madrid” de YouTube. En lo que respecta a Internet, la iniciativa ha tenido un gran éxito de visitas y de participación viral entre los jóvenes. El martes 2 de febrero de 2010 los dos videos habían tenido más de 77.000 –Tienda de fotos 46.018 y Cafetería 31.822–. Durante la semana del 25 al 31 de enero de 2010, el canal “Agencia de Protección de Datos de la C.M estaba en el puesto 33 de los más vistos en YouTube, habiendo tenido más visitas en esa semana que los de Antena 3, rtve.es, MiSexta o Cadena 100 en YouTube. También se situó en el puesto 13 de la semana como canal con más suscripciones).

101.- El seguimiento que recibió la iniciativa por parte de la prensa escrita fue también muy importante. Cfr. entre otros muchos:
<http://www.abc.es/20100128/medios-redes-web/cosas-contarias-extrano-hacerlo-201001281047.html>
<http://www.prnoticias.es/index.php/prmadrid/472/10051855-ipor-que-contar-en-internet-lo-que-no-le-contarias-a-un-extrano>
<http://www.diaadia.com.ar/?q=content/%C2%BFpor-que-lo-contarias-en-internet>
<http://www.europapress.es/madrid/noticia-proteccion-datos-informara-manana-cerca-80000-chicos-comunidad-privacidad-redes-sociales-20100127175127.html>
<http://www.adn.es/local/madrid/20100127/NWS-2237-Proteccion-Comunidad-Datos-privacidad-informara.html>
<http://noticias.terra.es/2010/local/0127/actualidad/proteccion-de-datos-informara-manana-a-cerca-de-80000-chicos-de-la-comunidad-sobre-la-privacidad-en-las-redes-sociales.aspx>
<http://ecodiario.eleconomista.es/espana/noticias/1865460/01/10/Proteccion-de-Datos-informara-manana-a-cerca-de-80000-chicos-de-la-Comunidad-sobre-la-privacidad-en-las-redes-sociales.html>
<http://derechonuevastecnologias.wordpress.com/2010/01/26/madrid-quiere-advertir-a-los-jovenes-sobre-su-privacidad-en-redes-sociales/>

La mayoría de los jóvenes afirman haberse sentido maltratados alguna vez dentro de una red social. Sin embargo, nadie va a renunciar a Internet o a las redes sociales aunque haya riesgos. Se trata, en definitiva, de minimizar estos riesgos, explicando la naturaleza de estas tecnologías y las consecuencias presentes y futuras de los propios actos, tratando de concienciar a los ciudadanos –especialmente a los más jóvenes– en un uso responsable de Internet y de las redes sociales, y en el valor de su privacidad y la de otras personas. La solución como siempre está en educar, una labor que corresponde no sólo a los profesores sino especialmente a los padres, y que contribuirá a encontrar un equilibrio entre el deseo de comunicación y de ampliación del círculo de amistades y el respeto a la dignidad de la persona en Internet.

MESA REDONDA:

PROTEGER A LOS MENORES EN LAS REDES SOCIALES

ARTURO CANALDA GONZÁLEZ
Defensor del Menor de la Comunidad de Madrid (2006-2012)

147

El Defensor del Menor es una institución que a lo largo de sus 15 años de existencia se ha mostrado siempre como un elemento de referencia en la protección de la infancia, y durante los últimos años ha dedicado especial atención al ámbito de las nuevas tecnologías.

Desde la institución del Defensor del Menor se ha insistido durante muchos años en la necesidad de que los adultos se implicaran más en lo que hacen los hijos en el mundo virtual, donde prácticamente todo el mundo es anónimo y nadie es quien dice ser. En ese espacio, los menores, probablemente, no tienen conciencia de que a veces determinadas actividades, actitudes o contenidos que suben día a día a la Red de forma probablemente inocente, pueden tener consecuencias, en ocasiones, demoledoras para ellos.

En este caso, se van a tratar cuestiones que entran dentro de los aspectos conceptual y educativo de los niños, para con ello ver la gran incidencia que tienen las redes sociales y las nuevas tecnologías y el porqué se producen determinadas situaciones que afectan a los niños o que, desgraciadamente, tienen como protagonistas a los propios infantes cometiendo algún tipo de delito.

Para los adultos, la amistad es una relación entre dos personas que se conocen, una relación de cariño, de afecto, en la que se prestan apoyo, que muchas

veces está amparada simple y llanamente por el roce diario o generada por ese. Es algo muy importante en la vida del ser humano y en el desarrollo de las personas, y los amigos de verdad se cuentan con los dedos de una mano.

Para un adolescente de 14 o 15 años ese concepto de amistad es radicalmente distinto, y éste es un tema gran relevancia. Ha cambiado porque para ellos la amistad es más una adhesión virtual, una amistad de teclado. Desde que se levantan hasta que se acuestan los niños están permanentemente conectados con mediante Whatsapp, Messenger, Facebook, Tuenti, etc., y están interactuando entre ellos, cambiando mensajes y contenidos a través del ordenador o del teléfono móvil. Esto es clave porque en el mundo virtual, prácticamente, nadie es quien dice ser y los chicos muchas veces no son conocedores de ello.

148 Son amistades virtuales en las que un niño te dice que en la red tiene 4.372 amigos. Y esto no deja de ser chocante. En entornos tan grandes se generan problemas de gran dimensión. Por ejemplo, si el joven coloca en la red social o en el muro de su perfil un comentario diciendo que su padre le ha regañado porque he sacado malas notas, lo lógico es que ese niño reciba muchos mensajes de apoyo de todos los compañeros, de su grupo de iguales contándole que su padre no sabe lo que dice y que él ha sacado malas notas por esto o por esto otro. En definitiva, el mensaje que dan los padres, que dan los adultos, es inmediatamente contrarrestado por un número muchísimo mayor de personas, que es el grupo de iguales, supuestos amigos de los hijos en las redes sociales. Esto desde el punto de vista educativo tiene su trascendencia. El mensaje único de un padre o de una madre que dice al hijo que hay que estudiar más, que en esta vida para ser algo uno tiene que esforzarse, tiene que trabajar, se transforma en que tus padres no te entienden, que eso es una barbaridad, que haces muy bien, etc. Esto es un gran reto educativo para los padres.

Esto también tiene que ver con los derechos de autor, de propiedad intelectual, derechos que están amparados por la ley, pero que, con el uso de las nuevas tecnologías, los menores no tienen interiorizados y su sensación es que todo es gratis, que se puede obtener cualquier cosa sin esfuerzo, pues no asumen que cuando alguien hace algo, desarrolla un producto, crea una canción, un libro, software, etc., le ha supuesto un esfuerzo, un trabajo y una inversión. ¿Dónde está el problema? ¿En que se está vulnerando la Ley de Propiedad Intelectual? Sí, eso es un problema, pero más grave es que el niño sea consciente de que alcanzar aquello que le apetece no le cuesta ningún esfuerzo, que todo en la vida es gratis. Eso se traduce después en el ámbito educativo en fracaso escolar. Hoy día los chicos tienen el umbral de frustración tan bajo, que cuando no consiguen en tiempo real lo que quieren se genera esa enorme decepción.

Hay otra serie de conceptos que también son importantes. Por ejemplo, la intimididad. Día a día se está vulnerando el derecho al honor y a la intimidad por parte de los menores. Los chicos suben mucha información que les atañe a ellos, normalmente de sus familias, de su entorno más cercano. Y no solo hacen eso, sino que escriben información correspondiente a compañeros de forma indiscriminada, sin valorar, sin ponderar la incidencia o la importancia que pueda tener eso en los protagonistas de la misma. Pueden ser casos de acoso escolar, que cada día son más numerosos y con mayor trascendencia.

Hasta la llegada de Internet, el acoso escolar, aún siendo importante y con unas consecuencias realmente graves para el que lo sufría, tenía unos límites temporales –la estancia en el centro educativo– y unos límites espaciales –el aula o el patio del colegio–. El acoso escolar utilizando las nuevas tecnologías, el conocido como *cyberbullying*, rompe esos límites de tiempo y espacio para transformarse en un hostigamiento permanente. En el acoso tradicional se producía, además, la barrera de la mirada del otro, que usando las nuevas tecnologías no existe, por eso juegan una especial relevancia quiénes en el mundo real jamás se hubieran atrevido a meterse con un compañero, pero que utilizando el teclado del ordenador sí que lo hacen. Y también se produce el efecto bola de nieve: “si todos los compañeros lo están haciendo yo no voy a ser menos”. Por tanto, el acoso escolar es mucho más grave utilizando las nuevas tecnologías, normalmente con sus consecuencias, que el acoso escolar presencial. Lo que ocurre es que hoy en día, lamentablemente, el acoso escolar presencial, real, se complementa con el acoso escolar usando las redes sociales.

149

Por todo ello es tan importante trabajar en el ámbito de la educación y de la prevención, y que en el aula los profesores sean capaces de detectar cualquier situación de acoso escolar. Las nuevas tecnologías evolucionan a una velocidad tan tremenda, que cuando se plantean soluciones a problemas que se han presentado, éstas normalmente quedan obsoletas.

Esto se aplica también al ámbito legal, aunque España tiene uno de los códigos penales probablemente más avanzados en esta materia, sobre todo en el entorno de la Unión Europea. Pero de nada sirve un Código Penal muy avanzado si aquel que tiene que aplicarlo no está realmente especializado en saber entender e interpretar lo que se está diciendo, de tal manera que permita perseguir de forma efectiva los delitos. Esto significa que hay que dotar de muchos más medios tanto a las Fuerzas y Cuerpos de Seguridad del Estado, para crear grupos especializado en esta materia, como a la Fiscalía, que es quien tiene de alguna manera que articular todo esto.

Hay otra idea básica y es que el compromiso de los adultos con los menores va mucho más allá de lo que muchos piensan. Porque los hijos son lo que ven, el ejemplo cuenta mucho. Los padres tienen que implicarse con sus hijos en el uso correcto de las nuevas tecnologías.

Es verdad que los chicos tienen la capacidad a los 14 años de tener un perfil en Facebook o en Tuenti porque legalmente se les permite. Pero una cosa es lo que dice la ley, que pueden disponer de sus datos personales, y otra que sus padres entiendan que el niño no tiene la madurez suficiente para hacer uso de según qué cosas. Si el niño dice, con 13 o 14 años, que quiere tener un perfil, tendrá que pedir permiso o autorización a sus padres y si éstos entienden que no debe, no lo tiene y nada ocurre, es así de sencillo, porque no todos los chavales tienen la misma madurez.

Otro tema es la labor de supervisión que tienen que realizar los padres con respecto a lo que hacen sus hijos en la Red. Cuando el niño es muy pequeño hay que supervisarle, cuando el niño es más mayor simplemente hay que tener una cierta prudencia sobre qué hacen con Internet, y explicarle clarísimamente que cuando tenga un problema a quien tiene que acudir es a su padre o a su madre para pedir ayuda.

150

Los adultos se tienen que implicar de verdad. Las redes sociales son estupendas, son un medio de comunicación maravilloso, pero lo que hay que hacer es hablar más con los hijos, sentarse con ellos, saber con quiénes van, etc. Hay que insistir mucho en que es una obligación de los adultos ocuparse de los hijos, no es inmiscuirse en su vida, no es vulnerar su intimidad, es ejercer de padres.

Hay que implicarse mucho con los hijos y con nuevas tecnologías. Pero, ¿qué ocurre cuando el hecho catastrófico ya se ha producido?, ¿qué hay que hacer? Primero, ser conscientes de lo que ha ocurrido; segundo, ver qué consecuencias tiene para el chico o chica; y tercero, buscar las soluciones. Eso es lo más importante, y para ello hay que educarse, buscar información, que hay muchísima, tanto en el Ministerio del Interior, a través de la página web de la Policía y de la Guardia Civil, del Instituto Nacional de Tecnologías de la Comunicación (INTECO), de la Secretaría de Estado de Telecomunicaciones (red.es), la Asamblea de Madrid, etc. en definitiva, todas las administraciones tienen multitud de información que sirve a los adultos para saber qué hacer en casos complicados.

Y para terminar, algo fundamental: el niño educado en valores en el mundo real es un niño educado en valores en el mundo virtual. Eso pasa siempre, la educación queda. Aquel que ha vivido desde chiquitito el respe-

to, el esfuerzo, el trabajo, el sacrificio, el ayudar a sus padres, el respetar a los abuelos, el respetar a los profesores, etc., lo lleva dentro.

Hay que educar a los hijos en valores, explicarles que en el mundo virtual es tanto o más importante el respeto a los demás que en el mundo presencial, sobre todo porque normalmente no se sabe con quién están hablando.

PROTEGER A LOS MENORES EN LAS REDES SOCIALES

CELIA CARREIRA VIGO
Inspectora del Cuerpo Nacional de Policía.
Jefa del Grupo III, de la Brigada de Investigación
Tecnológica, de Protección al Menor

*Internet es una herramienta muy poderosa de libertad,
de información, de comunicación, con grandes y
diversas utilidades.*

153

Las comunicaciones personales han ido evolucionando, desde la mensajería instantánea como el Messenger, Internet Relay Chat (IRC), I Seek You (ICQ), etc., hasta el concepto actual de redes sociales, que es una novedosa forma de relación humana haciendo uso de las nuevas tecnologías. La utilización de las redes sociales como medio de comunicación es un fenómeno que está en desarrollo, en evolución y en auge. En este caso, los interlocutores realizan una puesta en común de aficiones, gustos, experiencias, etc., generando así un perfil público con la única finalidad de que sus contactos puedan acceder a esa información. Esta aplicación on-line posibilita compartir, colaborar en la generación de contenidos, e incluso participar de manera espontánea en movimientos sociales y corrientes de opinión.

Hay muchas razones para el éxito de Internet. Obviamente es una herramienta básicamente relacional, que relativiza el concepto espacio-tiempo (inmediatez en las comunicaciones). También están la gratuidad, la sencillez, la rapidez de interconexión, que la convierten en un instrumento muy útil en todas las relaciones humanas, en el sentido que se mantienen hoy. El avance de la tecnología también favorece la utilización de este medio de comunicación, porque supone un abaratamiento de los costes, la alta velocidad de conexiones, como puede ser 3G, por cable, por ADSL, etc.

La Red es un fenómeno social y económico, que lo que implica es un número muy alto de usuarios y, a la vez, unos beneficios enormes. Sin embargo, son muchos los peligros que encierra, sobre todo cuando se habla de menores, que son el motivo de mayor protección pues se encuentran una situación de especial indefensión.

Los adultos utilizan Internet, los jóvenes están en Internet, conocen perfectamente su funcionamiento, las utilidades, los beneficios. El peligro para ellos radica en la falta de madurez y de experiencia, de conciencia de los peligros y riesgos que puede implicar el uso de este medio de comunicación. Pero para ellos es, sin duda, una herramienta básica de identidad y de relación.

Ocurre que, precisamente por estas características de los menores, las instituciones públicas, así como la legislación, deben de otorgarles un mayor grado de protección. A estos efectos, destacar que en el año 2009 se firmó en Luxemburgo el Convenio Europeo de Protección a Menores, en el que 17 redes sociales rubricaron por primera vez un acuerdo para reducir, evitar o disminuir las amenazas de los menores en el uso de las redes sociales.

154 **RIESGOS DE MENORES ANTE EL USO DE LAS REDES SOCIALES**

Estos peligros pueden ir desde hechos claramente delictivos, como puede ser la figura del grooming, a otros que rozan la línea entre lo ilegal y lo inapropiado, como contenidos a los que no debería acceder un menor, por ejemplo pornografía para adultos, que obtienen a través de las redes sociales o a través de Internet en sí mismo.

Grooming

El primer gran problema es el grooming (está tipificado expresamente en el Código Penal en el artículo 183 BIS, y está previsto que se modifique su contenido para ajustarlo y endurecerlo), que consiste en acosar a menores a través de Internet con la finalidad de obtener fotos e imágenes de los menores desnudos o en actitudes claramente sexuales.

Existe la creencia de que las víctimas de grooming son en su mayoría niñas, sin embargo afecta a ambos sexos por igual, aunque los agresores son en su mayoría hombres.

Este tipo de hecho delictivo se caracteriza porque los delincuentes utilizan tácticas y técnicas muy sofisticadas para conseguir su objetivo. No es un

engaño burdo por lo que también un adulto, con su experiencia, podría ser engañado. También es un factor común en todos los autores de grooming que no les importa en absoluto el daño que puedan causar a sus víctimas, llegando éstas incluso en muchos casos, como ya ha ocurrido, al extremo del suicidio.

¿Cuáles son los medios que utilizan los agresores de grooming para contactar con menores? Son las mismas plataformas que emplean los niños y que, obviamente, también son atractivas para pedófilos y pederastas, que acceden como primer medio de contacto con las víctimas..Tienen especial relevancia los chats, o las webs Fotolog y Vota mi cuerpo, que son páginas en las que, en muchos casos, los menores exhiben públicamente su cuerpo sin saber quién los está viendo. Son imágenes que suelen tomarse ellos voluntariamente y que cuelgan en Internet, sin saber que están a disposición de terceros que pueden acceder a dicha información.

¿De qué manera se desarrolla ese hecho delictivo? Una vez que el agresor elige a su víctima, utilizan MSN Messenger para contactar y hablar con él/ella de una manera más íntima y personal, es decir son conversaciones ya de carácter privado. De esta manera empieza lo que se llama “la seducción”, en la que tratan de engatusar a la víctima para, claramente, obtener material pornográfico infantil, imágenes del menor en poses provocativas o explícitamente sexuales. En un principio lo habitual es que sean fotografías provocativas pero con connotaciones sexuales para, posteriormente, incluso llegar a algún encuentro sexual con el menor.

155

Muchas veces comienza con la otra forma de contacto, que es directamente la amenaza y el chantaje. Esto sucede cuando con el método anterior –el criminal es educado o utiliza muy buenas maneras– no consigue lo que quiere y entonces emplea otras técnicas tales como los lanzadores de exploits, que son virus con los que pueden obtener las contraseñas del correo electrónico de los menores para chantajearlos o recuperar sus cuentas de correos para enviar una fotografía, etc. Eso supone la entrada en un círculo vicioso del que es muy difícil salir, y más para un niño.

Los menores que acceden a ese chantaje lo hacen por miedo a:

- Perder su correo, y con ello el contacto con sus amigos y conocidos
- Ser agredido físicamente. Aunque esto normalmente no suele suceder
- Que difunda las imágenes que ya tiene, desprestigiándolo

El *grooming* tiene unas terribles consecuencias psicológicas en las víctimas.

Ocurre también que las cuentas robadas pasan a ser utilizadas por el agresor para representar más identidades y así conseguir más víctimas. Estos actos se prolongan durante tiempo, e incluso pueden continuar tras la detención del agresor.

En la operación Camaleón de la Brigada de Investigación Tecnológica se identificaron 250 víctimas, y se desconoce si habrá alguna más. El agresor contactaba con ellas a través de las redes sociales votamicuerpo y netlog y disponía de 12 personalidades diferentes, de distintos sexos, según la técnica que en concreto quisiese aplicar con la víctima. Utilizaba estrategias muy elaboradas. Tras su primera detención continuó acosando a las víctimas, lo que provocó un segundo arresto, su juicio y encarcelamiento.

Los hechos que se le imputaron, para que pueda entenderse la gravedad de este tipo de figura, que es bastante compleja porque hace referencia a distintos hechos delictivos, fueron:

- Posesión, distribución y producción de pornografía infantil
- Amenazas y coacciones
- Descubrimiento y revelación de secretos, porque accedía a las cuentas de correo de los menores, se apoderaba de sus contraseñas, accedía a sus contactos y asumía su personalidad
- Suplantación de identidad, para captar nuevas víctimas o bien para desprestigiar públicamente a la primera
- Sustracción de dinero

Cyberbullying

Se trata del acoso escolar, pero con el uso de las nuevas tecnologías adquiere una dimensión diferente, especialmente grave en el sentido de que supone acoso con vejaciones, que ya en el entorno de las nuevas tecnologías agrava incluso más esta circunstancia.

El *cyberbullying* significa intimidar, y se utilizan actitudes agresivas, intencionadas y repetidas, comentarios injuriosos, montajes hirientes, hacia una o varias personas, que ocurren sin motivación evidente, adoptadas por uno

o más estudiantes, pudiendo desembocar, incluso, por su insistencia, en el suicidio.

En el *ciberbullying* la Responsabilidad Penal puede hacer referencia a distintas figuras, desde las lesiones hasta delitos contra la libertad (amenaza, coacción y detención ilegal), la integridad moral, la indemnidad sexual y el honor.

Las medidas preventivas que conviene realizar son controles en esas plataformas para intentar erradicar y evitar la publicación de imágenes de este tipo y, por supuesto, identificar a los autores.

Sexting

Es una figura que con las redes sociales adquiere una dimensión distinta. Es la difusión o publicación de contenidos (fotografías o vídeos) de tipo sexual, producidos por el propio menor, utilizando para ello el teléfono móvil u otro dispositivo tecnológico, a través de e-mail, redes sociales o cualquier otro canal que permitan las nuevas tecnologías. Al reenviarse ese contenido, el usuario pierde el control completo sobre el mismo.

Claramente es un delito contra el honor, la intimidad y la propia imagen, y está muy relacionado con la pornografía infantil.

157

Los motivos por los que hoy en día se producen supuestos casos de sexting son:

- Falta de la cultura privacidad
- No existe una conciencia clara del riesgo por parte de los menores. Desconocen lo que implica subir una imagen, reenviarla y perder el control de la misma, ya que luego es prácticamente imposible retirarla de la Red, y las consecuencias son muy graves, porque podría ser víctima de las conductas anteriores, es decir, del grooming o del cyberbullying
- Esto tiene una relación especial también con la pornografía infantil, en el sentido de que tanto las redes como los foros de pornografía infantil se nutren de este tipo de imágenes, que en esos círculos de nominan “de calidad”, es decir, muy específico, de producción propia
- La adolescencia supone el despertar sexual y puede producirse una sexualización precoz

- La inmediatez de comunicaciones, con la inexistencia de períodos de reflexión

Ya se están produciendo las primera condenas por *sexting*.



Condenado un menor por incitar al sexting con engaños y usarlo para chantajear a varias chicas y parejas 30nov10



El condenado, que en el momento de los hechos (2008) tenía 16 años, fingía representar a una agencia de modelos, y asumía otras identidades falsas para obtener fotos y vídeos de sus víctimas desnudas y en actitudes sexuales. Ha sido condenado a varios meses de realización de tareas socioeducativas relacionadas con la sexualidad. Es la primera sentencia dictada en la Región de Murcia contra un menor como responsable de un delito de *descubrimiento y revelación de secretos* y otros de *prostitución y corrupción de menores*.



El procesado había creado numerosas cuentas de correo electrónico y perfiles en redes sociales diferentes para poder entrar en contacto con chicas menores, jóvenes o parejas usando diversas triquiñuelas.

Así, por ejemplo, contactó con varias menores a las que «*bajo la promesa de un trabajo para la supuesta agencia les solicitaba primero datos personales, como edad o medidas, y finalmente les pedía que posaran ante la 'webcam' desnudas*», tal y como consta en la sentencia. Otras veces chantajeaba a sus víctimas exigiendo que se desnudaran asegurando que disponía de vídeos sexuales de ellas y que los difundiría si se negaban.

158

CONTENIDOS NOCIVOS. ILEGALES/INAPROPIADOS

Hay una serie de contenidos nocivos en la Red que son claramente ilegales –favorecen el racismo, la xenofobia, son sexistas, etc.–, o son inapropiados –páginas de pornografía, violentas, etc.– a las que tienen acceso los menores. Son espacios en los que se publican, por ejemplo, ejecuciones, accidentes, crímenes, etc., o son sites de grupos violentos, *gore* o *snuff*, en las que lo que se ven violaciones, simuladas o reales, se hace apología del tráfico y consumo de drogas, pactos suicidas, sites que favorecen la anorexia o la bulimia. A estos contenidos los menores no deberían de acceder.

COMPORTAMIENTOS ARRIESGADOS

Hay que hacer una especial mención a lo que son los comportamientos arriesgados de los menores en la Red. Ellos revelan información personal:

nombre, apellidos, dirección, teléfono, lugar de residencia habitual, etc., que en el contexto *off-line* no lo harían pero, por esa irresponsabilidad y por esa falta de cultura de la privacidad, acaban mostrando en su perfil una serie de datos sin ser conscientes de los riesgos que conllevan.

También se da la posibilidad de que se produzcan encuentros que sean inapropiados, es decir, que la relación on-line pase a ser un encuentro en la vida *off-line*. En este ámbito de enmarca la operación Ruber de la Brigada de Investigación Tecnológica que, entre otros, llevó a la desarticulación de un grupo criminal organizado que contactaban con menores a través de este tipo de plataformas y, posteriormente, mantenían encuentros en la vida cotidiana. Operaban en toda España, concertando sus encuentros con los menores en hoteles en los que filmaban las relaciones sexuales que mantenían con esos chicos, para, posteriormente, vender ese material. Llegaron a identificarse hasta 17 menores en España y se saldó con 19 detenidos.

ADICCIÓN

Un consumo excesivo de Internet puede derivar en un Desorden de adicción a Internet, cuyos síntomas son el aislamiento y la falta de socialización del menor. Esta adicción se da especialmente a los con los juegos y videojuegos on-line.

159

La herramienta fundamental para evitar todos estos riesgos es, básicamente, la enseñanza y el diálogo. Enseñanza y diálogo que tienen que correr a cargo de los padres, en los que se eduque en los riesgos para evitarlos. El resto son medidas complementarias, como puede ser el filtrado de contenidos, informar sobre el funcionamiento de Internet, así como la posibilidad de señalar contenidos ilícitos o chocantes.

CONCLUSIÓN

La rapidez de las redes sociales en su ascenso y la iniciación temprana que supone por parte de los menores la utilización de éstas, pone de relieve la necesidad de implementar en el sistema educativo una formación sobre el uso responsable de Internet, es decir, que se conozcan todas las posibilidades: sus beneficios y sus riesgos y cómo prevenirlos y/o evitarlos, que los padres sean conocedores de los peligros, que tengan conocimiento del funcionamiento de Internet en sí mismo y adopten las precauciones.



POWERPOINT

CELIA CARREIRA VIGO
Inspectora del Cuerpo Nacional de Policía.
Jefa del Grupo III, de la Brigada de Investigación
Tecnológica, de Protección al Menor

CUERPO NACIONAL DE POLICIA



162



GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

CUERPO NACIONAL DE POLICÍA
REDES SOCIALES







GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

CUERPO NACIONAL DE POLICÍA





- Nueva forma de relación humana haciendo uso de las nuevas tecnologías.
- Fenómeno en constante crecimiento y desarrollo.
- Perfil público



GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

CUERPO NACIONAL DE POLICÍA
REDES SOCIALES





Aplicación online que posibilita compartir información, colaborar en la generación de contenidos y participar de forma espontánea en movimientos sociales y corrientes de opinión.



GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

CUERPO NACIONAL DE POLICÍA



¿Cuál es el motivo de su éxito?

- ☐ Herramienta relacional. Descentralización. Globalización. Interacción ilimitada.
- ☐ Gratuidad, sencillez y rapidez de interconexión.
- ☐ Avance tecnología
- ☐ Fenómeno social y económico





GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

CUERPO NACIONAL DE POLICÍA
Menores y redes sociales:






- ☐ Herramienta básica de identidad y relación
- ☐ Los adultos utilizan Internet. Los jóvenes están en Internet.
- ☐ Instituciones públicas y legislación: mayor grado de protección a menores.
- ☐ Convenio Europeo de Protección de Menores.



GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

CUERPO NACIONAL DE POLICÍA



RIESGOS DE
MENORES ANTE EL
USO DE LAS
REDES SOCIALES




GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

CUERPO NACIONAL DE POLICÍA




CAPTACION DE MENORES CON FINES SEX GROOMING





GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

CUERPO NACIONAL DE POLICÍA




GROOMING

CONSISTE EN ACOSAR A MENORES A TRAVÉS DE INTERNET PARA OBTENER FOTOS O VÍDEOS DE ELLOS DESNUDOS O EN ACTITUDES SEXUALES

APECTA A AMBOS SEXOS POR IGUAL, AUNQUE LOS AGRESORES SON CASI TOTALMENTE HOMBRES.


UTILIZAN TÁCTICAS Y TÉCNICAS SOFISTICADAS PARA CONSEGUIR SUS OBJETIVOS.

NO LES IMPORTA CAUSAR EL DAÑO O LOS TRAUMAS QUE PUEDAN CAUSAR.



GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

CUERPO NACIONAL DE POLICÍA



Captación de menores con fines sexuales



YAHOO! 

GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

CUERPO NACIONAL DE POLICIA

FOTOLOG:

CHATS:

FOTOLOG:

Vota Mi Cuerpo!

VOTAMICUERPO:


[illegible]

CUERPO NACIONAL DE POLICÍA


```
graph TD; A[ENTREGA DE FOTOS Y VIDEOS] --> B[CHANTAJE CON LAS IMÁGENES ENTREGADAS]; B --> A;
```

ENTREGA DE FOTOS Y VIDEOS

CHANTAJE CON LAS IMÁGENES ENTREGADAS



CUERPO NACIONAL DE POLICÍA




ALGUNOS ACCEDEN AL CHANTAJE


Por miedo {

- A perder su correo y con ello, el contacto con sus amigos y conocidos.
- A que la agrede físicamente.
- A que difunda las imágenes que ya tiene.
- A que se haga pasar por ella ante familiares y amigos, desprestigiándola.








Terribles consecuencias psicológicas



CUERPO NACIONAL DE POLICÍA



Las cuentas robadas a sus víctimas pasan a ser utilizadas para representar más identidades a la hora de conseguir más víctimas



Todos estos actos se prolongan meses, incluso años.
En muchos casos sólo acabarán tras la detención.




CUERPO NACIONAL DE POLICÍA



OPERACIÓN CAMALEON

- 250 Víctimas
- Contacto en redes sociales: votamicuerpo y netlog.
- 12 personalidades diferentes, distintos sexos
- Técnicas muy elaboradas
- Continúo acosando tras su detención






GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

CUERPO NACIONAL DE POLICÍA

OPERACIÓN CAMALEON



Hechos:

- Posesión, distribución y producción de PI
- Amenazas, coacciones
- Descubrimiento y revelación de secretos
- Suplantación de identidad
- Sustracción de dinero




GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

CUERPO NACIONAL DE POLICÍA






BULLYING



GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

CUERPO NACIONAL DE POLICÍA




QUÉ ES...

☐ Significa INTIMIDAR.

☐ Actitudes agresivas, intencionadas y repetidas, hacia una o varias personas, que ocurren sin motivación evidente, adoptadas por uno o más estudiantes, pudiendo desembocar, incluso, por su insistencia, en el suicidio.

☐ Acoso con vejaciones + entorno TIC + posible chantaje y amenazas

☐ Tipos: sexual, exclusión social, psicológico y físico.





GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR


CUERPO NACIONAL DE POLICÍA

BULLYING



- Utilización de redes sociales: FB, Tuenti..
- Publicación de imágenes, comentarios injuriosos, montajes hirientes u obscenos, etc.






GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

CUERPO NACIONAL DE POLICÍA

RESPONSABILIDAD PENAL



- De las Lesiones.
- Contra la Libertad: Amenaza, Coacción y Detención ilegal.
- Tortura y contra la Integridad moral: Trato degradante, vejatorio y contra la integridad moral.
- Contra la Libertad e Indemnidad Sexual: Agresiones, Abusos y Acoso sexual, y los delitos relativos a la prostitución y corrupción de menores.
- Contra el Honor: Calumnia e Injuria.

Medidas Preventivas: Control e identificación autores.

Una chica inmigrante se suicida en la EEUU a causa del cyberbullying

05/02/2010 — pantallasamigas

Phoebe Prince, una joven irlandesa de 15 años recientemente emigrada a Massachusetts, se suicidó hace dos semanas tras haber sufrido bullying por Internet en forma de mensajes e emails. Al parecer en alguno de esos mensajes se la induce expresamente a ahorcarse, algo que finalmente hizo. Según la experta Parry Aftab el cyberbullying es equiparable a la tortura para los menores: *Los abusos del patio te pegan y luego te vas a casa, explica. Pero los ciberabusos te pegan en tu casa, en la casa de tus abuelos... en cualquier lugar donde estés conectado/a a la tecnología.*

Según los datos de Aftab, la mayoría de quienes ciberabusan responden al arquetipo de chicas malas, que acosan a otras adolescentes por medio de emails y redes sociales. Una pista sobre un posible cyberbullying la da precisamente un cambio repentino de actitud hacia la tecnología en menores que habitualmente son entusiastas de los juegos online, Facebook, etc.

El mejor consejo en esos casos, según Aftab, es **parar** (de leer los mensajes insultantes), **bloquear** (al abusón) y **contar** (lo que sucede a los padres u otros adultos que puedan ayudar).

En la actualidad 42 Estados de los EEUU tienen algún tipo de medida anti-bullying, 23 de ellos legislaciones específicas. Pero Massachusetts no es uno de ellos.

El caso de Phoebe recoge muestras de especial crueldad, pues el incesante acoso que padeció en vida ha continuado incluso en una página de recuerdo que se le ha hecho en Facebook donde los administradores han tenido que borrar mensajes insultantes que continuaban llegando.



CUERPO NACIONAL DE POLICÍA

SEXTING:

Difusión o publicación de contenidos (fotografías o videos) de tipo sexual, **producidos por el propio remitente**, utilizando para ello el **teléfono móvil u otro dispositivo tecnológico**, a través de e-mail, redes sociales o cualquier otro canal que permitan las nuevas tecnologías.

D. Contra honor, imagen e intimidad.
Voluntariedad- 3º- reenvío masivo


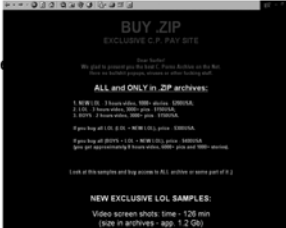
CUERPO NACIONAL DE POLICÍA

MOTIVOS:

- ☐ falta de cultura privacidad
- ☐ no conciencia del riesgo
- ☐ adolescencia, despertar sexual y sexualización precoz
- ☐ inmediatez de comunicaciones: inexistencia de período de reflexión

CONSECUENCIAS:

Aumento riesgo de grooming y bullying
Relación con P.I. (redes y foros de PI se nutren de estas imágenes)
Menor productor



GOBIERNO DE ESPAÑA

MINISTERIO DEL INTERIOR




Condenado un menor por incitar al sexting con engaños y usarlo para chantajear a varias chicas y parejas 30nov10

El condenado, que en el momento de los hechos (2008) tenía 16 años, fingía representar a una agencia de modelos, y asumía otras identidades falsas para obtener fotos y vídeos de sus víctimas desnudas y en actitudes sexuales. Ha sido condenado a varios meses de realización de tareas socioeducativas relacionadas con la sexualidad. Es la primera sentencia dictada en la Región de Murcia contra un menor como responsable de un delito de descubrimiento y revelación de secretos y otros de prostitución y corrupción de menores.

El procesado había creado numerosas cuentas de correo electrónico y perfiles en redes sociales diferentes para poder entrar en contacto con chicas menores, jóvenes o parejas usando diversas triquiñuelas.

Así, por ejemplo, contactó con varias menores a las que «bajo la promesa de un trabajo para la supuesta agencia les solicitaba primero datos personales, como edad o medidas, y finalmente les pedía que posaran ante la 'webcam' desnudas», tal y como consta en la sentencia. Otras veces chantajeaba a sus víctimas exigiendo que se desnudaran asegurando que disponía de vídeos sexuales de ellas y que los difundiría si se negaban.





GOBIERNO DE ESPAÑA

MINISTERIO DEL INTERIOR



CUERPO NACIONAL DE POLICÍA

CONTENIDOS NOCIVOS: Ilegales / Inapropiados



GOBIERNO DE ESPAÑA

MINISTERIO DEL INTERIOR

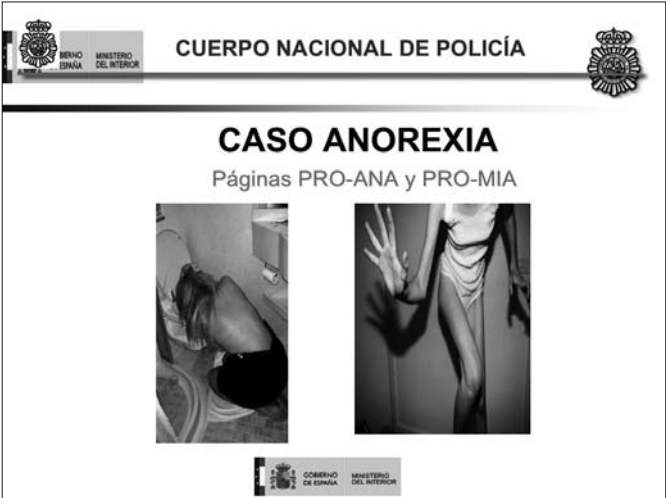
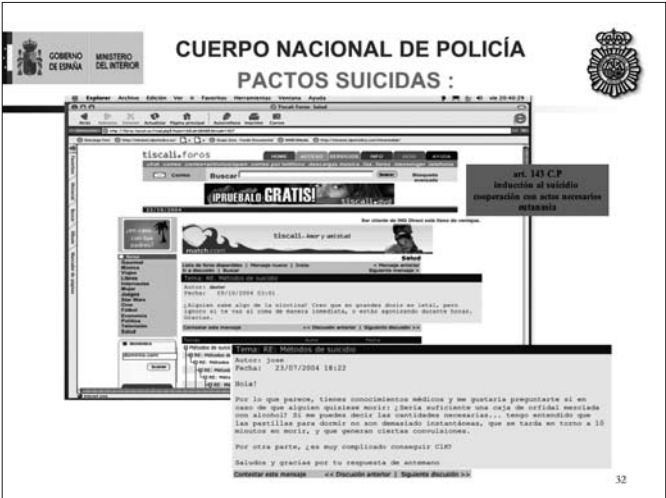



CUERPO NACIONAL DE POLICÍA

EJECUCIONES, ACCIDENTES, GUERRA, CRIMENES:











GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

CUERPO NACIONAL DE POLICÍA



☐ Revelación de información personal

☐ Encuentros inapropiados






Cesión de los derechos de propiedad intelectual de los contenidos publicados, incluyendo textos, imágenes, videos, etc.

YouTube - Broadcast Yourself

Denuncia

Porografía infantil



5. Your Use of Content on the Site

In addition to the general restrictions above, the following restrictions and conditions apply specifically to your use of content on the YouTube Website:

A. The content on the YouTube Website, except all User Submissions (as defined below), including without limitation, the text, software, audio, graphics, photos, videos, music, images, interactive features and the like, is the property of YouTube and its licensors. All rights in the content on the YouTube Website are reserved to YouTube and its licensors. All rights in the content on the YouTube Website are reserved to YouTube and its licensors. All rights in the content on the YouTube Website are reserved to YouTube and its licensors.

B. You may access User Submissions for your information and personal use only as intended through the product functionality of the YouTube Website. You shall not copy or download any User Submission unless you see a "Download" or similar link displayed for YouTube on the YouTube Website for that User Submission.

C. User Comments are made available to you for your information and personal use only as intended through the normal functionality of the YouTube Website. User Comments are made available "as is," and may not be used, copied, reproduced, distributed, transmitted, or otherwise used in any way without the prior written consent of the respective owner. YouTube reserves all rights not expressly granted in and to the Website and the Content.



GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

CUERPO NACIONAL DE POLICÍA

OPERACIÓN RUBER



Desarticulación de red de pederastas.

Abuso sexual y posesión, distribución, producción PI


Agravante de beneficio económico

17 menores identificados

19 detenidos








GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR


CUERPO NACIONAL DE POLICÍA



☐ Riesgos:


- Redes pedofilia
- Intromisión ilegítima intimidad, honor y propia imagen
- Robo datos personales
- Suplantación de identidad
- Fraudes...

174



GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

CUERPO NACIONAL DE POLICÍA



ADICCIÓN:
CONSUMO EXCESIVO




GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

CUERPO NACIONAL DE POLICÍA

VIDEOJUEGOS ON LINE








GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

CUERPO NACIONAL DE POLICÍA



PREVENCIÓN:





1. Enseñanza y diálogo

2. Control parental.

3. Información del funcionamiento de Internet.



lícitos o





GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

CUERPO NACIONAL DE POLICÍA



CONCLUSIONES:

- ☐ Formación sobre el uso responsable de Internet.
- ☐ Conocimiento de posibilidades y peligros.
- ☐ Adopción de precauciones.
- ☐ Internet como en la vida: Sentido común



PROTEGER A LOS MENORES EN LAS REDES SOCIALES

JORGE VILLAMAYOR IBÍAS
Inspector del Cuerpo Nacional de Policía.
Jefe del Grupo de Delitos Tecnológicos de la Brigada Provincial
de la Policía Judicial de Madrid

177

Las redes sociales no son algo nuevo sino que son una derivación de Internet: primero aparece ésta, se expande y, como consecuencia de esa propagación, llegan las redes sociales, aproximadamente en el año 2000. En 2004 nace Facebook, en principio como una plataforma para conectar estudiantes universitarios, en 2006 se inaugura Twitter y en 2012 Facebook se prepara para entrar en el mercado bursátil.

Según el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI) en referencia a las redes sociales:

- El 72 por ciento de los usuarios de Internet tienen su perfil, al menos, en una red social (usuarios en general y desde los 12 años)
- España ocupa el tercer puesto en el ranking mundial de usuarios
- El 29 por ciento de los usuarios se conectan a diario, el 18 por ciento una vez por semana y el 7 por ciento una vez al mes
- Las personas entre 18 y 34 años son las que más asiduamente las utilizan

- El 29 por ciento acceden desde su móvil. Ya no es a través del PC o del portátil, lo que implica una serie de innovaciones
- Al 74,8 por ciento de los usuarios no les preocupa lo que otros vean o piensen de ellos en las redes sociales. Esto es una consecuencia más de la mutación de las características sociales, de la intimidad. Lo que las personas hasta cierta edad cuidaban (el domicilio, el número de teléfono) la juventud lo cuelga sin ningún pudor en su perfil

CAMBIOS SOCIALES

La llegada de las redes sociales ha aportado una serie de cambios en la sociedad:

- Disminución de las relaciones sociales físicas y aumento de las relaciones on-line

Los jóvenes se reúnen y hablan entre ellos a través del móvil, con lo que la comunicación no verbal que nos aporta una relación física desaparece cuando pasamos a la Blackberry o al PC. Es la sociedad que nos ha tocado vivir

- Aislamiento físico

En el momento en que el niño o el joven se encierran en su habitación y es prioritario tuitear o entrar en el Messenger, en lugar de jugar con las muñecas o al balón, el aislamiento físico va a existir

- Mayor egocentrismo
- Conductas asociales
- Pérdida valores intimidad

Se da por las mismas circunstancias. Son conductas asociales. Es una pérdida de valores que viene como consecuencia de la disminución de ese contacto físico entre niños, adolescentes y mayores. Y la pérdida de valores de la intimidad, lo que con anterioridad señalaba.

USUARIOS DE LAS REDES SOCIALES

Facebook, Twitter, LinkedIn, Google + tienen millones de usuarios. ¿Esto va a ser siempre así? Considero que es probable que no y que puede que las



179

redes sociales hayan tocado techo, que dejen de ser un mecanismo de intercambio de opiniones entre jóvenes o adultos, porque la tecnología avanza muy rápidamente y estos sites han tenido su momento.

Considero que la redes sociales serán utilizadas a partir de ahora por políticos, por personajes con relevancia pública, para expresar sus opiniones, para darse a conocer, etc., pero que dejarán de ser un mecanismo de comunicación entre particulares. Por ejemplo, Whatsapp ofrece las mismas prestaciones que una red social y sin embargo se lleva encima y es gratis.

LAS REDES SOCIALES Y LA INVESTIGACIÓN DE DELITOS

En primer lugar, la infracción penal viene determinada por el texto del mensaje, que puede ser:

- Injurioso/calumnioso

- Amenazante
- Vejatorio

Y debe entenderse que ha de existir una mínima posibilidad de que la amenaza, el mal pueda llegar a cumplirse, se precisa que exista una extralimitación del derecho a la libertad de expresión. Evidentemente, si es una amenaza física el agresor sí tiene la posibilidad de agredir o de matar o de cumplir el mal. Por Internet es un poco más difícil, suele quedar siempre en faltas.

Aparte del texto del mensaje, una segunda posibilidad es la forma de acceder. Hoy día está ya plenamente tipificado como delito el descubrimiento y revelación de secretos.

180 En el caso de Facebook, los datos de los que dispone la policía para contactar con esta empresa son los que hay en cualquier base de datos pública, y a la que puede acceder todo el mundo: Facebook Inc. Menlo Park. California. Estados Unidos. Facebook se somete a la legislación del Estado norteamericano de California. Tanto esta red como Twitter, consideran que los datos que tienen se someten a la legislación del Estado donde se conservan, que es en California. Lo que debería ser es que se rigiesen por la normativa del estado y/o nación donde esa información se genera. Una comunicación, una intrusión o un comentario injurioso realizado en Twitter o en Facebook en España, debería estar sometido a la legislación del estado español. Estas empresas consideran que no, y de momento nadie les ha dicho lo contrario.

Ante esto, las dificultades a las que se enfrentan los Cuerpos y Fuerzas de Seguridad del Estados son:

Estas redes sociales no tienen representantes legales en España, nadie que pueda responder y/o colaborar con la policía, que tienen que contactar con ellos a través de un correo electrónico y un formulario y les responde una máquina pasados 3 o 4 meses con información obsoleta.

Se ubican en California porque para facilitar datos requieren el principio de Doble Incriminación, es decir, que el delito por el que se piden los datos lo sea en España y también en Estados Unidos, lo que implica que hay que abrir un procedimiento penal en USA para determinar que efectivamente ahí hay una infracción. Una vez que se establece que hay delito, ya enviarán la respuesta que la policía le ha solicitado, y pueden pasar dos años. El problema de ello es que la Ley 25/2007 obliga a los ISPs (los proveedores de servicios de Internet: Movistar, Orange, etc.) a guardar los datos un año desde que han

sido generados, con lo que al remitir la respuesta, más de un año después, Facebook o Twitter ya no tienen esos datos, de modo que, si no hay otros medios de investigación, el delito ha quedado impune.

Si existe la posibilidad de que atiendan rápido en casos extremos: catástrofes, atentados terroristas, supuestos gravísimos, pero lo que es el día a día, las necesidades del ciudadano de a pie, de que a su hijo le están molestando, de que le han robado la cuenta de correo, son para estas redes delitos menores a los que no le prestan ni la menor atención. Con lo cual se están produciendo unos problemas gravísimos para perseguir estos delitos.

Ante esto, la policía trabaja en lo que llaman la investigación tradicional, es decir, nadie roba, insulta o veja por gusto, por regla general. En este tipo de casos, de relaciones personales, de amenazas, siempre hay una persona, el denunciante, que sospecha de alguien en concreto. Lo que no da la investigación tecnológica se puede obtener por el otro medio, aunque suele acarrear una acumulación de indicios. La investigación tecnológica, aunque lenta, es definitiva, acredita fehacientemente que un mensaje de correo electrónico se ha enviado desde este ordenador en concreto y el titular de este ordenador es fulanito. Es prueba irrefutable.

Tuenti en cambio tiene sede en España y colaboran al cien por cien con los Cuerpos y Fuerzas de Seguridad. Se han resuelto situaciones bastante graves cuando se trataba de asuntos de Tuenti. Ha sido llegar, pedir y al día siguiente tener la contestación.

En el caso de Google, aunque supuestamente tiene sede en España, en Madrid, estos representantes están únicamente para gestionar los beneficios económicos obtenidos en la Península Ibérica. Tras la intervención del juez de la Audiencia Nacional, Eloy Velasco Núñez, Google colabora más con la policía. Aun así, cuando se investiga un correo electrónico, por ejemplo Hotmail -Microsoft es el representante legal de Hotmail en España-, Microsoft aporta con una orden judicial, evidentemente, lo que necesitamos, pero en el caso de un correo electrónico de Google -Gmail-, hay que obtener una doble orden judicial, para la cabecera técnica del correo electrónico y para que Google abra esa cabecera en su totalidad.

ACTIVIDADES DE LOS MENORES EN LAS REDES SOCIALES

En este entorno, los jóvenes escriben sus ideas, sus pensamientos, sus vivencias diarias, sus preferencias, agregan a sus amigos (cuantos más amigos tengas más popular eres) suben las fotos del fin de semana, reuniones con amigos, etc.

Recomendaciones a los menores en las redes sociales:

En este supuesto de relación entre padres e hijos evidentemente lo que prima es la confianza del menor hacia los progenitores. Si hay una relación fluida entre padres e hijos todo irá sobre ruedas. Si hay reticencias, si hay problemas de comunicación posiblemente salte algún tipo de problema.

- La información personal que se pone en el perfil pasa a ser de todos. Esto es algo que los chavales no tienen suficientemente claro. En el momento que incorporas algo a Internet, dejas de ser dueño de él y hay un efecto multiplicador enorme
- Si subes una foto pueden capturarla para otros fines. La mayor parte de los autores del *grooming* son gente de 30 a 50 años. Evidentemente, si ponen su imagen no van a conseguir captar víctimas, de modo que capturan la de un chaval de 15 o 16 años. No hace falta ser ingeniero informático para ello, basta tener unos conocimientos mínimos a nivel de usuario, simplemente una captura de pantalla y listo
- Si se pone el nombre completo lo pueden asociar a esa foto
- Hay que evitar poner datos exactos de domicilio o lugares frecuentes
- Las ideas que se publican pueden ser criticadas

Recomendaciones para los jóvenes:

- Hay que aceptar como amigo solo a quien se conoce en la vida real
- Si al niño le amenazan, intimidan o insultan, debe decírselo a sus padres y no callarlo. Si el niño tiene confianza, tiene una relación fluida con sus padres, se lo va a decir. Si hay problemas, se lo va a callar. Y, al final, la doble víctima va a ser el niño
- Hay que configurar los perfiles sólo para que los vean los amigos
- El ordenador y el móvil son una parte en la vida del niño, pero no pueden ser su vida

RECOMENDACIONES DIRIGIDAS A LOS PADRES:

- La habitación del menor no es un buen lugar para instalar los ordenadores, mejor una zona común de la casa. Dejar al niño aislado en su habitación con su ordenador es dejarlo en la soledad frente a un problema. Si le están amenazando, si está siendo víctima de un *grooming*, esa habitación para el niño es un infierno
- Hay que controlar, no espiar lo que el niño hace con el ordenador. Hay que aprovechar los controles parentales que ofrecen los sistemas
- Tiene que haber una relación relacional entre la edad del menor y sus actividades tecnológicas. ¿Tiene necesidad un niño de 10 años de tener un perfil en Facebook o un teléfono móvil?



POWERPOINT

JORGE VILLAMAYOR IBÍAS
Inspector del Cuerpo Nacional de Policía.
Jefe del Grupo de Delitos Tecnológicos de la Brigada Provincial
de la Policía Judicial de Madrid



CUERPO NACIONAL DE POLICÍA

**B.P.P.J. MADRID - GRUPO VIII
(DELITOS TECNOLÓGICOS)**



185

REDES SOCIALES Y LA NUEVA DIMENSIÓN DE SEGURIDAD

PROTEGER A LOS MENORES EN LAS REDES SOCIALES

EL ESCORIAL, 10 de julio de 2012



NUESTRAS COMPETENCIAS

CNP

• INVESTIGACIÓN DE DELITOS COMETIDOS MEDIANTE EL USO DE LAS NUEVAS TECNOLOGÍAS, EN ESPECIAL INTERNET:

- Fraudes on line y FUT.
- Pornografía de menores.
- Child grooming.
- Sexting.
- Emisión de informes técnicos sobre estas materias.

* AMBITO TERRITORIAL: Comunidad de Madrid

2



NOTAS INTRODUCTORIAS

CNP

• LAS REDES SOCIALES SON UN "MODELO DE UTILIDAD" CUYA "PATENTE" SERÍA INTERNET.

- SURGEN COMO CONSECUENCIA DE LA EXPANSIÓN DE INTERNET (año 2000).
- AÑO 2004: SE LANZA FACEBOOK como una plataforma para conectar a estudiantes universitarios.
- Año 2006: se inaugura TWITTER.
- Año 2012: Facebook se prepara para entrar en el mercado bursátil.

3



ESTUDIO SOBRE LAS REDES SOCIALES EN ESPAÑA (*ONTSI)

CNP

• El 72% de usuarios de Internet tienen perfil en al menos una red social.

- España ocupa el tercer puesto en el ranking mundial de usuarios en RS.
- El 29% de usuarios de RS se conectan a diario, el 18% una vez por semana y el 7% una vez al mes.
- Las personas entre 18 y 34 años utilizan las RS más asiduamente.
- El 29 % de usuarios acceden a las RS a través de su móvil.
- El 74,8 % de usuarios no les preocupa que otros vean o piensen de ellos en las RS (mutación del concepto de intimidad)

* Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información.

4



CAMBIOS SOCIALES

GNP

- ◆ DISMINUCIÓN DE LAS RELACIONES SOCIALES FÍSICAS Y AUMENTO RELACIONES ON LINE.
- ◆ AISLAMIENTO FÍSICO.
- ◆ MAYOR EGOCENTRISMO.
- ◆ CONDUCTAS ASOCIALES.
- ◆ PÉRDIDA VALORES INTIMIDAD.

5



USUARIOS RR SS

GNP

	Mundo: 800 España: 15	Millones de usuarios de redes sociales	FACEBOOK
	Mundo: 200 España: 4,5'		TWITTER
	Mundo: 135 España: 2		LINKEDIN
	Mundo: 65		GOOGLE PLUS
	Mundo: 12,5		TUENTI

6



LAS REDES SOCIALES Y LA INVESTIGACIÓN DE DELITOS

GNP

- LA INFRACCIÓN PENAL VIENE DETERMINADA POR EL TEXTO, QUE PUEDE SER:
 - INJURIOSO/CALUMNIOSO.
 - AMENAZANTE.
 - VEJATORIO.
 - (...)

- SE PRECISA QUE EXISTA UNA EXTRALIMITACIÓN DEL DERECHO A LA LIBERTAD DE EXPRESIÓN.

7






Technical Contact, Zone Contact:
Domain Administrator
Facebook, Inc.
1601 Willow Road
Menlo Park CA 94025
US
domain@fb.com +1.6505434800 Fax: +1.6505434800

SE SOMETEN A LA LEGISLACIÓN DEL ESTADO DE CALIFORNIA
NO TIENEN REPRESENTANTES LEGALES EN ESPAÑA.
SE EXIGE REQUISITO DE LA DOBLE INCRIMINACIÓN.
SE CONTACTA CON ELLOS MEDIANTE EL ENVÍO DE UN FORMULARIO QUE CONTESTA UNA MÁQUINA.




Tech Name..... Tech Admin
Tech Address..... 795 Folsom Street
Tech Address..... Suite 600
Tech Address..... San Francisco
Tech Address..... 94107
Tech Address..... CA
Tech Address..... UNITED STATES
Tech Email..... domains-tech@twitter.com

SOMETIDO A LA LEGISLACIÓN DE CALIFORNIA.
PRINCIPIO DE DOBLE INCRIMINACIÓN.
TENEMOS UN N° DE FAX... Y POCAS RESPUESTAS.

dnsmaster@tuenti.com
Plaza de Las Cortes, 2, 4 planta
Madrid Madrid
28014 ES
+34 914294039 fax:+34 913694438



ACTIVIDAD DE LOS MENORES EN LAS RS



- ♦ ESCRIBEN SUS IDEAS Y PENSAMIENTOS.
- ♦ SUS VIVENCIAS DIARIAS.
- ♦ SUS PREFERENCIAS.
- ♦ SUS AMIGOS.
- ♦ SUBEN LAS FOTOS DEL FIN DE SEMANA Y REUNIONES CON AMIGOS.

11



RECOMENDACIONES A MENORES EN EL USO DE RS



- ♦ LA INFORMACIÓN PERSONAL QUE PONGAS EN TU PERFIL PASA A SER DE TODOS.
- ♦ SI PONES TU FOTO, PUEDEN CAPTURARLA PARA OTROS FINES.
- ♦ SI PONES TU NOMBRE COMPLETO PUEDEN ASOCIARLA A TU FOTO.
- ♦ EVITAR PONER DATOS EXACTOS DE DOMICILIO Y LUGARES FRECUENTES.
- ♦ SI PUBLICAS TUS IDEAS, PUEDEN SER CRITICADAS.

12



RECOMENDACIONES A MENORES EN EL USO DE RS



- ♦ ACEPTA COMO AMIGOS SOLO A QUIEN CONOZCAS EN LA VIDA REAL
- ♦ SI TE AMENAZAN, INTIMIDAN O INSULTAN, DÍSELO A TUS PADRES Y NO TE LO CALLES.
- ♦ CONFIGURA TUS PERFILES PARA QUE SOLO TUS AMIGOS PUEDAN VER LO QUE PUBLICAS.
- ♦ EL ORDENADOR Y EL MÓVIL SON UNA PARTE DE TU VIDA, PERO TU VIDA NO PUEDE SER EL ORDENADOR Y EL MÓVIL

13



RECOMENDACIONES A LOS PROGENITORES

CNP

- LA HABITACIÓN DEL MENOR NO ES UN BUEN LUGAR PARA INSTALAR LOS ORDENADORES. MEJOR UNA ZONA COMÚN DE LA CASA.
- NO "ESPIAR" LO QUE EL NIÑO HACE CON EL ORDENADOR.
- APROVECHAR LOS CONTROLES PARENTALES QUE OFRECEN LOS SISTEMAS.
- RELACIÓN RACIONAL ENTRE LA EDAD DEL MENOR Y SUS ACTIVIDADES TECNOLÓGICAS.
- EN EDADES INFERIORES, EL NIÑO NO PUEDE NAVEGAR POR INTERNET SIN QUE UN ADULTO ESTÉ A SU LADO.
- CUANTO MÁS FLUIDA SEA LA RELACIÓN PATERNO FILIAL, MENOS PELIGROS PARA EL MENOR EN LA RED... SI LE AMENAZAN, COACCIONAN O VEJAN, NOS LO CONTARÁ.

14



CONTACTO GRUPO VIII

CNP

- Av. Dr. Federico Rubio y Galí 55, 28040 Madrid
- madrid.bppj8@policia.es
- Tf. 91 3223583-4
- Fax 91-3223421



15



TERCER PANEL

REDES SOCIALES Y NUEVAS FORMAS DE DELINCUENCIA

MANUEL VÁZQUEZ LÓPEZ

**Comisario Principal del Cuerpo Nacional de Policía.
Jefe de la Brigada de Investigación Tecnológica de la UDEF Central**

La globalización que representa Internet la personifica también el delito cuando se comete a través de la Red. Si actualmente la delincuencia organizada tiene entre sus características la deslocalización, la ubicación por diferentes países y unas estructuras muy abiertas, en la ciberdelincuencia esto es paradigmático, y es corriente que en cualquier operación el delincuente esté en un país, las víctimas en otro y los servidores en un tercero, con lo que la investigación se vuelve muy compleja.

193

El número y target de víctimas al que se pueden dirigir los ataques es inmenso. Se cifra en 7.000 millones de dispositivos conectados a la Red, la mayoría ordenadores. Con la llegada de los dispositivos móviles: *smartphones*, tabletas, se multiplica el número de potenciales perjudicados quiénes, además, pueden estar conectados en todo momento y en cualquier lugar.

Todo tipo de delincuentes utilizan Internet y encuentra en ella nuevas formas de información. Existen foros, más o menos clandestinos, donde estas personas van ganando confianza y en donde se intercambian, compran, venden datos sobre diferentes temas relacionados con el delito, desde números de tarjetas, crédito, herramientas o todo tipo de instrumentos para que una persona, no excesivamente experta, pueda cometer delitos.

A eso se une el anonimato, que proporciona el acceso desde el sitio más simple, por ejemplo un cibercafé, o redes virtuales en las que el perfil se ad-

quiere, por poco dinero, sistemas de descifrado... Son mil formas de lograr no ser descubierto que hacen muy difícil detectar a las personas que comete el delito.

También hay que distinguir entre la delincuencia propia de Internet, la que se comete porque existe la Red, en la que la tecnología es fundamental, y los delitos de toda la vida que han encontrado en la Web un nuevo escenario y que es, simplemente, otra forma de cometer las mismas fechorías.

El Convenio de Cibercriminalidad del Consejo de Europa de 2001 estructuró los delitos que se cometen en Internet en:

- De contenidos: cuando se refiere a pornografía infantil y contenidos ilícitos
- De fraude
- Infracciones a la propiedad intelectual
- De *hacking*: son los relacionados con ataques a los datos y a los sistemas de Internet

194

Las redes sociales son unas estructuras compuestas por multitud de personas que se relacionan por intereses, por temas, por parentesco, etc. Hay infinidad de ellas, y entre las más utilizadas en España están: Twitter, Facebook, Tuenti, Badoo, Meeting, y las destinadas a los adolescentes, como Fotolog, Vota mi Cuerpo, etc...

Las jóvenes viven en las redes sociales, en lugar de estar en el parque o en el colegio jugando, los chavales están allí, con un gran número de aplicaciones desplegadas. Las redes ya son objeto de análisis científico en universidades, y sobre cómo van a evolucionar nadie lo sabe. Por ejemplo, en la actualidad se ve que están incorporando aplicaciones nuevas para no quedarse colgadas, porque en esto de las empresas tecnológicas, una decisión estratégica mal tomada puede llevar a una empresa a la ruina en poco tiempo porque alguien le sustituye en su negocio. Por ahora se ve que ese avance camina hacia la afiliación de app's que se adaptan a las necesidades de la gente que se va sumando.

Las redes sociales facilitan a todo tipo de organizaciones, incluida afortunadamente la Policía, cierta utilidad para las investigaciones, por ejemplo, permiten detectar por dónde se va a concentrar la gente, dónde va a haber manifestaciones, dónde pueden producirse problemas, con lo que colabora

con los agentes para garantizar la seguridad de los manifestantes y la del resto de los ciudadanos. La Policía Nacional tiene abiertos perfiles en: Facebook, Twitter –éste lo gestiona el Servicio de Prensa– y Tuenti, y desde ahí se publican alertas tecnológicas, recomendaciones, etc. Existe una interacción es positiva.

Actualmente, hay un gran número de herramientas que permiten despachar cualquier tipo de cuestiones de influencia en las redes sociales. Hay empresas dedicadas a influir, a crear una imagen de una determinada persona en la red, a seguir y analizar lo que en Internet se dice de una empresa, es decir, una organización puede tener información que le permita dirigir su camino en función de lo que se diga, de la imagen que tiene. Incluso ha surgido la figura del gestor de redes sociales, que administra estos canales. Han surgido nuevas profesiones dedicadas a este sector.

Facebook tiene 900 millones de usuarios, y aunque muchos pueden ser perfiles dobles, muertos, dormidos, etc., son 500 millones los acceden todos los días, y se suben 250 millones de fotos cada jornada. Twitter tiene 300 millones de usuarios, Tuenti 12 millones, y la red de contactos Badoo 150 millones, de los cuales en torno al 5 por ciento están en España. Eso también indica que la forma de relacionarse está cambiando, y el mapa del mundo según Facebook es ya un icono que se ve en muchas habitaciones de adolescentes.

195

Según un estudio del Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI) sobre redes sociales, entre los 15 y 20 años los chicos están “enganchados” a la Red todo el día, a partir de esa edad el uso va decreciendo. En esa etapa es importante el tema de los amigos, Robin Dunbar explica que más de 150 personas es difícil de gestionar en la Red, y esto es algo que se ve de forma habitual en los perfiles de los adolescentes. Es ahí donde se pueden “meter” muchas personas, en el caso de los menores, depredadores sexuales que utilizan Internet para entrar en contacto con ellos.

Es clave el también el papel que las redes han tenido en los movimientos de la Primavera Árabe (2010-2013). En el caso actual de Siria, las personas suben y envían vídeos y fotos, información que al resto le llega de forma directa. Se puede decir que han cambiado hasta el concepto, digamos, del periodismo clásico.

En las redes también se producen delitos, faltas, problemas relacionados con la intimididad, calumnias, injurias, amenazas, suplantación de perfiles. En este último caso, suplantar un perfil en sí mismo no tiene entidad pe-

nal si no es para injuriar o para cometer cualquier otro tipo de delito. Esto es, básicamente, uno de los mayores problemas en los delitos que se comenten.

En los delitos en los que están involucrados los menores y que se cometen en Internet, ellos son a veces infractores y a veces víctimas, porque el adolescente está utilizando Internet y tiene la sensación de que eso es impune, no tiene claro que las cosas que se cometen ahí sean delitos. Hay que educar a los jóvenes que lo que no se hace en el mundo real tampoco se puede hacer en Internet.

196 En la Red los menores aprenden muchas cosas. Hay muchas páginas, por ejemplo de *hacking*, donde un menor aprende fácilmente a *hackearle* la cuenta de correo a su compañera y lo toma como un juego, no le da demasiada importancia. Y también aprende que se puede defraudar fácilmente, por ejemplo con una página de recargas de móviles. Esto sirve para banalizar el delito y crear una cultura del “Gratis total”. Ésta está relacionada con el problema de los derechos de propiedad intelectual. En muchos países, entre ellos España, la sensación de que todo lo que está en Internet (películas, libros, vídeos, etc.) tiene que ser gratis necesariamente lleva a que, entre otros temas, existan listas negras de piratería. Desde el ámbito policial, el delito contra la propiedad intelectual está tipificado en el artículo 270 del Código Penal y exige ánimo de lucro y comunicación pública de una obra protegida por derechos de propiedad intelectual.

Las páginas donde se pueden descargar este material cultural son, básicamente, *sítes* con enlaces que redirigen a un servidor distinto de la página, pero ésta sí necesita mantenimiento (colocar los enlaces, administrarlos, subir contenidos, etc...). El resultado de las investigaciones sobre estos delitos es que los pronunciamientos judiciales son distintos unos de otros, en unos casos el juzgado ha archivado y en otros ha habido condenas.

En las investigaciones en las que se acreditó ánimo de lucro superior a 100.000- 120.000 euros anuales, obtenido mediante publicidad de empresas legales que comercializaban artículos relacionados con la informática, las sentencias judiciales eran contradictorias por los mismos hechos.

En 2011 se aprobó la llamada Ley Sinde, que deriva estos temas en un procedimiento administrativo. Hay una comisión que ante una denuncia abre un expediente administrativo y, en caso de no retirar la web se eleva

a una sala de lo Contencioso. Es probable que sólo los temas más graves lleven a la intervención policial.

Sobre el tema de la responsabilidad de los menores en Internet, ha habido algunos ejemplos como el de dos chicas que fueron multadas con 12.400 euros por crear un perfil falso en Tuenti que utilizaban para injuriar y amenazar a terceros.

Existen también un gran número de webs con contenidos que son inapropiados para menores y que es difícil de encajar en ningún tipo penal, por ejemplo: anorexia (la Brigada de Investigación Tecnológica realizó una larga investigación que dio como resultado que las páginas alojadas en España si se cerraron, pero no las que estaban ubicadas en otros países), bulimia, que hacen apología del sufrimiento, de ejecuciones, de atentados, de fusilamientos, que muestran cómo cortar el cuello a alguien, que simulan asesinatos, violaciones, tratan sobre drogas, enseñan cómo suicidarse etc. Un menor puede visualizar estos temas en cualquier momento del día y llegar a banalizarlo y pensar que eso es lo normal. A eso se unen juegos demenciales, como el que consiste en matar ancianos, y cuántos más se maten más puntos se obtienen.

En el contexto de las redes sociales los datos son claves, y los menores se prodigan en darlos. Un dato de por si no aporta nada, pero si se relaciona con otros se puede crear un perfil al que luego se unen fotos, y esas instantáneas, a través del dispositivo con las que se han hecho, se pueden geolocalizar y conocer donde están sacadas. Con todo ello se puede identificar al usuario de internet y utilizarlo para enviarle publicidad. El negocio de las empresas de Internet que son gratuitas son los datos de los usuarios.

Además, esos datos van a permanecer en la Red, pues es muy difícil, casi imposible, que desaparezcan. Por ejemplo, aunque Facebook retire una foto de un perfil, esa imagen la tienen un gran número de usuarios que pueden publicarla cuando quieran. Además, con ciertas herramientas que hay en las redes sociales con fuente abiertas se pueden construir perfiles de personas que se emplean para todo: una empresa de contratación laboral, seguros médicos, etc.

NUEVAS FORMAS DE DELINCUENCIA Y FUTURAS AMENAZAS

El cibercrimen se realiza desde el anonimato, se puede dirigir a millones de personas, no hay más que tener en cuenta el dato ya indicado de que existen 7.000 millones de dispositivos móviles conectados, y ataca a

sus víctimas de mil formas diferentes –correos desde la Agencia Tributaria, el banco, una chica rusa que dice que va a venir a España y pide que le envíen 500 euros–, estafando a muchos con cantidades no muy elevadas en lugar de a unos pocos con grandes sumas. Algunos análisis cifran en 300.000 millones de euros anuales el coste del cibercrimen, y la asociación mundial encargada de evaluar estos riesgos lo ubica en el tercer lugar, valorado como amenaza global de cara al futuro.

Los delitos o hechos que se dan en el mundo real y que, por su equivalencia, pueden verse en la ciberdelincuencia son, por ejemplo: cuando una persona sella una cerradura con silicona es comparable con el bloqueo de una página, como hace el grupo Anonymous; el robo con intimidación se puede comparar con el *ransomware*; el tocomucho con las nigerianas; las pintadas en la pared con el *deface*; el sabotaje a una industria con el gusano *stum*; y el espionaje industrial por otro *malware* o troyanos.

198 La actividad del crimen organizado en Internet está en manos de grupos que tienen una gran infraestructura, aunque luego hay otro conjunto de amenazas relacionadas con el *hacktivismo*, el *hacking* político. En el año 2006 se produjo el primer ataque documentado de negación de servicios, fue en Estonia y los agresores colapsaron su Administración. En la investigación que se realizó se determinó que los ataques procedían de Rusia. ¿Ciberterrorismo? Pues no, porque no proviene de una organización terrorista, pero es lo que se puede incluir dentro de lo que es el *hacking* patriótico. En cambio, en los conflictos que se produjeron entre Georgia y Rusia por Osetia del Sur y en donde se llevó a cabo otro ataque de negación de servicios a Georgia, sí hubo intervención de tropas rusas y se habla del primer conflicto de guerra física y ciberguerra.

Éstos son problemas que ya tienen los países y a los que se han de enfrentarse los servicios de inteligencia. El nivel de complejidad de los ataques de Internet es cada vez mayor, y en la actualidad se producen gusanos *malware* muy complejos y de sofisticada ingeniería como son el Conficker, también conocido como Downup, Downandup y Kido, etc. Una de los riesgos del futuro son las amenazas avanzadas y persistentes, que se dirigen a objetivos concretos, como el Stuxnet, que ataca los sistemas de administración de procesos industriales. La primera vez que se detectó fue atacando a la tecnología nuclear en Irán. Utiliza técnicas de ingeniería social para infectar, ya que si hay un sistema desconectado de Internet se contagia a la persona que le administra por ingeniería social y luego ésta va a contaminar al sistema y así van a obtener la información.

Otras amenazas son Zeus, un troyano bancario que se distribuyó e infectó millones de ordenadores obteniendo los datos de acceso de la banca on-line,

o Flame, que recopila información sobre tráfico, conversaciones, etc., para obtener datos.

En las redes sociales se realiza con gran asiduidad la distribución de *malware* mediante links. Siempre va a simular ser conocido del usuario cuando se hace el envío y al pinchar sobre la url se crea una red que, rápidamente, distribuye todo tipo de infecciones, porque el carácter viral de las redes permite una repartición muy rápida.

Contrariamente a lo que parece, el eslabón más débil de la seguridad sigue siendo el factor humano. En la actualidad, se están detectando muchos más problemas de seguridad entre las empresas con los empleados jóvenes, prácticamente nativos digitales, que están acostumbrados a moverse en las redes sociales y a dar datos como una cosa normal, y cuando se incorporan a la empresa siguen con la misma política.

Se están produciendo muchas denuncias con el tema de los ataques de negación de servicios a organismos, instituciones generalmente políticas -partidos, Senado, Congreso- que los reivindican bajo el paraguas de Anonymous, de Lulzsec, etc. porque estas colectividades siempre utilizan una fórmula que les proporciona una cobertura, una legitimidad social, es decir, protestas legitimadas socialmente. Las investigaciones descubren que detrás de ellas hay 4 o 5 personas que activan al resto porque tienen cierta infraestructura, no por generación espontánea. Y mucha gente piensa que participar con estos grupos no es delito.

199

El problema ya no es solo el ataque de negación de servicios, que es delito desde la reforma del año 2010 trasponiendo una directiva europea sobre ataques a sistemas y a datos informáticos, sino que detrás de todo esto se han utilizado, en ocasiones, ataques para robar datos, como le ocurrió a SONY. Éste es un tema de gran relevancia.

Los dispositivos móviles son otro objetivo de ataque en el futuro. Ya se han diseñado malware para infectar el móvil, de forma que lo que antes capturaban en el ordenador ahora pueden hacerlo en el móvil, un terminal que, además, permite interactuar instantáneamente.

En Internet el crimen se ha desarrollado como un servicio más, donde todo se vende: números de tarjetas de crédito, claves de acceso a banca on-line, etc. La Brigada realizó una operación en la que el vendedor estaba en Canadá y le compraban unos delincuentes de Alcalá de Henares (Madrid, España), que con esos números de tarjetas luego adquirirían billetes de avión, de tren, televisiones, ordenadores, todo tipo de artículos y bienes.

ORGANISMOS CON COMPETENCIA EN CIBERSEGURIDAD EN ESPAÑA

- El Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC)
- Las Unidades de Delincuencia Tecnológica de las Fuerzas y Cuerpos de Seguridad del Estado, que son los únicos habilitados para investigar si se producen delitos y denuncias
- El Instituto Nacional de Tecnologías de la Información (INTECO), ubicado en León y encaminado a la ciberseguridad del ciudadano. Tiene muchas herramientas interesantes, como la Oficina de Seguridad del Internauta (www.osi.es), donde se encuentran consejos de seguridad, herramientas para desinfectar el ordenador, etc.
- El Centro Criptológico Nacional, que se ocupa de la seguridad en las administraciones públicas
- Un departamento de Presidencia del Gobierno

200

Recientemente se está elaborando la Estrategia Global de Seguridad que, básicamente, es una oficina que va a aglutinar y aprovechar todo el conocimiento que se genera, y coordinar los anteriores organismos. El objetivo global es hacer frente a las amenazas y garantizar la seguridad por una parte de las administraciones y las empresas, impulsar la investigación de las Fuerzas y Cuerpos de Seguridad, tanto en el ámbito de la ciberdelincuencia como en el del ciberterrorismo, y sensibilizar a los ciudadanos de los riesgos que se derivan.

PROBLEMAS EN LA INVESTIGACIÓN DEL CIBERCRIMEN

Por un lado son problemas tecnológicos derivados de la propia arquitectura de la Red, que está dispersa por todo el mundo, no obedece a ningún tipo de frontera y, por consiguiente, a ningún tipo de jurisdicción, y a eso se suma que ahora ninguna corporación tiene los datos en sus máquinas sino en la Nube.

En el otro lado están los temas legales. En el 2010 reformaron el Código Penal para tipificar expresamente el acoso sexual a menores, el acceso a sistemas informáticos, el descubrimiento y revelación de secretos pero el simple acceso, y legislaron los daños a sistemas informáticos y a bases de datos. Ahora, dado que la tecnología ha evolucionado, ya hay otra Directiva

Europea que penaliza otras cuestiones como la pornografía infantil, que ya no se descarga sino que se visualiza por streaming, de modo que si lo que se penaliza es la tenencia y la distribución, ¿eso es tenencia? Es discutible, por ello hay una Directiva Europea que lo penaliza expresamente.

Los delincuentes se tienen que ir adaptando y también las leyes procesales, que en muchos casos casan poco con la rapidez que requieren estos delitos.

Otro tema muy importante en la investigación son la competencia y la jurisdicción, es decir, el 60 por ciento de los delitos económicos que se denuncian por Internet son de menos de 400 euros, y esto es una falta. Están distribuidos en mil juzgados, mil faltas, que sumados alcanzan 400.000 euros. Si se toma el hecho aislado no es nada, incluso un juez puede denegar una intervención telefónica o cualquier medida de este tipo que suponga violentar un derecho fundamental.

Y además, las compañías más importantes de prestación de servicios de Internet -Google, Hotmail, Yahoo- están fuera de España y no están sujetas a la legislación española. Esto ralentiza mucho las investigaciones porque en cualquier intervención es necesaria una comisión rogatoria, que lleva un tiempo tramitarla, con lo que es probable que la información, cuando llegue, no sirva. En este sentido, existen diversos organismos de colaboración internacional, y en Europa se está desarrollando el Centro Europeo del Cibercrimen, en el que se va a aglutinar la información de todos los países sobre determinados temas y ficheros como el Cyborg, de delincuencia económica, el Twins, de pornografía, para que los estados puedan cruzar información.

201

También está el Convenio de Budapest, al que ya se ha hecho referencia, y el Servicio de Criminalística del Tribunal Supremo español, que es una Fiscalía de Sala que se ocupa de la criminalidad informática. A nivel jurisdiccional cada juez es independiente, pero la Fiscalía sí puede dictar instrucciones y seguir unos criterios similares ante los mismos hechos, con lo cual se pueden unificar muchas cosas, y para la Policía es de gran utilidad en las investigaciones.

También hay leyes relevantes relativas a la Red:

- Ley de la Sociedad de la Información y el Comercio Electrónico, que regula determinados aspectos y retirada de contenidos
- Ley de Protección de Datos, que es fundamental porque para realizar una investigación tecnológica esta Ley obliga a las operadoras a guardar

por un año datos relativos a acceso a Internet, a uso de IP, correo electrónico, etc.

A modo de conclusión, para ser eficaces en la lucha contra la ciberdelincuencia y contra las amenazas futuras hay que:

- Ser ágil en los avances legislativos, hay que ir acomodando la legislación penal a los tipos delitos que van surgiendo
- Es básica la formación de unidades especializadas que se dediquen a la investigación de estos delitos, que son realmente complejos. En este sentido es imprescindible la colaboración internacional
- Es fundamental la sinergia entre el sector público y el sector privado, pues éste es el responsable de hasta el 80 por ciento de las infraestructuras críticas de un país –comunicaciones, alimentación, electricidad, finanzas, etc.– y la colaboración en las investigaciones entre ambos ámbitos
- Concienciar y educar a los ciudadanos en el uso correcto de Internet, con programas transversales, verticales, en el colegio, mediante ONG's, etc. Es importante formar, y la Policía, la Unidad Central de Participación Ciudadana, incluye en las charlas que da en los centros educativos estos temas de Internet, porque muchos delitos solo los podemos prevenir ya que, cuando se cometen es difícil llegar hasta el final

MESA REDONDA:

CIBERTERRORISMO

ALFONSO ESTÉVEZ OCHOA
Inspector Jefe del Cuerpo Nacional de Policía

203

El desarrollo de las tecnologías de la información en las comunicaciones ha dado lugar a un nuevo ámbito, un novedoso espacio de relación que se ha venido en llamar ciberespacio, compuesto por sistemas de información, redes, datos y servicios que han proporcionado una globalización sin precedentes a sus usuarios, y que se han constituido en una herramienta fundamental para el desarrollo social y económico de las sociedades.

Según los estudios que observatorios diversos realizan, periódicamente, sobre el grado de desarrollo de Internet y la penetración, la influencia de la Red en las economías, se observa dos resultados constantes en todos ellos: por un lado, crece la aplicación de Internet en el mundo, cada vez hay más usuarios y, en segundo lugar, se incrementa el peso de la Web en las economías.

Algunos datos estadísticos que apoyan esta información se encuentran en el último informe elaborado por la consultora Consulting Group, que estiman que la actividad económica generada por Internet en el año 2016 será de un 5,3 por ciento del Producto Interior Bruto agregado del G20; sobre el número de usuarios calculan en torno a los 3.000, lo que supone un relevante incremento con respecto a los 1.900 millones de 2010.

En cuanto a datos de España, el informe de la Sociedad de la Información, de la Fundación Telefónica, establece que se ha producido un crecimiento

del comercio electrónico de un 23 por ciento respecto al año anterior, lo que representa también una cifra considerable.

Los datos indicados llevan a determinar que las sociedades son cada vez más dependientes del ciberespacio, de la Red, lo que convierte en prioritario conseguir la seguridad en ese entorno, es decir, alcanzar la ciberseguridad, de tal forma que las ciberamenazas no afecten al normal funcionamiento de los servicios esenciales y no dificulten el desarrollo económico de las sociedades.

La estrategia española de seguridad, que fue aprobada en 2011, ya hacía referencia a que en el ámbito del ciberespacio existían potenciales amenazas que podían afectar a la seguridad nacional. Las amenazas que se consideran más relevantes dentro del ciberespacio para la seguridad del Estado son las siguientes:

- 1) Otros Estados. Estos, a través de sus servicios de seguridad o de las unidades cibernéticas de sus Fuerzas Armadas, pueden afectar a la información sensible de sistemas de información gubernamentales y de empresas privadas de sectores estratégicos y, en caso de conflicto, esas unidades cibernéticas, también pueden perturbar el funcionamiento de servicios esenciales para una sociedad. Presentes están los ciberrataques de Estonia, en el año 2007, la crisis entre Rusia y Georgia, en 2008, y casos más recientes de difusión de malware, como los de Sputnex o Flame.
- 2) La ciberdelincuencia. El delito se ha convertido en una de las actividades más lucrativas para el crimen organizado, y alguna de las que se realizan utilizando la Red son las que están relacionadas con la difusión de pornografía infantil, la vulneración de los derechos de propiedad intelectual e industrial y las estafas o fraudes.
- 3) El hacktivismo. Éste puede tener motivaciones políticas, religiosas o patrióticas. Habitualmente, solo afecta a servicios web, pero hay casos de grupos que también atacan información sensible.
- 4) El ciberterrorismo. Es la actividad que los terroristas desarrollan en Internet en una doble vertiente:
 - La utilización de la Red como arma, un instrumento para realizar ataques contra otros sistemas informáticos o la propia infraestructura de Internet
 - El uso de la Web como un medio, un recurso para desarrollar acti-

vidades operativas tales como comunicación interna, propaganda, reclutamiento, financiación o recogida de información

Hay que partir de la base de que los grupos criminales están presentes en Internet y que, al igual que el resto de organizaciones, intentan sacar partido de dos rasgos esenciales de la Red: su globalidad y las grandes garantías de anonimato que proporciona.

EL EMPLEO DE INTERNET COMO UNA RED

Los ciberataques, ya tengan como objeto el robo de información sensible o el ataque a otros sistemas informáticos o la propia infraestructura de Internet, son reales. Existen en ámbitos como el ciberespionaje, la ciberguerra, el hacktivismo o el cibercrimen. Los sucesos que se produjeron en Estonia en el año 2007, supusieron un punto de inflexión en lo que hace referencia a la visión que se tenía hasta ese momento de los ataques cibernéticos. A partir de ese momento, se demostró de forma fehaciente que un país podía ser objeto de una agresión de ese tipo.

En lo que respecta a las organizaciones terroristas, la estrategia que han seguido hasta ahora respecto a su uso de Internet no parece incluir la ejecución de ciberataques, no les han prestado demasiado interés, bien porque consideren que no tienen las capacidades necesarias para llevarlos a cabo, o bien porque entienden que pueden obtener más rentabilidad a través de la ejecución de operaciones convencionales. Como se indicaba anteriormente, la dependencia cada vez mayor que las sociedades tienen de Internet puede hacer que estos grupos varíen su estrategia, y se planteen una inversión a largo plazo para conseguir los recursos necesarios para llevar a cabo este tipo de ofensivas. O no modificar su estrategia, pero no en el sentido de mejorar sus capacidades sino de alquilar éstas a ciberdelincuentes profesionales, que les arrienden sus capacidades en infraestructura necesaria para llevar a cabo esas agresiones.

205

Sobre el papel, los ciberataques tienen una serie de ventajas:

- Grandes garantías de anonimato para los autores
- Permite realizar los ataques sin exponer la integridad física de los atacantes
- Su ejecución es independiente de la ubicación física de los autores

Las organizaciones yihadistas son las más activos en la Red, las que mejor han entendido la utilidad que podían sacar de Internet y las que hacen un

uso más intenso de ésta. En este sentido, en relación con los ciberataques de 2011 Al-Qaeda Central, a través de su Departamento de Comunicación, As-Sahab, emitió un vídeo en el que se animaba a los yihadistas a participar en la yihad electrónica, realizando ataques contra estructuras críticas y sistemas gubernamentales de los Estados Unidos y de sus aliados y también a medios de comunicación, según ellos poco favorables a la Yihad.

Esta forma de funcionamiento se enmarcaría en lo que algunos autores han denominado “a tercera ola del yihadismo global”, en la que Al-Qaeda Central marca objetivos, anima a cometer acciones a través de Internet y, posteriormente, dichas iniciativas son llevadas a cabo por grupos locales autónomos.

206 Situados en otro nivel dentro de lo que es la yihad electrónica, se encuentran gran cantidad de grupos hacktivistas, presuntamente yihadistas, que se dedican a realizar ataques contra servicios web, fundamentalmente de Deface (ataque consistente en cambiar la apariencia y contenido de una página web) y de negación de servicios. Esto no se considera propiamente ciberterrorismo, sino más bien hacktivismo con motivación ideológica o religiosa. Un ejemplo del resultado de uno de estos ataques contra un sitio web ubicado en un servidor español es el del grupo atacante Internet Islamic Brigadas, que cambió el contenido original de la página por la primera sura del Corán. Una escalada de ofensivas de este tipo se produjo a raíz de la publicación de unas viñetas sobre el profeta Mahoma en el periódico danés Jyllands-Posten, en el 2006, y por lo que recibió amenazas, así como otras cabeceras occidentales que le apoyaron publicando a su vez las viñetas. Se produjo una auténtica oleada de ataques a sistemas de esos países.

¿CUÁLES SON LOS POSIBLES ESCENARIOS DEL FUTURO?

En caso de que estas organizaciones terroristas progresen o alquilen las capacidades necesarias para llevar a cabo estos ataques, podrán darse asaltos contra:

- Infraestructuras críticas para alterar el normal funcionamiento de las mismas
- Servicios on-line, tal como banca o comercio, con el fin de menoscabar la confianza en la Red y, de esta forma, intentar perjudicar las economías occidentales
- La información sensible de sistemas gubernamentales

Otro escenario sería la ejecución de operaciones en las que se combinen ataques convencionales con cibernéticos, dirigidos a perjudicar o retrasar la acción de los equipos de emergencia, los servicios policiales, para de alguna forma amplificar el efecto de las acometidas.

USO DE INTERNET COMO UN RECURSO

En este caso, la Web es un medio para desarrollar actividades operativas, que es lo que está ocurriendo hoy día en el ciberespacio. Hay que partir de un principio básico: todas las agrupaciones terroristas tienen presencia y usan Internet, pero, cada una, dependiendo de sus características. No tiene nada que ver el manejo de Internet que una organización terrorista de carácter local y autóctona como ETA pueda realizar de Internet, que el de las colectividades yihadistas, que tienen un alcance global.

Las actividades que desarrollan a través de Internet son las comentadas anteriormente.

Los sistemas de comunicación tradicionales, tales como telefonía móvil o telefonía fija, han sido completamente sustituidos por las comunicaciones a través de Internet, fundamentalmente a través del correo electrónico, de mensajería como Whatsapp, voz IP como Skype, plataformas como Paltalk, incluso el empleo de foros o redes sociales, todo ello dependiendo de la clandestinidad de la que se quiera dotar a la comunicación. En muchas ocasiones se usan técnicas criptográficas con sistemas de cifrado, tales como herramientas DGP (Pretty Good Privacy), de distribución libre que utilizan el algoritmo RSA, para evitar la interceptación de los mensajes por las fuerzas de seguridad. Hay instituciones que han creado sus propias aplicaciones de cifrado, como en el caso del ámbito yihadista con el Muyahidin Secrets, una herramienta antiforense, de cifrado, que fue difundida por el Global Islamic Media Front en el año 2007, ésta era su primera versión. El Global Islamic Media Front es uno de los grupos de distribución de material yihadista más relevantes, y también en algunas ocasiones de producción de su propio material. En 2008 apareció su segunda versión, que fue distribuida por la yihadista Al-Ekhlaas Islamic Network. Es una herramienta con bastantes posibilidades, permite el cifrado tanto de mensajes como de archivos, el empleo de distintos algoritmos de cifrado y utilizar los cifrados simétrico y asimétrico. También es una aplicación que proporciona el borrado seguro. Es una herramienta que se sigue utilizando y recomendando en los foros y en las revistas electrónicas yihadistas.

En un sentido más amplio de la difusión de contenido terrorista a través de Internet, se ubica la propaganda propiamente dicha y la transmisión de otro tipo de contenido, como manuales de fabricación de explosivos, de

técnicas terroristas, de seguridad informática, es decir, todo tipo de textos vinculados con actividades terroristas.

Las organizaciones yihadistas son las que mejor han entendido la importancia que tiene Internet para la difusión de propaganda, y sus líderes se han preocupado de contarlos en numerosas ocasiones en sus comunicados públicos. De esta forma, ya en el año 2005, en un comunicado producido por Al Sahab, Al-zawahiri hacía referencia a que la Red era una herramienta excepcional para animar a los musulmanes a abrazar la Yihad. En el año 2008, en otra nota difundida en abril por esa organización en relación a la importancia de Internet en la distribución de propaganda, explicaba un hecho bastante relevante: la Yihad mediática había logrado romper el monopolio de los medios de comunicación occidentales.

La distribución de propaganda a través de Internet tiene una serie de ventajas y, al hilo de lo que manifestaba Al-zawahiri, la primera de ellas es que la información se puede difundir directamente, sin intermediarios, de tal forma que el mensaje llega a los destinatarios exactamente igual que como fue producido. En algunos momentos, Al Qaeda Central transmitió sus materiales a través de Al Jazira, pero llegó un momento en que decidió divulgarlos directamente a través de la Red.

208

Otra de las ventajas de la Web es el anonimato, que es constante. Se puede difundir propaganda de incógnito, pues es bastante complicado seguir el rastro de los militantes que la están distribuyendo en la Web. Y permite publicarla en distintos formatos: audio, texto, vídeo, etc., de tal forma que se aumenta el impacto que el mensaje puede producir en los destinatarios. También se puede difundir contenido a cualquier lugar del mundo, simplemente con que exista una conexión a Internet.

Las organizaciones yihadistas crearon toda una estrategia de difusión de material a través de la Red, y lo primero que constituyeron fueron los departamentos de comunicación. Prácticamente, cada sociedad yihadista tiene ese departamento, dedicado en exclusiva a la creación de material. Graban cada acción, después la editan y luego la publican a través de Internet.

Otro aspecto relevante son las compañías distribuidoras de material yihadista, como el Global Islamic Media Front o Al Fajir que, en algunos casos, son responsables de homologar la veracidad del material y también el que un foro yihadista es real y no ha sido creado por un servicio de información occidental.

Junto con los departamentos de comunicación y las agencias de distribución, el otro elemento fundamental son los foros yihadistas. Son puntos de

encuentro de yihadistas de todo el mundo y un elemento fundamental en la distribución del material. No se trata solamente de propaganda, sino también de información que puede servir para llevar a cabo acciones terroristas, es decir, que en la propaganda, de alguna forma, estarían englobadas también actividades de entrenamiento a través de Internet.

Una vez que el material es producido, las productoras lo editan con distintas calidades para que pueda acceder un mayor rango de destinatarios y lo suben a sitios gratuitos de almacenamiento de ficheros (Megaupload, Rapidshare, etc). Los enlaces a esos sites son distribuidos en los foros yihadistas, indicando el tamaño del material y, como normalmente se suelen distribuir comprimidos y con contraseña para dificultar la labor de rastreo y de limpieza de material ilícito por parte de los sitios gratuitos de almacenamiento de ficheros, también suele aparecer la clave de acceso. En muchas ocasiones las producciones de vídeo tienen subtítulos para alcanzar una audiencia más amplia.

Foros yihadistas hay muchos, pero existe un núcleo duro a través de los cuales se remite primero y, posteriormente, a través de distribuidores voluntarios, llega incluso a páginas visibles –redes sociales, diversas plataformas de distribución de vídeo tipo YouTube o mediante enlaces en redes sociales–. Ese núcleo duro es lo que se ha dado en llamar la web oscura o profunda, que es aquella parte de Internet que no es indexable por los motores de búsqueda.

209

Aparte de la propaganda, también se distribuye material dedicado al entrenamiento o fabricación de explosivos, manejo de armas, técnicas terroristas, seguridad informática. El sistema de difusión es exactamente el mismo que con la propaganda. Un ejemplo es el de la revista electrónica *Inspire*, que es producida por Al Qaeda en la Península Arábiga y que en su novena edición incluyó varios artículos, que pueden ser bastante ilustrativos de cuál es el tipo de material que se distribuye: se anima a la comisión de incendios forestales mediante artefactos incendiarios, buscando que las masas forestales que se incendien estén lo más próximas posibles a zonas densamente pobladas para provocar más daños, especificando que deben cometerse, primordialmente, en Estados Unidos, en Reino Unido, Israel y en países de la Organización del Tratado Atlántico Norte (OTAN). En otro de los textos se propone la comisión de atentados individuales dentro de los países occidentales.

Una de las cosas que más llaman la atención es la metodología cada vez más profesional que se utiliza. Incluso en la revista *Inspire* llama la atención la gran calidad que tiene.

La creación de departamentos específicos en las organizaciones terroristas yihadistas es algo ya indicado. Cada una tiene el suyo: Al Qaeda Central

tiene Al Sahab, Al Qaeda en el Magreb Islámico tiene Al Andalus, y cada una tiene su departamento mediático propio, con lo cual se consigue un grado de profesionalización bastante elevado. Un ejemplo del efecto que este tipo de material tiene es un atentado frustrado que se produjo en el año 2006 por parte de unos ciudadanos libaneses en Alemania, que pusieron dos artefactos explosivos en sendos trenes en la estación de Colonia, que finalmente no explotaron por un defecto de fabricación. Se comprobó que el material que habían utilizado para elaborar los explosivos procedía era un vídeo yihadista que habían bajado de Internet.

Otro aspecto muy importante relacionado con la difusión de material yihadista es la influencia que tiene Internet en los procesos de radicalización, es decir, es un vector de radicalización de primera magnitud por dos razones:

- La gran cantidad de contenido extremista que existe en la Red
- Esos procesos no dejan de tener un componente social. Individuos con planteamientos radicales que empiezan a moverse en Internet en entornos virtuales, encuentran personas con planteamientos similares a los suyos de una forma bastante más fácil que en el mundo real y, por supuesto, en un entorno en el que se encuentran más cómodos y seguros

También hay que tener en cuenta que en esas comunidades virtuales radicales no hay debate de ideas. Las ideas moderadas son expulsadas inmediatamente, de tal forma que un individuo con planteamientos extremos que entra en la órbita de este tipo de comunidades, los procesos de radicalización lo que hacen es, en la mayoría de las ocasiones, llevarle a más.

Muy vinculado con los procesos de radicalización están los métodos de reclutamiento. Todas las organizaciones terroristas tienen presencia en Internet, cada una adopta la estructura, utiliza los medios u organiza las actividades que considera más oportunas, en función de sus características. La Red es un ámbito apropiado para la realización de captaciones dentro de las organizaciones yihadistas, sin embargo, en un entorno de una entidad como ETA, de carácter local, no tiene sentido realizar captaciones a través de Internet.

Hay distintos tipos de foros yihadistas, los más habituales son los abiertos, en los que no hace falta ningún tipo de registro; los foros semiabiertos son aquellos en los que se requiere, exclusivamente, un proceso fácil de registro y ya se puede participar en ellos; y los foros cerrados, a los que solamente

se puede acceder a través de invitación. La mayor parte de la gente empieza utilizando los foros semipúblicos, en los que se registran, utilizan un nick y una cuenta de correo electrónico y, a partir de ahí, ya pueden funcionar. Cuando comienzan su actividad en el foro ya son supervisados por los moderadores y los administradores. Estos usuarios privilegiados empiezan a evaluar el comportamiento de los nuevos. Si las aportaciones que realizan son relevantes, aportan material interesante y sus intervenciones se consideran adecuadas, se les propondrá pasar a otro nivel, ser moderadores, encargarse de la supervisión de los contenidos, supervisar la actividad de otros usuarios y, sobre todo, tendrán ya acceso a determinadas partes del foro que les estaban también restringidas.

La finalidad de la captación puede ser para formar parte de una red yihadista virtual encargada de la difusión de propaganda o es una finalidad es operativa, en cuyo caso, evidentemente, a los contactos virtuales tendrán que seguir contactos en el mundo físico, contactos personales. Un aspecto muy interesante y muy importante en relación con toda esta utilización de Internet por estos grupos es que está muy vinculado al desarrollo tecnológico. Desde hace tiempo hay una verdadera expansión de los dispositivos móviles. Estos, tales como *smartphones* o tabletas, han producido a su vez la expansión de las redes sociales. En algunas de ellas no tiene sentido participar si no se está permanentemente conectado a Internet, porque lo bueno de esas redes es poder participar en ellas en tiempo real, de esta forma aparecen contactos nuevos, conceptos nuevos, como el comunicador digital, permanentemente conectado. Son las personas que están permanentemente recibiendo y transmitiendo información en tiempo real. Hay redes sociales, como por ejemplo Twitter, cuyo sentido precisamente es ese: estar conectado constantemente.

211

Esos cambios que se producen en los ciudadanos de a pie también tienen su influencia en el *modus operandi* de esas asociaciones, de tal forma que aparecen individuos que están “enganchados” a Internet 24 horas desarrollando una actividad febril, es decir, empiezan a bucear en foros yihadistas, recuperan su material, lo difunden a través de la web visible, administrando y manteniendo varios blogs, perfiles en distintas en redes, organizan charlas a través de paltalk, etc.

Otra cuestión a tener en cuenta, aunque es de menor relevancia debido a la influencia que puede tener hasta ahora, son las actividades de financiación a través de la Red. Hay grupos radicales violentos que han solicitado dinero a través de sus propias páginas web, o que han creado tiendas virtuales con productos vinculados con ellos. Hay ocasiones en las que también, ya dentro del ámbito yihadista, se han producido inversiones mediante la comisión de fraudes a través de Internet, como es el caso de un ciudadano marroquí

afincado en el Reino Unido que utilizaba en Internet el nick yihad007 y que, además de ser administrador de multitud de foros yihadistas y distribuir propaganda en la Red, usaba el fraude de tarjetas de crédito como medio para financiar a grupos yihadistas. Lo detuvieron en el año 2005 en el Reino Unido.

Otra actividad que desarrollan estos grupos es la recogida de inteligencia, de información a través de Internet, que es una fuente estupenda, tanto para las fuerzas de seguridad como para los ciudadanos de a pie. Existen multitud de datos útiles, como planos de edificios, de ciudades, información sobre políticos, sobre responsables de organizaciones, utilizando Google Earth o Google Maps para localizar objetivos, de una forma más rápida, menos costosa y más cómoda.

CONCLUSIONES

Debido a la cada vez mayor dependencia que las sociedades modernas tienen de Internet, la consecución de un ciberespacio seguro y libre de contenido ilícito debe ser un objetivo prioritario para cualquier Estado moderno. En segundo lugar, las organizaciones terroristas hacen uso intenso de Internet, han llegado al ciberespacio y no se van a ir de él, es decir, les resulta muy útil y van a seguir utilizándolo si se les permite. Y en tercer lugar, algunas medidas que se podrían adoptar en la lucha contra el uso que las organizaciones terroristas en Internet podrían ser:

- 1) Fortalecer la colaboración policial y judicial en el ámbito internacional. Todas esas investigaciones tienen un carácter transnacional, en todas participan más de un país, por lo que se hace necesaria la colaboración internacional y, además, estos canales de deben transmitir esa información de forma rápida, debido a la volatilidad de las evidencias electrónicas.
- 2) Es muy importante adaptar el marco legal español a las necesidades creadas por los delitos relacionados con las nuevas tecnologías, fundamentalmente en lo que hace referencia al tratamiento procesal de las evidencias electrónicas, a las circunstancias que rodean al anonimato en el ciberespacio y a la utilización de herramientas de cifrado. También es muy relevante y sería muy importante tender a una armonización de las legislaciones entre los países del mismo entorno, para evitar la existencia de lagunas que dificulten luchar eficazmente contra estas actividades.

- 3) Promover la colaboración con el sector privado. Hay que tener en cuenta que la mayoría de los servicios de Internet están en manos privadas. Esas empresas tienen una experiencia y unos conocimientos, están acostumbrados a luchar contra las ciberamenazas y su colaboración es de gran interés, sobre todo en lo referente a la detección y eliminación de contenido ilícito y a la preservación de datos que puedan ser necesarios en las investigaciones policiales.
- 4) Potenciar la información y los recursos de las Fuerzas y Cuerpos de Seguridad del Estado y de los funcionarios judiciales que trabajan en estos ámbitos, y también potenciar la colaboración ciudadana. Esta última es muy importante en todos los ámbitos de actuación policial, y en el caso del ciberterrorismo no lo es menos.

CIBERTERRORISMO

MANUEL ENRIQUE MARLASCA GARCÍA
Periodista

Los atentados terroristas son entendidos por cualquier activista, por cualquier terrorista, como una herramienta de propaganda de la ideología que da sustento a todas sus acciones, la que le sirve de base o justificación. Un atentado para ellos no es más que una herramienta de propaganda de esa idea. Y si un atentado no es reivindicado rápidamente, no se conoce pronto de quien es la autoría, no sirve para nada. Cualquier terrorista lo sabe. Un buen ejemplo de todo eso es la rapidez con la que los terroristas del 11M (11 de marzo de 2004) reivindicaron su actuación en Madrid (España). El 13 de marzo, dos días después de los hechos en la capital española, los terroristas avisaron al canal de televisión Telemadrid de que había una cinta de vídeo en una papelería al lado de la Mezquita de Madrid en la que Rachid Oulad, uno de los autores, reivindicaba la acción como de una célula relacionada con Al Qaeda. En los restos de la voladura del piso del de Leganés, que se produjo el 3 de abril, también se encontró un vídeo, grabado por Jamal Ahmidan, “El Chino”, en el que reivindicaba no solo la acción de los trenes sino también el intento de atentado en la vía férrea, y amenazaba con más crímenes en el caso de que el Gobierno español no hiciese caso a sus peticiones.

215

Por tanto, a mayor difusión de sus atrocidades, de sus crímenes, mayor éxito consideran que tiene la acción. Para esa divulgación, Internet es, desde hace ya casi 10-15 años, una herramienta extraordinaria para los terroristas. Desde hace mucho tiempo, los yihadistas guardan en sus ordenadores, en sus pen drives, en todo tipo de soportes, imágenes, ya que en cada acción terrorista que realizan les acompaña alguien que va grabando. Las primeras grabaciones fueron a los guerrilleros chechenos, que son musulmanes, degollando o volando por los aires a soldados rusos en la guerra de Chechenia.

Grandes éxitos en los foros yihadistas, y en todo este conglomerado, fueron las decapitaciones de Daniel Pearl, un periodista que murió asesinado en Afganistán en febrero de 2002, y de Nicholas Berg, en mayo de 2004. Esos asesinatos se grabaron en vídeo y fueron, y son hoy día, bastantes las visitas que reciben en esos foros.

Otro ejemplo: durante la instrucción del sumario de los atentados del 11M, se averiguó que la célula de Madrid, gran parte del núcleo duro de los terroristas que cometieron los atentados, se reunían en la madrileña calle de Virgen del Coro para ver ese tipo de vídeos, ese material con acciones que realizaban otros terroristas.

En la Operación Dátil de 2001, que fue la primera gran acción contra el yihadismo internacional que se llevó a cabo en España, que fue realizada por la Comisaría General de Información e instruida por el juez Baltasar Garzón, gran parte de los terroristas detenidos, miembros de Al Qaeda, disponían de material de adoctrinamiento procedente de numerosas webs. En el año 2001 no existía, lógicamente, el desarrollo que tiene Internet ahora, pero sí comenzaban a aparecer páginas islamistas, con contenido yihadista. Más adelante, en el año 2004, entre los restos de la casa de Leganés en la que se inmolaron los terroristas del 11M, había ordenadores y memorias cargadas con ese tipo de documentación. Había textos, discursos y vídeos de verdaderos ideólogos de la yihad como Sayyid Qutb, Abu Qutada, Mohamed Fizazi. Estos imanes radicales son un buen alimento ideológico y dinamizador para cualquier célula.

La atomización de Al Qaeda, sobre todo después del atentado del 11 de septiembre de 2001 (11S) en Nueva York (Estados Unidos) y de la intervención norteamericana en Afganistán, posibilitó que en nombre de Al Qaeda muchísimas organizaciones pequeñas, locales, cometiesen atentados sin la intervención de ningún dirigente de la Red. No hacía falta la organización de Al Qaeda, no hacía falta que Mohamed Atta se fuese a ver a Bin Laden y que adoctrinase a los que participaron en el 11S, sino que ya cualquier célula local podía organizar su atentado. Casablanca, Madrid y Londres fueron perfectos ejemplos de esto. Basta con una célula o con una autorización difundida a través de esos medios digitales yihadistas.

“El Irak del Yihad, esperanzas y riesgos”, fue un documento difundido por la página Global Islamic Media en septiembre del año 2003, y en él se preveía perfectamente lo que ocurriría en España en caso de un gran atentado yihadista. Se establecían las líneas y las bases de lo que iba a pasar, el cambio, el vuelco electoral y político, la retirada de las tropas españolas, es decir, anticipaba todo lo que iba a producirse. En diciembre de 2003, ya apenas

tres meses antes de los atentados del 11M, la misma Global Islamic Media publicó “Mensaje al pueblo español”, en que el se mencionaba el asesinato de siete agentes del Centro Nacional de Inteligencia (CNI) muertos en Irak, pero en realidad quemados unos días antes, y se anunciaba lo que ocurriría tres meses después: los atentados del 11M.

Internet es una herramienta utilísima como propaganda para los yihadistas. No está controlada y, además, tiene la dimensión global que no tienen la televisión, la radio o la prensa escrita. Por ejemplo: Mustafá Setmarian fue un alto operativo de Al Qaeda. Procedente de Siria, llegó a España, se nacionalizó, se casó con una mujer española, Elena Moreno, y trabajó entre 1995 y 1996 en una revista tradicional de papel que se llamaba Al-Ansar, que era la cabecera oficial de propaganda del GIA argelino y estaba dirigida por el clérigo radical Abu Kutada. Tras trabajar en esa revista y lanzar soflamas yihadistas y radicales en la misma, pasó a convertirse en Abu Musab al-Suri, se convirtió en alto operativo de Al Qaeda y empezó a difundir y a aleccionar en la Red a posibles yihadistas en el uso de venenos, de armas químicas, etc. El viaje que hizo Setmarian desde su trabajo en una revista hasta llegar a la cúpula de Al Qaeda, es el mismo viaje que ha hecho el yihadismo.

Ya en el año 2002, en el sitio de *Azzam Publications*, aparecía el siguiente mensaje: “Animamos enérgicamente a los profesionales de Internet para que propaguen y diseminen noticias de información sobre la Yihad a través de listas de correo electrónico, grupos de discusión y sus propias páginas webs. Cuantas más webs mejor para nosotros. Debemos convertir Internet en nuestra propia herramienta”. Y así lo han hecho.

217

Además, la Red les proporciona una conciencia de comunidad global. Es un caso similar al de los pederastas. Estos acudían hace años a la puerta del colegio, a un parque, escondiéndose para dar rienda suelta a esas perversiones. Ahora, Internet se ha convertido en un lugar de encuentro de pederastas, donde ven que hay más gente como ellos, que comparten esos gustos sexuales y, además, les proporciona esa reafirmación. Con el yihadista pasa lo mismo, ha salido de la oscuridad de las mezquitas radicales, de los garajes, de los bajos donde se reunían para emitir sus mensajes radicales y tienen la Red, en la que intercambian información, opiniones y experiencias. Han salido también de esas tortuosas rutas por Turquía, por Siria, que antes realizaban para llegar a los campamentos de Afganistán o en la Bosnia musulmana. Por ejemplo, Yusuf Galán, que fue uno de los detenidos en el año 2001 por el 11M, tuvo que desplazarse hasta la isla indonesia de Poso para acudir al campamento de un tipo que se llama Parlindungan Siregar, un indonesio que había estado en Madrid y que le reclutó para su célula. Yusuf Galán hizo un viaje terrible, larguísimo y muy complicado para llegar

a Indonesia, entrenarse y regresar a Madrid con los conocimientos de un terrorista. Probablemente, si hoy Yusuf Galán quisiera convertirse en terrorista, lo tendría más sencillo a través de todas esas páginas web. Por cierto, Yusuf Galán ya está en libertad, fue condenado y está en libertad.

Internet también permite la reafirmación emocional de pertenecer a una comunidad global. El yihadista a veces tiene esa necesidad, de buscar referentes, ejemplos, y la Web es un instrumento ideal para difundir las proezas de otros yihadistas. Los autores del 11M guardaban numerosos vídeos homenaje a los autores del 11S, donde la figura de Mohamed Atta aparecía sobre el fondo de las torres gemelas, con imágenes y mensajes de alabanza. Tras los atentados del 11M, sus autores han pasado a formar parte de ese imaginario de héroes de la Yihad. Se han encontrado en numerosas páginas yihadistas menciones a lo que llaman “La bendita acción de Madrid”, y se ven iconografías de los atentados de los trenes o de la explosión de Leganés mezcladas con las caras de los terroristas.

218 La Red es una pieza fundamental para el adiestramiento, una escuela virtual eficacísima. Parece ser que los autores del atentado del 7 de julio (7J) de 2005 en Londres obtuvieron, parte de sus conocimientos, a través de páginas web que explicaban cómo fabricar los explosivos. Especial mención merece en este punto una pequeña memoria USB que se localizó entre los restos de la casa madrileña de Leganés donde se inmolaron los terroristas del 11M. En ese pen drive se encontró que en la web Global Islamic Media había un foro llamado Abu Bañan, que está considerado por la Unidad Central de Inteligencia como el órgano de propaganda de Al Qaeda en Irak. En ese foro se reivindicaban atentados, se exhibían degollamientos o se difundían imágenes de presuntas torturas en cárceles iraquíes. Entre el 1 y el 26 de enero de 2004, apenas dos meses antes de los atentados del 11M, uno de los terroristas, presumiblemente “El Chino”, descargó 15 archivos de las páginas de Abu Bañan con el título genérico “Cadena de preparativos para la lucha”, que contenía diversos capítulos: “La guerra de guerrillas”, “La guerra urbana”, “La preparación militar”, “El material explosivo”, “Las precauciones que hay que tener con los teléfonos móviles”, “Qué hacer en caso de ser detenido y ser interrogado”, etc. Probablemente, si no hubiesen existido Rafa Zouhier o José Emilio Suárez Trashorras, los terroristas del 11M no habrían hecho otra cosa que obtener el conocimiento para la elaboración de las bombas de esas páginas precisamente. No tuvieron que emplearlo porque apareció la posibilidad de obtener Goma2.

En cuanto a las comunicaciones privadas, el encriptamiento y el uso de Internet como una herramienta eficaz de comunicación, los yihadistas no han hecho más que imitar a otros grupos, a otras organizaciones criminales

o, incluso, a los pederastas. Crean foros restringidos, y se ha detectado el uso en las cuentas de correo electrónico de buzones con claves compartidas para intercambiar información en la carpeta de borradores. Esto es relativamente frecuente. Hay dos ejemplos recientes que lo ilustran, uno en Italia y otro en España, que resumen dónde está hoy la Yihad en relación con la Red.

Mohamed Jarmoune era un inmigrante marroquí con 20 años que residía, desde los 6 años, en la provincia italiana de Brescia. Esta persona fue detenida en marzo del 2012 por los servicios de información italianos, acusado de preparar un atentado contra la sinagoga de Milán. Mohamed estaba bien integrado en la sociedad italiana, cursó estudios de formación profesional, tenía un trabajo estable en el sector de la siderometalúrgica, acudía a discotecas, tomaba su cerveza, se le vía con chicos, es decir, estaba completamente alejado de las rigurosas normas islámicas, ni siquiera se le veía por los lugares de culto habituales. Tampoco estaba en riesgo de exclusión social, pese a que la crisis económica había golpeado, especialmente en la Europa mediterránea, a los emigrantes de segunda generación como él. Jarmoune fue detenido gracias a una operación de los servicios de información italianos, que vigilaban un foro de discusión yihadista en el que se intercambiaban materiales como, por ejemplo, la enciclopedia de la Yihad. Jarmoune tenía siete perfiles distintos en Facebook, diez cuentas de correo y, a través de esos soportes, sobre todo la red Facebook, divulgaba ideas yihadistas y vídeos que elaboraba con las imágenes típicas de atentados en Afganistán, en Irak y en Somalia. Además, dirigía un sitio de Internet que estaba destinado, ya no solo a compartir ideas, proclamas y soflamas yihadistas, sino a intercambiar conocimientos prácticos sobre explosivos, armas, una gran cantidad de material muy sensible. La Policía italiana detectó esos intercambios de información y ese aleccionamiento que Jarmoune estaba dando a otras personas, potenciales yihadistas en otros lugares de Europa, especialmente en el Reino Unido. En ese país había alguna mujer que había intercambiado con él información sobre materiales explosivos.

219

Jarmoune vio a Internet la triple utilidad que resume, perfectamente, lo que significa hoy día la Red para el yihadismo. Fue allí donde Jarmoune se formó ideológicamente, donde se ensució la mente con las ideas yihadistas, donde empezó a ser él el difusor de los mensajes de la Yihad y donde recibió los conocimientos adecuados para llevar a cabo su acción.

El otro ejemplo es el de un marroquí detenido en España por la Guardia Civil. Se llamaba Abdellatif Aoulad Chiba y contaba 37 años. Residente en Cádiz, fue apresado en 2011 y está actualmente en prisión acusado de integración, organización terrorista y conspiración para el asesinato. Su actividad se limita a la Red. Era usuario habitual de los foros yihadistas más importan-

tes del momento: Al Sumukh y Ansar Al Mujahideen. Esos foros son similares, aunque de una menor dimensión, al veterano Global Islamic Media. En esos foros se difunden comunicados, vídeos, que además sirven, lógicamente, para el reclutamiento, para la captación de nuevos miembros, así como para la difusión de material militar. Aoulad, aparte de consultar y de ser usuario activo con un nick en cada uno de esos foros, era administrador de su propia página yihadista: Shabaka Al Haqiqa Al Ikhbaria (Red de la Verdad Informativa), que era una hermana pequeña de las páginas antes citadas. Entre la documentación que se le localizó había un juramento que hizo de lealtad a Abu Hudaifa Al Musuli, que es el líder de Al Qaeda en el Magreb Islámico, y una especie de comunicado de los deseos de vengar la muerte de Osama Bin Laden y de otros mandos operativos de Al Qaeda. Hay una frase que dice: “Dios Mío, concédeme el martirio por tu causa. Que tenga la valentía y la suficiencia. Que mi cuerpo vuele en pedazos por amor a Ti hasta el punto de no poder reunirlos y enterrarlos en la tumba”.

220 Aoulad no se ocultaba, ni mucho menos, no tenía ningún reparo en mostrar sus intenciones, dejaba bien claro que quería hacer un atentado con el vocabulario típico de estos foros contra los infieles y, en este caso, lo que pretendía y de lo que se le acusó es de intentar envenenar las reservas de agua para consumo humano, de los depósitos de agua de algún camping o de algún complejo turístico. El Servicio de Información de la Guardia Civil fue observando cómo la voluntad de atentar iba creciendo en él cada día. Aoulad iba subiendo el tono de sus intervenciones y se iba mostrando cada vez más cercano a sus intenciones, y le detectaron una serie de llamadas que pueden interpretarse como de despedida a sus amigos, a su familia y a su mujer. En esos foros, a medida que iba creciendo su voluntad, otros usuarios iban poniendo a su disposición manuales para la fabricación y uso de venenos y de explosivos. Él incluso, en un momento dado, pide ayuda para envenenar un depósito de agua, y mientras un usuario le facilita un link donde se bajó el archivo “La Enciclopedia de los venenos”, otro le facilita la receta de la toxina de la botulina. El cómo los pide, tampoco deja ninguna duda: “Pido a los hermanos proporcionarme la fórmula de un veneno mortal de alta eficacia con el fin de introducirlo en los canales y los depósitos de agua que suministran a los complejos turísticos y viviendas de los infieles”. Aoulad sigue en prisión y el juez, en su auto, a la hora de expresar los fundamentos jurídicos y de razonar la pertenencia de Aoulad a una organización terrorista, señala lo siguiente, que probablemente siente un precedente y jurisprudencia, aunque sea un auto de prisión: “Los diversos foros yihadistas activos en Internet constituyen un centro de reunión vital entre simpatizantes de esta doctrina radical, los ideólogos que la sustentan y alientan y los miembros de las diferentes organizaciones terroristas que las ponen en práctica. La interacción entre unos y otros llega a constituir una amor-

fa supra organización yihadista, que coopera e interactúa para conseguir alcanzar los objetivos generales de la Yihad a través de actos de propaganda, de financiación, de apoyo, de formación y de enseñanza de técnicas y tácticas terroristas, hasta llegar a una ejecución efectiva de los atentados”. Lo que dice el juez de la Audiencia Nacional es que esa organización virtual formada por foros, por páginas, puede ser considerada en sí misma una organización terrorista.

Conclusión. Es muy importante la participación de las Fuerzas y Cuerpos de Seguridad del Estado en esa lucha, y se les tiene que dar herramientas suficientes a la hora de combatir a esos grupos yihadistas que actúan en la Red. La desinformación o la infiltración son herramientas nunca reconocidas, pero que son de gran utilidad y que se han practicado en otros países. Los terroristas, de hecho, en los últimos tiempos insisten mucho en la necesidad de tener fuentes o grupos propios que no sean susceptibles de infiltración, porque tienen una especie de paranoia en la que continuamente se ven infiltrados, y aquí tienen parte de razón. Por eso, cada vez más, en todos sus foros se expide una especie de certificado de garantía para demostrar que es un verdadero foro yihadista no susceptible de infiltración. De ahí nacen las herramientas de encriptación.

Lógicamente, para dar sustento a esa infiltración y a esa desinformación, hace falta también un apoyo jurídico, equivalente al que se da a la figura del policía infiltrado, de agente encubierto.

221

La monitorización también es importantísima, igual que se vigilan las comunicaciones telefónicas, los servicios de información deben tener el soporte jurídico y los recursos técnicos y materiales para poder poner en permanente vigilancia esas páginas, los servicios de mensajería: WhatsApp, Skype, y todos los lugares susceptibles de poder ser objeto de intercambio de comunicación entre los terroristas islamistas.

La cooperación internacional también se hace imprescindible por el carácter global de la Red.

Y la reforma judicial. Ya en el año 2010, el Código Penal incluyó una pequeña reforma donde la formación, el adiestramiento y la captación de futuros terroristas era ya un delito en sí mismo. Ese es el camino que creo que hay que seguir. Hasta entonces ha habido muchas sentencias muy frustrantes en las que los jueces indicaban que había que esperar a que los grupos pasasen a la acción para poder enviar a prisión o condenar a alguien. Vemos muchas veces que no hace falta pasar a la acción para ser un elemento verdaderamente peligroso.



CUARTO PANEL

REDES SOCIALES Y COLABORACIÓN CIUDADANA EN LA ACCIÓN POLICIAL

JUAN JOSÉ ESTEBAN SERVUS

Director de Comunicación de la Dirección General de la Policía

La Policía Nacional ya hacía -y sigue haciendo- comunicación social al margen de la llamada web 2.0. antes de que este canal comenzara su andadura.

225

Hace más de tres lustros, había varios retos o puntos en los que era necesario poner todo el esfuerzo para que la labor diaria de la Policía y su eficacia fuera visible para los españoles, y la institución, gracias a esa labor profesional de comunicación, ganara en eficacia. Cuanto mayor sea la confianza en la Policía, ésta podrá desarrollar un mejor servicio al ciudadano.

Los medios de comunicación y las empresas de Internet apostaban fuertemente por los conocidos portales en Internet, cuyo uso aumentó geométricamente, hasta ser un referente informativo imprescindible a partir del año 2000, por su inmediatez, por la variedad de fuentes e informaciones accesibles a cualquier persona y por su disponibilidad gratuita, localizada por intereses y términos de búsqueda, gracias a los buscadores.

Esas empresas de telecomunicaciones, entonces todopoderosas, así como los grandes imperios mediáticos y medios de comunicación, compañías de televisión o productoras, junto a los clásicos diarios escritos y revistas de información general, eran el referente principal de la comunicación y como tales, eran imprescindibles para desarrollar cualquier misión o acción de comunicación.

Ya entonces era evidente como una parte importante de esa institución la del servicio público: ser útil a los ciudadanos en todas las necesidades posibles de seguridad. Desde siempre se ha solicitado colaboración ciudadana. Incluso desde hace bastante más de un siglo, tal y como reflejaba el típico cartel de las películas del viejo Oeste norteamericano, con el rostro del delincuente buscado, la recompensa y las palabras “Wanted” o “Reward”, esta última para incentivar la ayuda de las personas.

Esa petición de cooperación ciudadana ha ido evolucionando, adaptándose principalmente a los usos sociales y las posibilidades de comunicación, casi tanto como ha cambiado la forma de comunicarse la Administración con el ciudadano y, sobre todo, éste con las autoridades.

Continuando con la evolución de la comunicación en los últimos años, desde principios de este siglo se masifica el uso de Internet para informarse. Y aunque se pensaba que estaba ya todo muy desarrollado, a partir de 2006 llega otro cambio muy relevante para la información on-line: la aparición de Youtube y la aplicación paulatina de su tecnología por todo tipo de webs y medios digitales, para incluir de forma ágil y barata vídeos con los que complementar su información escrita.

226

La creación de Youtube no supone ninguna revolución técnica especial, pues ya existían los vídeos en la Red, incluso la llamada Televisión por Internet. Lo que supuso, sin ser ningún invento especial, fue facilitar a cualquier internauta la aplicación práctica de la televisión a la carta y el acceso a una tecnología que, hasta entonces, requería una inversión millonaria.

Hay que recordar la fiebre que se desató por los vídeos on-line y el nacimiento de un nuevo fenómeno, que hasta ese momento solo conocía algo similar con imágenes o presentaciones de fotos muy concretas: era el principio de los ahora ya célebres virales, vídeos que se distribuían con enorme rapidez y de forma muy extensa, gracias a que los internautas los compartían, atraídos por lo divertidos o impactantes que eran, y que los propios internautas grababan y colgaban en la Web.

El fulgurante éxito de Youtube fue aplicado por los medios de comunicación y empresas, y en la Policía Nacional tomaron nota de ello. Tras meses de reflexión en torno al potencial de Youtube para su aplicación en la policía, en mayo de 2007, tras una reunión con Google, se puso sobre la mesa las sinergias que había entre Youtube y la Policía Nacional, así como la utilidad de que esta última tuviera su propio canal en esa plataforma. La entidad policial fue una referencia dentro de la Administración

General del Estado por el lanzamiento y, sobre todo, por los contenidos que hacía accesible al público a través de esa videoteca tan popular.

www.youtube.com/policia tiene tres secciones, muy básicas:

- “Así es la Policía Nacional”, con vídeos que muestran cómo es la institución y cómo trabajan sus distintas unidades
- “Actuaciones de la Policía Nacional”, que presentan las acciones u operaciones puntuales de la Policía, la actualidad policial
- “Consejos de seguridad de la Policía Nacional”, apartado que incluye útiles recomendaciones para los ciudadanos que explican los agentes

No fue necesario ajustar el presupuesto en este ámbito, pues se emplearon recursos propios, abandonando la búsqueda de la calidad profesional por un espíritu amateur, natural, cercano, directo y real de los vídeos, que denominan “tipo Youtube”, en el que tan bien encajaba la austeridad policial.

El canal fue lanzado con un reportaje que mostraba el dispositivo de la Policía Nacional en un evento de relevancia, ¡todo un reto en seguridad!, 2.000 agentes de distintas Unidades trabajaron durante la semana de la final de la Champions en Madrid, con la misión de velar por el Bayern y el Intern y sus aficiones.

El soporte mostraba la excelente labor que realizan los agentes de la Policía Nacional en ocasiones como esa. Como en el resto de vídeos, la grabación y el montaje fueron realizados por los profesionales de Audiovisuales, agentes de la Policía.

El resto de vídeos iniciales eran de presentación de la institución, pero no tardaron en grabar un vídeo también novedoso y, sobre todo, muy útil para el ciudadano: los clásicos consejos de seguridad ciudadana para las vacaciones y el verano. Éste no ha perdido actualidad respecto a otros periodos estivales.

Poco a poco, se han ido subiendo nuevos vídeos a www.youtube.com/policia, pero sin ningún objetivo cuantitativo ni urgencia alguna para incorporar contenidos. De igual forma, el criterio para la grabación y emisión de los mismos han sido siempre la utilidad e interés de los vídeos para el ciudadano, por el tema, por la actualidad, etc. A estos axiomas de interés y beneficio se suma el de la información policial y, uno mucho más importante, la colaboración civil para la acción policial.

Y para buscar esa aportación, esos vídeos en Youtube mostraron y muestran un gran resultado, primero de forma independiente y, posteriormente, viralizados en las redes sociales. Algunos ejemplos de campañas de colaboración ciudadana que ha realizado la Policía con estos soportes han sido:

- El primero, uno de los delincuentes más buscados por la Brigada de Fugitivos. Estéticamente no era atractivo, pero que la gente entendió su importancia y el objetivo fue logrado: que los fugados fueran vistos por millones de personas que pudieran reconocerles. Meses después, uno de los fugitivos, conocido como “Cabeza de Cerdo”, se entregó ante la presión social que supuso verse en todas las televisiones e Internet
- Unos meses después, y en vista del éxito operativo que supuso esa acción, se lanzó otro vídeo, con las 10 obras de arte más buscadas por la Brigada de Patrimonio Histórico
- Posteriormente se publicaron otros soportes audiovisuales, como el que el Día de los Inocentes alertaba contra posibles fraudes, y otras campañas que se distribuyeron también a través de varias redes sociales:
 - Campaña de concienciación a las víctimas de la violencia de género
 - La *tweetredada* contra el tráfico de drogas
 - “Usa tu *smartphone* con inteligencia”, para celebrar el Día Mundial de Internet

En definitiva, Youtube, como videoteca de acceso permanente para el internauta ha dado un excelente resultado, no sólo cuantitativo (es el canal de una institución pública española con más visitas), sino, sobre todo, su utilidad para concienciar al ciudadano, informarle y facilitarle que colabore con la Policía.

Otra red social en la que la institución creyó ver beneficio para el ciudadano y eficacia para la comunicación de seguridad ciudadana fue Tuenti, la red social española por excelencia y cuyos usuarios son, de forma mayoritaria, muy jóvenes, algunos, según sus padres, demasiado. La Policía decidió apostar por esta red social como una extensión en Internet del Plan Director, que esta institución y la Guardia Civil realizan en los centros escolares españoles, para informar y explicar a los jóvenes las cuestiones más relevantes referida a la seguridad.

Desde el lanzamiento del Plan Contigo, denominación de la página policial en Tuenti, se pudo comprobar que la información a los jóvenes de cuestiones de seguridad cercanas a ellos y sus inquietudes, generó un rápido y fuerte seguimiento, convirtiendo esta página en la plataforma institucional líder en las redes sociales española. Con los meses, el Plan Contigo y sus 75.000 usuarios se consolidaron como referente indiscutible en España de concienciación e información o educación para los jóvenes, no sólo en España, sino también para los Ministerios de Educación o Interior de distintos países europeos.

Nuevamente, aquí lo importante no era la cifra de usuarios, realmente llamativa, sino la enorme utilidad de servicio público que se logró con esta plataforma, tanto en la información o concienciación como en la atención o ayuda al joven internauta. En el primer año de este programa, los agentes de cada especialidad atendieron más de 3.000 consultas o peticiones de ayuda, de chicos y padres que pedían asesoramiento o intervención de todo aquello que estuviera relacionado con la seguridad. Plan Contigo sigue recibiendo preguntas y peticiones de ayuda, y continúa primando las referidas a la seguridad y privacidad en las redes sociales, el ciberbullying o ciberacoso, y las consultas sobre el uso de imágenes, las injurias, el robo de cuentas, el robo de contraseñas, etc. y qué es legal y qué es delito.

229

Son decenas las acciones de comunicación que, en nombre de los agentes especializados de la Policía y la Guardia Civil, se han realizado a través de esa plataforma, con excelente acogida por sus usuarios, sus padres, el ámbito educativo, instituciones públicas y privadas, etc. Algunas de las más interesantes, que siempre se han tratado de realizar con la adecuada periodicidad, sin ser excesivamente machacones, dado el público al que se dirigen, son:

- Campañas de consejos de seguridad y privacidad para los menores en las redes sociales
- Test autoevaluadores y de concienciación sobre temas de especial relevancia en la seguridad de los jóvenes:
 - “Contigo sobre Navegación Segura en Internet”
 - “¿Te mueves seguro en la carretera?”, sobre seguridad vial
 - “¿Estás preparado para unas vacaciones seguras?”

- Campañas para alertar sobre la alcoholemia y la conducción, y el tráfico de drogas
- Concursos para concienciar sobre el acoso escolar. Han tenido un gran éxito de participación, a pesar de un premio prácticamente simbólico (1.000 euros)
- Campañas por la privacidad en las redes sociales y alertando de riesgos como el ciberacoso, el *grooming* (chantaje sexual a través de Internet), el *sexting* (envío de imágenes de carácter sexual que acaban siendo un problema), la usurpación de identidad y la recomendación de agregar a los perfiles personales únicamente a las personas que se conocen también en las redes sociales

Lo más importante de todo ello no ha sido la aportación cuantitativa, sino la cualitativa. Las consultas y peticiones de ayuda que se han atendido, bien directamente por los agentes que gestionan las redes sociales, bien por los especialistas, han mostrado una necesidad cubierta y una utilidad evidente para un sector de la sociedad en el que su seguridad es muy importante, no tanto para ellos como para sus familias.

230

Para entender las necesidades de seguridad de los jóvenes usuarios de Tuenti, basta con explicar que su Servicio de Soporte al Usuario recibe cada día 5.000 correos diarios de peticiones, consultas o reclamaciones vinculadas a su seguridad en esta red social.

Y también esta red se ha mostrado como un canal de comunicación muy útil para la operatividad policial. Varios de los correos recibidos se referían a cuestiones de clara ilegalidad y que exigían la intervención policial. Por otro lado, otra muestra del beneficio e interactividad de este programa de información y atención a través de Tuenti, es que se han recibido decenas de peticiones de centros escolares para que agentes de la Policía Nacional o de la Guardia Civil acudieran a explicar claves de seguridad a los alumnos.

La especial protección de la intimidad y privacidad de los menores, así como evitar poner en riesgo su seguridad, es una rémora a la hora de realizar más acciones de comunicación o colaboración con la Policía de estos jóvenes, pero los datos muestran que la relación con los jóvenes a través de las redes sociales funciona.

En redes sociales, el gran referente mundial es Facebook, una plataforma que cuenta con 800 millones de usuarios en el mundo y que es el objetivo

de comunicación y utilización por parte de empresas, instituciones, asociaciones, campañas, partidos y *mass media* para, básicamente, conseguir seis fines: informar; fidelizar; convencer; cohesionar a afines o potenciar una marca; generar tráfico hacia una web; y, cómo no, el sueño de todas las compañías: lograr lo que llaman “compras sociales”, vender a través de estas plataformas.

La Policía también fue precoz en Facebook, y lo hizo por varios motivos. En primer lugar, para conocer cuál era potencial en comunicación y las posibles ventajas de cercanía o máxima accesibilidad al ciudadano. En segundo lugar, para evitar que cualquier otra persona o entidad intentara apropiarse ilegítimamente del nombre o marca de la Policía, una práctica que, desgraciadamente, ocurre con mucha frecuencia en las redes sociales. Y en tercer lugar, para trabajar en dos aspectos operativos policiales: la atención al ciudadano y la participación de la sociedad, cuestión que es transversal a la presencia policial en la web 2.0.

La Policía Nacional –una institución que, esencialmente, es un servicio público para los ciudadanos, las 24 horas del día, que atiende a un 80 por ciento de la población española y que no sólo se ocupa de la investigación especializada sino también de la seguridad ciudadana, con sus agentes de uniforme–, debe tener un servicio institucional de atención e información al público. Está presente con comisarías y centros policiales en ciudades de más de 20.000 habitantes, desarrollando competencias de todo tipo en el ámbito de la seguridad.

231

El contribuyente –en definitiva, su “cliente”– reclama un óptimo servicio público y una transparencia e información detallada a través de todos los soportes posibles, así como conocer con claridad qué es legal y que no, cuáles son sus derechos y las normas a cumplir. Surge una evidente necesidad: atender de formar eficaz, ágil y accesible al ciudadano.

Atender a la población en Facebook y en Twitter no sólo sirve para ser útiles a la gente, sino también para que la Policía se muestre como un servicio público eficiente y adaptado a las tecnologías más innovadoras.

Facebook permitía la posibilidad de abrir al público una oficina de atención con los medios del siglo XXI. La institución tenía reservados tanto perfiles personales como páginas de la Policía. Los primeros, aunque no era lo apropiado, para evitar que otros los tomaran. Y la página, que aunque está desarrollándose todavía con perfil bajo, ya tiene la importante utilidad de atender al ciudadano, y más desde que Facebook permite que los usuarios envíen también mensajes privados.

Hoy día, tanto los organismos de distintas administraciones como las entidades privadas de cualquier sector, priorizan la comunicación bidireccional con sus usuarios, a través de infinidad de canales y plataformas existentes. Y un verdadero servicio de información al público sólo cumple su misión si no está escondido, si es útil, accesible y cubre una demanda o necesidad de su público objetivo. Si se ofrece un servicio y no se logra que la gente lo conozca o no está a su alcance, éste no logrará su objetivo: “lo que no se conoce, no existe”.

Facebook es en la actualidad un canal excelente, porque permite esa máxima difusión y accesibilidad a los españoles: cuenta con más de 15 millones de usuarios en España y el 96 por ciento de los internautas españoles la conoce. Un dato: esos 15 millones de miembros de Facebook no los alcanza la suma de los noticiarios de TVE, Tele5, Antena3 y Cuatro juntos, por ejemplo.

232 Facebook es líder claro entre los usuarios de redes sociales en España: el 89 por ciento la utiliza o visita, frente al 44 por ciento de Tuenti. Además, Facebook abarca un espectro de edad realmente general, frente al usuario tipo de Tuenti, muy joven. En Facebook ya están 3 generaciones: si bien al principio fueron los jóvenes y sus padres los que primero se inscribieron, ahora hay una presencia notable de “abuelos” en esta comunidad. Por género, señalar que las mujeres son mayoría frente a los hombres.

Con esta página de la Policía Nacional para informar, atender las dudas y las necesidades del internauta y ayudarle, se logra un servicio público transparente y eficiente para el ciudadano.

La razón de ir a Facebook fue la misma que la de otras muchas empresas: la accesibilidad máxima al internauta. Igual que en las ciudades la Policía trata de estar en los sitios más transitados, en Internet, también.

La elección de una red social masiva como Facebook ofrecía una gran accesibilidad y visibilidad de esa “ventanilla” de atención al ciudadano y, por tanto, un servicio de calidad. La web oficial (www.policia.es) tiene una estructura e información pensada más para otras funciones y contenidos, además de no poder competir en cuanto al tráfico de páginas y usuarios con las redes sociales.

En definitiva, se trataba de trasladar la clásica oficina situada en la plaza central de la ciudad al espacio virtual más accesible para los millones de “transeúntes” por Internet. De esta forma, además de atenderles, se les facilita que se enteren cuando la Policía solicita la colaboración ciudadana, y puedan hacerlo.

La Policía tiene presencia con perfiles y páginas reservadas en numerosas redes sociales, así como proyectos conjuntos de colaboración con otras plataformas y empresas de comunicación. Pero no quiere “estar por estar” en todo lo que huele a web 2.0, ni entrar en ninguna carrera o competición por formar parte de todos los espacios on-line posibles.

La plataforma on-line que más seguidores -y, sobre todo, utilidad, tanto policial como puramente informativa- ha aportado es Twitter, que algunos llaman red social, pero que tanto sus ejecutivos como la Policía consideran que también es una potentísima red de información-comunicación.

La Policía Nacional española fue una de las primeras instituciones que tuvo presencia en Twitter. Se dio de alta en marzo de 2009 y, desde el primer día, investigó el potencial de esta herramienta para su uso como soporte de comunicación. Asumió que si ese canal se desarrollaba como lo hizo, sería muy potente, capaz de hacer la competencia a las agencias de información como fuente para los medios e instituciones. El tiempo no sólo lo ha avalado, sino que ha mostrado una influencia y capacidad de transmisión por parte de Twitter enorme, muy superior a las previsiones más optimistas.

La Policía se planteó esta red de información como una herramienta de comunicación breve (el ya célebre tope de 140 caracteres), instantánea y accesible a gente bien informada, de forma cómoda, inmediata y a tiempo para ampliar. Y acertó parcialmente: lo que empezó siendo un público profesional de la información, institucional o tecnológicamente muy avanzado, se convirtió en una plataforma de información y comunicación bidireccional y su uso se masificó, hasta superar los 5 millones de usuarios en España.

En marzo de 2009 había muy pocos usuarios de la red del pajarito azul en España, y no había una forma fácil de conseguir lo más importante: ser accesible para los usuarios españoles. De hecho, el Cuerpo de Policía arrancó con un nombre que aún tiene reservado en Twitter, @policianacional y, a pesar de identificarse como la Policía española, recibía muchos seguidores y mensajes pidiendo información o ayuda de usuarios de toda Latinoamérica: Brasil, Argentina, Venezuela, Colombia, Ecuador, etc.

Poco a poco, consiguió seguidores de una forma muy discreta en cuanto al número, pero muy relevantes por la “calidad” de los mismos: instituciones, asociaciones, políticos, periodistas y agentes de opinión en España. En julio de 2009 no había vuelta atrás, y la Secretaría de Estado de Comunicación lanzaba la cuenta oficial del Gobierno, @desdelamoncloa, al igual que los

partidos políticos, principales empresas e instituciones, medios de comunicación y periodistas.

En 2010 contaba con un perfil de usuario muy elitista, apenas les seguían 3.000 tuiteros. Hoy puede parecer una cifra muy baja, si se compara con los 225.000 que tiene en la actualidad, pero ya entonces era un soporte de comunicación muy eficaz: los 3.000 seguidores eran lo que la gente del marketing llama el *target* o “público objetivo” que como Gabinete de Prensa se busca, además de cuerpos policiales y agentes de policía de todo el mundo.

En Twitter los Cuerpos de Policía de todo el mundo han sido, como en otros muchos ámbitos, pioneros en su utilización, que la mayoría emplean para la información de Servicio Público al ciudadano y la actualidad policial. Desde el Federal Bureau of Investigation (FBI) a policías locales de todo el mundo, se puede hablar no de cientos, sino de miles de cuentas corporativas de Fuerzas de Seguridad de todo tipo.

234 La utilidad informativa, desde el punto de vista de comunicación corporativa unidireccional era y es evidente. De hecho, sólo en España, en los últimos meses no sólo los cuerpos policiales, sino también servicios de emergencias con mayor o menor tamaño o competencia, cuerpos de bomberos, Delegaciones de Gobierno y organismos locales, autonómicos y estatales, tienen su cuenta en Twitter.

Los primeros mensajes eran bastante sobrios, sin foto, meros titulares de información policial. Poco a poco la Policía fue probando, aprendiendo, experimentando y ampliando el contenido y utilidad de su cuenta, comprobando la mayor o menor eficacia de esos mensajes. E interactuando, dialogando con los usuarios para aportarles algo con su respuesta.

De los primeros 3.000 usuarios, el 70 por ciento eran el público que se buscaba desde el Gabinete de Prensa, pero al llegar a los 10.000, ese porcentaje de profesionales de la comunicación o representantes institucionales se fue diluyendo, hasta no llegar en la actualidad al 10 por ciento de sus *followers*. Son los perfiles de más de 20.000 entidades o profesionales.

El resto de seguidores son también muy importantes, y no sólo porque la hacen la institución pública líder en España en seguidores y el segundo cuerpo policial del mundo, tras el FBI.

Es especialmente importante la eficacia en la función de la comunicación y en una cuestión mucho más relevante: la acción de “ventanilla cibernética” de la Policía Nacional, tanto en la vertiente de atención al ciudadano en sus

dudas y necesidades de seguridad, como en la formación y concienciación del ciudadano ante cuestiones de seguridad, como las alertas tecnológicas, recordatorios de medidas y riesgos fundamentales de la época y, cómo no, la colaboración ciudadana que se consigue al promover y canalizar a través de las redes sociales.

Hace ya muchos meses que se superaron los 10.000 *followers*, una masa crítica más que suficiente para centrar el contenido y planificación de Twitter en la atención policial del internauta medio, en vez de pensar en un enfoque profesional desde el Gabinete de Prensa para medios y periodistas. Con el tiempo, la Policía ha ido asumiendo el rol que los tuiteros le han dado con su apoyo masivo y múltiples consultas: es el referente indiscutible de la seguridad en español en Twitter, para lo bueno y para lo malo. Los ciudadanos les piden ayuda, felicitan o protestan por cualquier cuestión sobre seguridad o noticia policial.

La gente felicita o critica a la institución por todo tipo de actuaciones de cualquier cuerpo policial, y preguntan por sus necesidades de seguridad a todos los niveles, sin importarles que sea un caso de consumo (curiosamente, una pregunta o petición muy frecuente es perseguir a las empresas que hacen *spam* telefónico), de seguridad vial (cuando, por ejemplo, un famoso sale en la televisión cometiendo una infracción, recibe decenas de tweets pidiéndole que se le sancione o detenga...), de protección civil (pautas para evitar desmayos y requerir asistencia médica en determinados acontecimientos) o de los bomberos o agentes forestales, en el caso de los incendios más relevantes acaecidos en los montes españoles.

235

Ese papel de referente de la seguridad que le han adjudicado los tuiteros españoles, supone una enorme responsabilidad, todo un reto de gestión que conlleva, además, varios inconvenientes que asumen, al margen de la satisfacción que supone reforzar la “marca” de la Policía Nacional en España y Latinoamérica.

Igual que asume con naturalidad y responsabilidad esa representatividad global de la seguridad en español en esos casos, lo hace muy frecuentemente con alertas, información, consejos, orientación o respuestas sobre temas de seguridad cuya competencia legal no es de la Policía Nacional, pero con cuestiones que no implican vinculación normativa alguna.

Curiosamente, los *tweets* más retuiteados (repicados o redistribuidos por los *followers* para compartirlos con los suyos) son los de fraudes de consumo o alertas ante algunos riesgos de seguridad ciudadana (robos al descuido en unas circunstancias conocidas o sufridas por bastante gente, etc.).

Ese interés o demanda de la gente porque la Policía le sea útil y cercana le ha obligado a trabajar mucho, tanto en el contenido como en la forma de dirigirse a ellos: cercana, clara, coloquial, llamativa, a veces, hasta provocadora, dependiendo del tema.

Algunas instituciones y sus responsables aún creen que una entidad debe ser muy formal u oficialista en el tono en todos los soportes o canales en los que esté presente, y sea cual sea el motivo de la comunicación. La Policía tiene muy claro que no: no es lo mismo una comparecencia parlamentaria u oficial del Ministro del Interior o el Director de la Policía, que la resolución de un caso que generaba gran preocupación social, el aviso ante un posible fraude cibernético o la alerta por un virus que trata de asustar y estafar al internauta por supuesto almacenamiento o visionado de pornografía infantil; la preocupación, dolor y homenaje a compañeros fallecidos heroicamente en acto de servicio; el lanzamiento de una campaña por los principales artistas de la música española o un videoclip grabado por la Unidad de Audiovisuales que muestra cómo es el trabajo de la Policía en el Distrito Centro madrileño, uno de los que más movimiento tiene en España.

236

Twitter, como es el caso de Tuenti, Youtube o Facebook, no es el Boletín Oficial del Estado (BOE) ni la Orden General de la Policía, ni tan siquiera, la web oficial de la Policía española. No hay que olvidar que es una empresa privada, con sus normas, que se tienen que acatar y que pueden cambiar o moldear a su gusto. Si no hubieran tratado de adaptarse a la plataforma y a sus usuarios, es probable que se hubieran quedado como un canal oficialista, para la Prensa e instituciones, y no como el referente universal de la seguridad en Internet.

Los resultados cualitativos obtenidos son más que satisfactorios, y no sólo por las decenas de felicitaciones y mensajes de apoyo que recibe a diario, ni por el importante y evidente refuerzo de la imagen de la institución, tanto en su globalidad como en lo que los profesionales de la comunicación denominan “reputación on-line”. También, ha logrado optimizar la difusión de sus noticias y actividad cotidiana a través de esos nuevos canales, y ha puesto en valor la labor de la Policía Nacional, sus agentes y las respectivas Unidades en su especialidad. De igual forma, ha realizado esa función de “ventanilla” de Atención al Ciudadano, en la que tratan de resolver no sólo sus dudas, sino sus consultas y necesidades en su seguridad, a todos los niveles. Se anticipan con sus consejos y alertas tecnológicas o de seguridad ciudadana, muy vinculadas a la actualidad o a las vivencias, riesgos y prácticas más comunes para todos los ciudadanos, formándoles en cuestiones útiles y previniéndoles. Esas funciones y contenidos no po-

drían realizarse en la web de la Policía, pues jamás conseguirían el tráfico que obtienen gracias a esas redes sociales.

Las funciones puramente policiales son un valor añadido que sólo ha sido posible gracias al rotundo éxito cuantitativo y plena consolidación del perfil policial en Twitter, como plataforma eficaz para la institución.

La primera muestra del potencial de Twitter como canal de utilidad policial se obtuvo con las distintas operaciones policiales contra la pornografía infantil en Internet. La distribución y tenencia de pornografía infantil puede que sea de los delitos que más conmueven a los ciudadanos normales. Ese rechazo social absoluto se transforma en una movilización de los internautas que la Policía percibe gracias a estas redes sociales, y en el caso de Twitter, el número exacto de retuiteos (veces que se comparte o repite) de su mensaje. El correo que se da habitualmente tras informar de una operación contra la pornografía infantil y sus correspondientes datos es: “Por favor, Retuitear: La colaboración ciudadana es clave contra la pedofilia” y se incluye una cuenta de e-mail para denunciarla: denuncias.pornografia.infantil@policia.es. El mensaje aquí expuesto fue compartido 1.469 veces, lo que supone que pudo llegar a cientos de miles de personas, dependiendo del número de seguidores de cada perfil (de media, el número de los seguidores de cada perfil superan ampliamente el centenar, pero las personas que se implican en estos temas suelen ser gente de gran predicamento en esta red).

237

La Brigada de Investigación Tecnológica (BIT) de la Policía Nacional ha desarrollado en los últimos años numerosas operaciones contra redes e internautas que compartían contenido de carácter pedófilo, y en varias de las operaciones realizadas tiene constancia de la vinculación directa de la colaboración ciudadana.

Esa colaboración es inducida o solicitada directamente por la Policía, pero también ha vivido en estos años varios ejemplos de asistencia de los internautas. Hay varios ejemplos que muestran la utilidad de ser accesible a los ciudadanos: hace dos años, un internauta contactó desde un país latinoamericano porque creía que podía facilitar información de utilidad para la Policía española sobre personas vinculadas al terrorismo de las que él tenía conocimiento allá. Se comprobó en Internet quién era él, y se le dio la suficiente credibilidad como para seguir esa línea de investigación y facilitarle el contacto directo y confidencial a la Comisaría General de Información, al ver que tenía una trayectoria razonablemente creíble.

Otro aspecto en el que aparece la colaboración ciudadana y que se procura no fomentar, por los riesgos y complejidades operativas que conlleva, es

la utilidad del 091: gente que comunica cualquier incidencia o petición de intervención a través de la mención pública en Twitter. La Policía se enteras mucho antes por los mensajes de los tuiteros de cualquier cuestión, como una amenaza de bomba, escándalo, intervención llamativa, etc., que por la información remitida por teléfono desde las respectivas Unidades centrales o Responsables de Prensa de la Jefatura correspondiente. Un ejemplo: la Policía conoció la detención de José Bretón, en Córdoba, por periodistas tuiteros, antes de que informara el Responsable de este tema tan relevante socialmente y antes de que llegaran teletipos de las agencias de información y a las web de los medios sobre el tema.

También ha ocurrido que han alertado de supuestos atracos y robos, pero, además de comprobarlo con la Sala del 091, por si hiciera falta enviar a una patrulla al lugar, se le solicita al tuitero que también llame a la referida Sala, por motivos de operatividad y credibilidad de la misma. Además, se evitan los problemas que surgirían si se diera la misma validez policial a este canal que al 091, más eficaz y con más recursos. No atender alguna petición de ayuda urgente e importante por este canal tras anunciarlo como canal de máxima operatividad –o dejar que la gente lo interprete como tal– sería un error de gestión por parte de la Policía.

238

La institución no quiere convertir esa red social ni ninguna otra en un canal oficial de comunicación, para evitar riesgos que no tiene porqué asumir. Por ejemplo, en la huelga general que se convocó el 29 de marzo de 2012, desde la madrugada se solicitó a los tuiteros que indicaran las incidencias y solicitarán la ayuda policial utilizando el 091, y no las decenas de mensajes que se recibieron durante esa noche para contar acciones violentas aisladas, sabotajes o acoso a determinadas empresas para que cerraran. La gente sabe que la llamada al 091 es lo suficientemente seria como para pensárselo, y puede llegar a no valorar suficientemente que, en un momento de ofuscación personal, pedir supuesta ayuda o intervención policial es algo muy serio, por mucho que sea a través de Twitter y de forma más o menos anónima.

Pero la interactividad con los tuiteros es fundamental, por varios motivos. Quizás el más positivo para la Policía como responsables de difundir información y consejos de seguridad es que los toma de ellos mismos. Cada día recibe entre 10 y 30 consultas o peticiones para que se investiguen posibles fraudes, engaños, riesgos de seguridad, prácticas irregulares, enlaces de webs o anuncios sospechosos, etc. Eso, sólo a través de las menciones públicas. Otros piden una cuenta de correo para enviar información detallada de forma privada. Todos ellos sirven de ayuda.

Son muchos los agradecimientos o felicitaciones que la Policía recibe por sus consejos o avisos, sea cual sea la práctica detectada: *phishing*, *sexting*, minifraudes telefónicos, virus, etc. Esos mensajes son claros, con un lenguaje directo, nada oficial.

Mención especial en este punto merece un virus que en 2012 hizo estragos, según especialistas tecnológicos: se trataba de un intento de estafa que se hacía pasar por la Policía Nacional española y decía haber detectado que el ordenador que había recibido esa notificación había visto pornografía infantil, por lo que se le indicaba que era sancionado con 100 euros de multa y hasta que no pagara no se le desbloquearía. Ese virus, masivo y muy dañino para los ordenadores, además de ser un intento de estafa, mutó en supuestas multas de la Policía y la Sociedad General de Autores de España (SGAE) por descargas de archivos ilegales y sanciones de la Policía y la Agencia de Protección de Datos por uso irregular de datos. Cada día, cientos de personas se vieron afectados por este virus, muy extendido en España. El Gabinete de Prensa recibió cientos de llamadas pidiendo información y ayuda, y la Dirección de Comunicación emitió alguna nota de prensa, y una treintena de veces la alerta a través de Twitter, para tratar de avisar a la gente. Aun así, fueron muchos los que, asustados, pagaron, y tras hacerlo se enteraron del fraude en el que han picado. Desgraciadamente, al igual que la mayoría de prácticas de *phishing*, no es fácil actuar policialmente con la fuente del mismo, ya que operan desde otros países y las estafas las realizan a través de canales que no son fácilmente rastreables.

239

La Policía ha proporcionado todos los pantallazos que los usuarios afectados les han remitido del conocido como “virus del porno”, para que sirva de ejemplo al resto, y lo sigue recordando de forma periódica, mientras considere que puede ser útil para el internauta medio. Cada vez que recuerda esta estafa, facilita el enlace de la Oficina de Seguridad del Internauta, (www.osi.es), en el que se dan los pasos a seguir para solucionarlo.

Otro ejemplo muy similar de asistencia ciudadana fue la de contar a la gente los minifraudes telefónicos, que tratan de que el usuario llame o envíe uno o varios SMS de tarificación especial con artimañas o engaños varios. El ciudadano lo cuenta a la Policía, el Cuerpo se cerciora de que es intento de fraude y lo avisa, para que la gente no pique. Para evitar problemas legales no proporciona las dos últimas cifras del teléfono, pero consigue que cuando el ciudadano recibe esa llamada perdida, sepa qué es. Al mismo tiempo, pide a los afectados que lo denuncien, para poder actuar policialmente contra ellos.

Al hablar de participación ciudadana, destaca la importancia de que se impliquen tuiteros de gran predicamento o seguimiento en esa plataforma,

para multiplicar el alcance de los mensajes, consejos o peticiones de colaboración. He aquí dos ejemplos: un personaje televisivo muy conocido en España remitió un caso de intento de secuestro de su cuenta en Twitter. Es una práctica más frecuente de lo que parece, en especial en el correo electrónico, con el fin de enviar *spam* desde fuentes conocidas y así con más credibilidad para el internauta. En las redes sociales lo intentan con las cuentas cuantitativas más relevantes, para conseguir llegar al mayor número de personas con un solo *tweet*. Gracias a ese célebre tuitero, la Policía pudo alertar a través de Twitter de ese riesgo. Este mismo *tuitstar*, como se conoce popularmente a las cuentas con cientos de miles de seguidores, volvió a colaborar poco después con el Cuerpo Nacional de Policía al retuitear una petición de colaboración ciudadana, con una reacción inmediata: aumentar muy notablemente la repercusión del mismo, hasta conseguir varios millones de impactos en unos minutos. Ese caso fue el de la colaboración que la Policía inglesa pidió a través de la organización Crimestoppers a las Fuerzas y Cuerpos de Seguridad españoles, para tratar de localizar a un ciudadano de nacionalidad británica que podría ocultarse en el sur de España tras haber asesinado a un matrimonio y sus dos hijas en el Reino Unido. La reacción a la petición policial de ayuda fue excepcional: miles de retuiteos, que suponen millones de impactos y que mostraron que el uso de las redes sociales para la colaboración ciudadana, bien utilizadas, puede ser muy eficaz.

La Policía tiene claro su potencial, pero también la importancia de ser inteligentes en su uso y siempre, con criterios profesionales, tanto policial como de comunicación.

Un criterio policial que ha impuesto en su Twitter es relacionarse con los el resto de tuiteros con la máxima privacidad o confidencialidad posible, y eso lo lleva al máximo en los casos de colaboración ciudadana, facilitando cuentas de correo para evitar riesgos operativos, de seguridad o de privacidad. E insiste especialmente en esta cuestión si esa cooperación se trata de denunciar pornografía infantil.

Si se habla de ayuda ciudadana, eficacia policial y redes sociales, hay que mencionar la acción más eficiente desarrollada hasta ahora. Algunos especialistas afirman que es un ejemplo idóneo de uso de los nuevos canales con resultados directos de operatividad policial en el ámbito internacional. Es lo que llamamos *Tweetredada*, campaña con la que se pretendía facilitar a la gente una forma fácil, directa y eficaz de colaborar en la lucha contra el narcotráfico.

Cuando llegó el actual Director de la Policía, Ignacio Cosidó, pidió a la Dirección de Comunicación que potenciara el uso de las redes sociales, no

sólo incrementando los seguidores, sino cuidando al máximo la atención y ayuda al ciudadano y que, además, se diera un paso más, intentando que esos canales aportaran lo máximo posible no sólo a la imagen policial, sino también a las labores propiamente policiales. El aumento, desde los 60.000 usuarios con que se empezó en el año 2012 a los más de 216.000 seguidores actuales, demuestra que se logró la mejora cuantitativa. Respecto a la utilidad policial, se describe con un ejemplo de la *tweetredada*.

Para lanzar esa campaña la Policía creó una cuenta de correo con buena usabilidad, recordable y que invitara a colaborar (antidroga@policia.es). Además, diseñó un cartel, para poder transmitirlo vía Twitter y en los medios de comunicación. Y por último, grabó un vídeo, para solicitar a través de Youtube esa colaboración.

No contó con profesionales para el cartel, tampoco el vídeo era especialmente bueno, y la invención del término para lanzar la campaña (*tweetredada*) también generó críticas y chanzas, que la Policía recibió a través de las redes sociales. Pero los cientos de referencias a la campaña y cuestiones anecdóticas colaterales en estas plataformas mostraron que la campaña iba a ser un éxito. Los medios de comunicación tardaron horas en convertirlo en uno de los temas del día, en Internet, televisión, prensa, radio, etc. con lo que el objetivo fue conseguido.

241

La sorpresa y alegría llegó cuando desde la Brigada Central de Estupefacientes, empezaron a dar cifras de e-mails operativamente válidos recibidos en esa cuenta. Se alcanzaron cifras realmente impresionantes. Un mes después se habían descartado 500 correos por inútiles, pero otros 2.000 habían sido gestionados por la propia Brigada Central o derivada a las respectivas brigadas provinciales. Algunos correos daban detalles sobre investigaciones ya en curso por la Unidad de Drogas y Crimen Organizado (UDYCO), y otros muchos servían para abrir nuevas pesquisas. Pronto se hicieron las primeras detenciones por tráfico de drogas, a pesar de que muchas otras continuaron investigándose, para tratar de llegar a un distribuidor principal, al máximo nivel de narcotráfico posible. El balance de esta acción fue fantástico, y debe servir de referencia para intentar conseguir nuevos éxitos policiales a través de estas herramientas.

Respecto al narcotráfico, la Policía también trata de hacer pedagogía, con mensajes que cualquiera puede interpretar como un aviso a navegantes: cada vez que se hace una operación contra productores y distribuidores de marihuana con los cultivos hidropónicos en domicilios y plantaciones en terrazas o jardines, informa a la gente de la detención, con fotos de dichos cultivos. Estas noticias son de las más retuiteadas por los ciudadanos, lo cual

demuestra que a la gente le interesa (probablemente, por empatía), hasta le divierte, pero al mismo tiempo sirve para recordar qué es delito y qué no, y que el narcotráfico se persigue en todas sus escalas, no sólo a los capos que la intentan introducir en España.

El potencial de estos canales para la colaboración ciudadana se observa también en un caso que se produjo en 2012: el día que España se alzaba con la Eurocopa (1 de julio de 2012), con todo el país con la mirada puesta en esa final en Ucrania. La Policía ya tenía previsto dar algunos mensajes de información útil para el ciudadano y, tras ganar la Selección española, pedir a la gente una celebración respetuosa con los demás y segura.

242 La persona que estaba de guardia, al finalizar el partido, detectó algo muy extraño en un día con un acontecimiento deportivo y social de tanta visibilidad como la Eurocopa: en ese momento, tres de los diez *Trending Topic* correspondían al grave incendio que asoló 50.000 hectáreas de monte en Valencia. Entre los muchos *tweets* que solicitaban información y ayuda para esa zona de Valencia, obviando, una vez más, que no era competencia de la Policía (que fue la única institución oficial de la Administración General del Estado que tuiteó esa noche), el agente vio uno que consideró oportuno modificar y retuitear: la petición de colaboración ciudadana desde una localidad valenciana para que acudieran voluntarios con motosierras y tractores con cubas que permitieran el transporte de agua.

La respuesta fue impresionante. En sólo unos minutos, mientras Casillas alzaba la Eurocopa y millones de aficionados celebraban la victoria también a través de las redes sociales, ese mensaje de colaboración ciudadana fue retuiteado al instante por miles de personas. En dos horas, desde las 11 de la noche hasta la 1 de la madrugada, se superó los 10.000 retuiteos, que supuso millones de impactos y lo más importante: el mensaje fue lo más visto en Valencia, según datos internos.

La Policía fue, junto a alguna institución oficial de la Generalitat valenciana, la referencia en Twitter sobre este tema de máxima importancia y urgencia. A pesar de ello, la institución fue prudente y evitó un excesivo protagonismo en una cuestión que no era de su competencia.

Lo más importante de este caso fue comprobar la enorme capacidad de estas redes sociales como canal de colaboración ciudadana, en un caso de emergencia como fue ése, a pesar de coincidir temporalmente con un acontecimiento que monopolizó el interés de los ciudadanos fuera de Valencia: el triunfo español en la Eurocopa.

Hay que tener muy claro que ese potencial ha de manejarse con oportunidad, profesionalidad, inteligencia y moderación, para asegurarse de que es un canal con credibilidad para el ciudadano y máxima eficacia para la Policía.

Dejando al margen los delitos de tráfico de drogas comentados anteriormente, la Policía tiene muchas veces consultas y peticiones de ayuda para personas muy conocidas en Twitter, que reciben el acoso y persecución de sus *trolls*, ciberacosadores que amenazan e insultan directamente a profesionales muy conocidos o personajes públicos a través de las redes sociales. Cada día recibe peticiones de los fans, seguidores o amigos de determinados personajes públicos para que ayude a su ídolo frente a lo que ellos creen que es una actividad delictiva que está sufriendo. Hay casos famosos como el de Eva Hache y Juanma Castaño, o los menos conocidos del humorista Santi Rodríguez, o de periodistas y políticos de primera fila.

Tanto si los propios amenazados como si alguien de su entorno solicita ayuda, la Policía les atiende de forma privada, para asesorarles y ayudarles en todo lo que necesiten. La institución es cauta en este tema, porque hay mucho usuario que confunde el odio, las burradas y provocaciones de fans deportivos o de gente muy radicalizada en ideologías políticas antagonistas con amenazas o injurias. Hay más gente de la que parece que se cree que Twitter es como un recinto en el que la Policía puede y debe poner orden ante el ciberacoso y ofensa, haya o no delito, y ese no es así, el Cuerpo Nacional de Policía no puede ni debe ejercer de profesor en el patio del colegio a la hora del recreo.

243

Alcanzar el número de seguidores que la Policía tiene y que participan y retuitean sus mensajes no es una labor de corto plazo, sino pensada y labrada durante años, con una estrategia siempre *largoplacista*. En esos años ha realizado diversas campañas y acciones de comunicación, para fomentar la vinculación del tuitero con el organismo público: desde las referidas campañas contra la pornografía infantil a la campaña para que se denuncie la violencia de género, fomentar el uso seguro de los *smartphones* o consejos de uso seguro de Internet, que dan los artistas más célebres de la música española. También ha organizado un concurso de microrrelatos, conmemorando efemérides y jornadas relevantes en el ámbito de Internet, y ha desarrollado decálogos e información relacionada con la época o acontecimientos de actualidad.

Ha llevado a cabo también un *tweetencuentro* con los internautas para solventar las dudas tecnológicas o la *tweetpatrulla*, con dos agentes femeninas de la Policía para celebrar el Día de la Mujer Trabajadora.

También tiene un perfil en inglés, @SpanishPolice, que le permite, por un lado mantener informados y comunicación bidireccional con los numerosos medios, profesionales y residentes interesados en la actualidad policial española, en especial, la que ocurre en zonas con gran presencia de extranjeros (la costa mediterránea y archipiélagos, principalmente). Y es un canal a través del cual también mantiene las relaciones institucionales con las Fuerzas y Cuerpos de Seguridad de otros países.

Todas esas acciones, con el trabajo y preparación que requieren, no sólo tienen un resultado inmediato, sino también esa vinculación a largo plazo que, con el tiempo, se ve plasmada en la confianza y credibilidad generalizada en la sociedad española, como demuestra su liderazgo entre las instituciones.

Esa labor en las redes sociales ha sido reconocida en España por profesionales, compañeros, instituciones y usuarios, pero también fuera de España: representantes de cuerpos policiales de otros países la han visitado para conocer su trabajo, y contactado vía email y vía redes sociales.

244 En resumen, la Policía está en la web 2.0 con el objetivo de mejorar de forma directa la seguridad de los usuarios en España, aumentar la confianza en la seguridad de Internet y la labor de las Fuerzas de Seguridad en la Red, realizar un servicio público eficaz para el ciudadano y, cómo no, obtener toda la utilidad policial posible de esta herramienta tan potente de comunicación.

Los objetivos principales de la Dirección de Comunicación en la gestión de las redes sociales son: conseguir una buena imagen de la Policía, sus agentes y acciones; un Internet más seguro y unos ciudadanos mejor informados y más tranquilos; un canal de comunicación directo con los internautas y, por último, una especial ambición, que comparte con la Dirección General, y que es promover y facilitar la colaboración ciudadana a través de esos canales de una forma eficaz y segura.

La presencia de la Policía en las redes sociales está muy reflexionada, trabajada y analizada, tras meses de estudio. La labor ya realizada ha sido muy intensa, tanto en la planificación como en la creación del contenido (información de servicio público, consejos, aplicaciones, noticias, videos, eventos...) y la atención a los miles de usuarios. Entre los retos del futuro está desarrollar aún más esa cooperación de los internautas, mejorar la eficacia policial.

Las redes están cambiando la forma de trabajar de la Policía, que debe seguir evolucionando aún más, reforzando sus capacidades en seguridad y comunicación en esos entornos, aunque lo hecho hasta ahora sitúa a la institución en la vanguardia mundial de las redes sociales. El Cuerpo Nacional de

Policía ha aprovechado la oportunidad de dar un salto tecnológico importante en su comunicación con el ciudadano, que se ha visto ya recompensada en el salto cualitativo que ha supuesto en la percepción de la gente (en especial, los internautas), como una institución orientada a atender al ciudadano y adaptada a los nuevos medios de comunicación.

POLICÍA 3.0

SANTIAGO CUADRO JAÉN
Excomisario General de Seguridad Ciudadana (1996-2004)

A lo largo de la historia, el Cuerpo Nacional de Policía (CNP), adecuándose a los cambios de la sociedad, se ha ido mimetizando con el entorno, de manera que ha ido ajustando su respuesta a la demanda. La institución ha llevado a cabo distintos procesos de cambio y, en la actualidad, está ante un nuevo escenario que le lleva a la necesidad de transformarse nuevamente, es decir, de adaptar su respuesta a las exigencias y demandas actuales.

247

Estamos en un contexto en el que la Red se plantea como un entorno multiformato en el que coexisten una variedad de representaciones inmensas, donde hay una accesibilidad casi permanente y una disponibilidad de información constante, es decir, a cualquier hora se puede entrar. Pero tiene un inconveniente, traspasa las fronteras nacionales y, por tanto, somete a los ciudadanos y a la Policía a importantes riesgos. La delincuencia también se está adaptando a ese contexto, está aprovechando las ventajas que le reporta el empleo de las nuevas tecnologías.

La evolución en el acceso y uso de Internet ha progresado muchísimo en muy pocos años. Desde 2002, se han multiplicado por cuatro los hogares conectados a la Red y en las empresas también se ha incrementado, aunque no en esos porcentaje. Pero, en cualquier caso, se ha producido un ascenso, una tendencia al crecimiento sostenido de siete puntos en la Web y de 30 puntos en los teléfonos móviles, entre 2002 hasta 2011. La consultora americana Gartner, en un estudio que realizó entre mayo de 2009 y agosto de 2010, observó cómo el desarrollo de los móviles iba a tener una gran influencia en la evolución hacia nuevas influencias, no sólo en la Red, sino en acciones cotidianas. Por ejemplo, en nuevas oportunidades de ocio. En la mayoría de los casos se trata de descubrir cuáles son las plataformas que puedan venir bien para llevar a cabo actividades.

IOS (Sistema Operativo de Iphone), de Apple, cuenta con una cuota de mercado en torno al 56 por ciento; Android con el 25 por ciento (Android es la fusión de Google y Sintia); y Sprint, el 19 por ciento de cota, éste es uno de los sistemas que se podía considerar como más seguro. CAI advertía que Android iba a ascender más del doble con respecto al resto de competidores, y realmente así ha sido, y se ha posicionado prácticamente en el primer lugar, junto con Apple.

En el mercado se ha pasado del correo convencional al correo electrónico, de los periódicos en papel a las cabeceras en formato digital y, con ellas, surge una gran cantidad de información y ha generado un problema tremendo en el mundo de la prensa, con la desaparición de una gran cantidad de diarios.

Pero no queda ahí la cosa, sino que además, en el año 2009, y ya en el año 2011, empiezan a aparecer iniciativas cuyo objetivo es cambiar el ámbito económico mediante la creación de nuevas monedas. Éstas han comenzado en Japón y en Estados Unidos, y se han empezado a realizar transacciones, y algunas compañías de negocios ya se posicionan en torno al manejo y a la promoción de este tipo de monedas.

248 Esto ha generado, sobre todo en relación con el blanqueo de capitales, distintas acciones. Por ejemplo, hace tres años, el Federal Bureau of Investigation (FBI) desarticuló una red, pero las restantes siguen ahí. Es lo que pasa en este campo, en el que lo que se ve es, simplemente, la punta del iceberg, es decir, cada negocio tiene toda una cadena de distribución de trabajo por detrás y un mercado, que se llama de “economía sumergida”, que está causando enormes problemas a los Estados, sobre todo desde el punto de vista de lo que es el empleo por parte de la financiación.

En el paso inmediato, el que abarca de 1996 al año 2000, la criminalidad se manifestaba con los hacker. Era una acción donde el reto personal movía a esta gente, y no se producía un afán de modelización de lo que estaban haciendo, que es lo que posteriormente ocurrió.

Del año 2001 a 2004 la situación empieza a cambiar y aparecen los primeros *fishing* masivos, aunque, a diferencia con lo que ocurre hoy día, la estructura de los grupos criminales, la consolidación de estos, el desarrollo organizativo y su aprobación, a tenor de la lista de estos países, era totalmente distinta, con una relación mucho mas consolidada y donde el principio de división de trabajo está muy estructurado. La terminología de la Era Antigua, Media, Moderna y Contemporánea es un símil que puede servir para definir cómo ha ido evolucionando la acción criminal en un corto periodo de tiempo.

En el periodo 2005-2006 comienza un cambio en la tendencia del fraude, y continúa el proceso de modernización. Aparecen las primeras *botnets*, las cadenas de ordenadores zombi utilizadas por grupos criminales que les hacen el trabajo, de manera que todo la acción que llevan a cabo está en un entorno transparente, y prácticamente no se ve. La acción de esos botnets se ha utilizado en diferentes momentos de la historia, y hoy día también se emplean.

También esa es la etapa de los gusanos, que son otro de los virus, otro tipo de *malware*, que empieza a establecer una cadena superior, a reproducirse a sí mismos en algunas redes sociales, concretamente en las de Google, que nace en 2004, o en las de Yahoo. Hoy existen otras redes sociales y también hay una evolución superior de los gusanos, que comienza con Conficker, que es un gusano que utilizan para cazar antivirus y que ha seguido manifestándose y replicándose a sí mismo. Esa es la posibilidad y la versatilidad que tiene ese tipo de *malware*.

El año 2007 hay un avance superior, un afán de modernización de los nuevos criminales, que empiezan a concebir la infraestructura, tanto del fraude como de prácticas de actividades criminales, con grupos organizados donde aparecen nuevos negocios, donde cambian el marketing, cambia el sistema de mercado, aparecen empresas que realmente se dedican a esta actividad criminal.

249

De este escenario se pasa, en el año 2011, al *gansterismo*, donde proliferan los ataques, aparecen pseudoejércitos o ciberejércitos, y donde se han ido produciendo asaltos, por ejemplo de India contra Pakistán. Son situaciones que, muchas veces, no tienen trascendencia en los medios de comunicación generalistas, pero que se están produciendo. Al final esto se visualiza en prensa y revistas especializadas, foros, blogs y este tipo de soportes de información.

La novedad se perfila en el bienio 2005-2006, en donde comienza un cambio cualitativo y cuantitativo, en el que se pasa de los ataques puntuales y esporádicos a agresiones cotidianas, con acometidas, principalmente, a entidades financieras, pues son, en principio, la forma de hacer dinero rápido. Poco después se lanzan hacia todo aquello en donde hay posibilidad de hacer riqueza, donde el incremento de los *smartphone* pone a los ciudadanos ante los criminales “a los pies de los caballos” y, donde lanzarse a un procedimiento es cada vez más complicado. Ahí es donde entran los Cuerpos que tienen responsabilidad de velar por la seguridad de los ciudadanos, en este caso el Cuerpo Nacional de Policía.

La mayor parte de estos delitos están contemplados en el Código Penal, sin embargo, empiezan a aparecer figuras que no. Una relación de estas acciones delictivas son: movilización de los directores, del *fishing*, una gran cantidad de *fishing* a través de *malware*, que son troyanos, gusanos, virus, el *ransomware* –que es lo que sigue al falso antivirus– o ataques de negación del servicio. Recientemente, se han abierto diligencias en la Sala II de la Audiencia Nacional, teniendo en cuenta la cantidad y la imputación de todo ese tipo de denuncias.

Como botón de muestra de cómo ha ido creciendo ese impacto de la acción criminal, en un análisis estadístico que desarrolla la empresa que se dedica a la prevención del Servicio Nacional para acciones como el *fishing*, las *webcam*, que son las estafas a través del correo electrónico, los troyanos, etc., éstas se han ido incrementando entre los años 2010 y 2011.

250 Las modalidades de *fishing* se pueden realizar mediante campañas rutinarias, como el regalo de teléfonos móviles, u otras de carácter estacional, como puede ser la de la recaudación de la renta. Esto es algo reiterativo y que se produce en diferentes Estados, por ejemplo, el pasado año en el Reino Unido facilitaron la web de todas las entidades financieras para recaudar por parte de quienes tenían que recibir la devolución sobre el importe de la renta. En esa institución, de manera estacional aprovechan motivos múltiples, por ejemplo, el día de San Valentín, Navidad, etc. para hacer esas campañas mediante correo electrónico. Es aquí donde los grupos criminales emplean las tácticas como el *farming* o el *fishing*, que redirige al usuario de una web legítima a una web ilegítima.

Está demostrado que los grupos criminales tienen una estructura bastante consolidada, con unos departamentos de marketing importantes y atentos constantemente a conocer cuál es la mejor vía para poderla aplicar a su “negocio”, ideando fórmulas para captar datos relativos a credenciales bancarias, tarjetas de crédito, todo aquello que puedan de alguna manera negociar; en otros casos, el robo de bases de datos o de información o el robo del perfil en redes sociales. Es decir, van en esa dirección de forma continua. Una fórmula es inventarse noticias falsas, de manera que inciten a la gente a acceder y, automáticamente, se descargan el *malware*.

Una técnica que también se está utilizando es la del posicionamiento en buscador, es decir, se dedican a ver qué noticias son aquellas que tienen un público muy destacado en las páginas de Internet para introducir ahí el virus, de manera que la persona se conecta a esa noticia se infecta y en cualquier transacción que realizan se pone en marcha automáticamente. También esa técnica de posicionamiento en buscadores se produce cuando

el usuario rellena el formulario del impuesto de la declaración de la Renta. En este caso, los delincuentes colocan su página delante la oficial con lo que, cualquiera que llegue, automáticamente entra y queda infectado.

El siguiente paso es la monetización, es decir, cómo obtener dinero de las acciones criminales que están llevando a cabo. En este caso, hay que hacer hincapié en torno a cada elemento de este ecosistema:

- En primer lugar, hay que empezar a desarrollar iniciativas para gastar el dinero, y éstas son infinitas
- Posteriormente, hay que montar el negocio para traducir aquello que se está pidiendo con ese capital. Aquí entran los muleros, y tiene gran relación con conceptos que están asociados a robo de información de tarjetas de crédito por distintas vías

En cuanto a los muleros, hay diferentes tipos:

- El inconsciente, es la persona ansiosa de tener un trabajo que entra en páginas de empleo o recibe algún correo de esta naturaleza y, automáticamente, se engancha. A estos les llaman agentes de transferencias locales o agentes de transferencias internacionales
- El ocasional “funciona” por precio. Viene a cobrar entre un 10 y un 20 por ciento de comisión
- El mulero profesional se lleva el 50 por ciento o puede estar en torno al 40 o 60 por ciento de la comisión, y a veces forma parte de la propia organización o es una empresa de seguridad

251

En este caso, incluso se establecen ediciones por entradas concretas de determinado soft o garantía de compensación, en el caso de que ocurra algún problema.

En torno a esto, posteriormente, se mueve también todo un sistema relacionado con aspectos dirigidos a ocultar la efectividad de las operaciones, con vistas a evitar detenciones por blanqueo de capitales, etc.

Desde el punto de vista del Farming (recolección mediante medios ilícitos de tarjetas de crédito), también en Internet se ofrece en el mercado negro tarjetas de crédito y Visa oro, ventajas que proporciona el precio, incluso la posibilidad de ver diferentes fotografías sobre lo que son los especímenes de cada uno de estos elementos o la venta de hologramas asociados a la entrega,

y también para la adquisición de billetes. Ese ámbito se está desarrollando en Sudamérica, en España todavía no se está moviendo, pero teniendo en cuenta la acción de globalidad que tienen estas “iniciativas”, no quiere decir que en ese país no se pueda poner en marcha también.

Lo mismo ocurre con los pasaportes, desde los más baratos, como pueden ser los de Georgia (1.000\$) o Azerbaiyán, el de España son 5.320\$, etc., o los permisos de conducir. También existe este tipo de ofertas con tarjetas de crédito, tanto en Europa como en Estados Unidos, y ahí están Visa, MasterCard y su precio son 650 dólares. También hay páginas donde se ofrece la posibilidad de realizar falsificaciones de tarjetas de crédito o de tarjetas de identidad, el permiso de conducir, de pasaporte, etc.

252 Los *ransomware* son una amenaza –señalan al usuario que sus archivos están encriptados y que si no paga el rescate automáticamente los pierde–, y empiezan a adquirir formas mucho más sofisticadas. En principio comienzan por la instalación de falsos antivirus bajo la excusa de que la persona ha accedido a lugares de dudosa reputación –páginas de pornografía para adultos, de pedofilia– y obligan al usuario a pagar para devolvérselos. Como ya se indicaba, la Audiencia Nacional está tramitando diligencias como consecuencia de una gran cantidad de denuncias que afectan a ese tipo de acción.

Esto se puede traducir, posteriormente, y en el ámbito de la seguridad ciudadana, en alteración del orden público y daños asociados como: convocatorias de cualquier tipo, ataque a instituciones y empresas, Gobiernos, ciudadanos, etc.

Esto está muy relacionado con el uso de las redes sociales. Éstas están siendo un instrumento más de lo que es la comunicación orgánica entre grupos criminales, bien sean de naturaleza terrorista, violenta, política, etc., que envían informaciones que rozan lo que podría considerarse delito, si no lo son, y en las que hay una incitación clara a la violencia.

En cuanto a la victimización, hay una encuesta que encarga Symantec a la empresa Norton, que la lleva a cabo en 24 países con una muestra de 19.636 personas. De ellos, la mayor parte son adultos, maestros en una proporción importante, concretamente más de 2.000, a los que se consulta acerca de su percepción de si en algún momento determinado han sido víctimas del delito de ciberdelito. La encuesta concluye que en el año 2011 un total de 431 millones de personas han sido objeto de engaño o robo, con un millón de víctimas diarias, 50.000 por hora, 820 por minuto y 50 por segundo.

El 69 por ciento señala que han sufrido delito, al menos, una vez en su vida, y se ha incrementado en torno a un 3 por ciento esa cifra en relación con el periodo anterior. Y en cuanto a la totalidad de las víctimas, el 65 por ciento lo ha sido en el año 2011. Si se observa el comportamiento de los troyanos, del *fishing* en los años 2010 y 2011, se advierte que se ha producido una evolución paralela.

En cuanto a la incomodidad que esto representa, el 44 por ciento manifestaron que se habían sentido molestos y el grado de incomodidad es tanto como puede ser el delito en el mundo físico (no se habla de delitos de lesiones ni de otro tipo, es decir, hay que matizar en su contexto: no han sido víctimas de atraco ni les han dado un navajazo).

Por otra parte, se observa que tres de cada cuatro personas son conscientes de poder ser víctimas cuando están on-line, con lo que la percepción de inseguridad que existe es bastante importante; que dos de cada diez han denunciado los diferentes hechos; que seis de cada diez consideran que tienen menos posibilidad de ayuda en el caso de que sea algún delito de cibercrimen; y que nueve de cada diez dicen que la medida está encaminada para llevar a esta gente a los tribunales.

Si comparamos ésta con la encuesta que hace el Centro de Investigaciones Sociológicas (CIS) sobre cifras oscuras, se observa que hay algunos tipos delictivos que tienen natura muy parecida, concretamente lo que hace referencia al vandalismo, que no se denuncia en un 81 por ciento de los casos, y el abuso de autoridad, que tampoco se denuncia. El primero que se denuncia es la agresión sexual, no la violación, y las estafas están en torno al 80 por ciento. Esta cifra es importante, principalmente en el aspecto de la demanda de la sociedad para que se haga algo en relación a poner a los delincuentes entre rejas.

La víctima puede ser cualquiera, ciudadanos, empresas, Gobierno y, por sectores, tanto la administración como los particulares. En el caso de empresas, un ejemplo es el robo de 70 millones de datos a Sony en 2011 o al Parlamento de Justicia de Estados Unidos.

Ante la pregunta de si las instituciones, en este caso los Cuerpos de Seguridad, pueden ser víctimas, la respuesta es sí.

Los datos que se recogen de un informe elaborado en el año 2011 por una empresa en Reino Unido, país que se caracteriza por tener todas las actividades catalogadas, hasta los que consideran intangibles -el daño emocional, de recuperación de las víctimas, etc.-, reconoce que sobre ese

tema basan sus conclusiones, muchas veces, en suposiciones o bien en comentarios de expertos, fuentes del Ministerio del Interior o del Ministerio de Justicia, pero que realmente no hay nada palpable y evidente en cuanto a denuncias tramitadas y en la probación de los daños provocados por esas denuncias. Sin embargo, establecen tres grandes vertientes: los ciudadanos, los daños en patrimonio en diferentes manifestaciones y en las empresas -por pérdida de negocio, bien sea por ataque o por la recuperación del desastre ocasionado en la producción, comercialización, distribución, venta por pérdida de confianza, reducción de facturación, rentabilidad, reputación, pérdida de producciones e inversión- y el Estado -disminución de ingresos fiscales, inversiones extranjeras por pérdida de confianza o continuidad en el crecimiento-.

En Reino Unido y para 2010, la valoración que hacen está establecida en esas tres grandes vertientes es: en robo de antivirus on-line es en lo que se manifiestan con más asiduidad; en el caso del Estado es en el fraude en la Hacienda central y locales, por pérdidas del sistema de pensiones de la Seguridad Social y, en el caso de empresas, productos de propiedad industrial, intelectual, datos de clientes, etc.

254 Esta encuesta también hace referencia a que los daños por carácter global son 388.000.millones de dólares, que dividen en:

- La recuperación del tiempo perdido, que se establece en función de los países, la media del tiempo de recuperación, que en el caso de España son seis días, en otros son 16 jornadas y en Reino Unidos e Irlanda son cuatro días
- Los costes directos. En España lo valoran en 5.900 millones de euros, de los cuales 432 millones son el impacto de la recuperación del tiempo perdido, que según se señalaba está en seis días

En cuanto al objeto, o al medio, o bien a los procedimientos del móvil, la advertencia se ha ido manifestado de esta forma, el *malware* aparece desde el punto de vista genérico, a continuación ya se cita y toma como objetivo la actividad financiera y, a partir de ahí, empiezan a desarrollarse familias de *malware* que no solamente atacan a las entidades financieras, sino a todo lo bueno. Las funciones que empieza a adquirir el *malware* son multidisciplinarias, ya que para acceder a la banca on-line automáticamente se teclea el password y la contraseña. Para adquirir esos datos, el software lo que hace es ver cómo puede captar las pulsaciones del teclado y, automáticamente, incorpora funcionalidades de captura.

Los *malware* están mejorando su sistema, desarrollan posibilidades en el software de manera que empiezan a gastar vía *fishing*, o vía de otro tipo de *malware*, o troyanos, etc., y obtienen esa información. Además, envían un segundo factor de autenticación vía móvil, y lo que hace el software es que coloca un elemento en medio que, de forma transparente para el usuario, automáticamente le roba la información.

A partir de ahí comienzan a controlar la información, robo de certificados, el acceso de la cámara de la web y del micrófono, la lectura de las imágenes del ratón, cambian la configuración del antivirus, llega el troyano y coloca sus motores antivirus, con lo que cualquier ataque automáticamente lo va a rechazar. Además, se meten en fondo del sistema operativo y no hay posibilidad de detectarlos. Las marcas de antivirus empiezan a introducir nuevas modalidades para ir mejorando. Esto es una carrera de obstáculos en la que los delincuentes siempre van un paso por delante, y automáticamente van ganando.

Por otra parte, el incremento de sistemas con detectores va a afectar, indudablemente, a las amenazas, y va a provocar la opción de congelar todo tipo de información, por ejemplo los nuevos tipos de *malware* van, y ya se hace, a provocar lo que son la generación de botnes controlables de forma remota. Y hay una realidad: el VMware, que es el mismo sistema de *fishing* pero llevado a punto virtual. Esto va a traer también problemas de seguridad.

255

Por otro lado, Internet ofrece todos los servicios, con lo que el usuario no tiene que tener nada almacenado, pero la empresa de almacenaje ya está siendo objeto de ataques por lo que se llama “la japete”. Por otra parte, hay una convergencia en que todos los grupos, sean de naturaleza terrorista, organizado o de cualquier otro, ya han utilizado o están utilizando las mismas herramientas porque le están dando buenos resultados.

Es una realidad actual que cada vez hay una mayor especialización en los ciberataques, y que esa complejidad, y la densidad del ciberespacio, van a traer una mayor cobertura. Además, los ataques que tienden a infectar todo lo que el usuario tiene en su casa: el ordenador, el router, el teléfono móvil, pues las infecciones alcanzan una dimensión global y, desde luego, hay cada vez un aprovechamiento mayor de las redes sociales para diferentes funcionalidades.

Las empresas de *hosting* son las que prometen servicios de internet y las que están utilizando servidores a todas horas, que son aquellos que tienen un mayor nivel de resistencia y, a partir de ahí, ese servidor se utiliza para mandar *spam*, *modem*, *scam* y toda esta fauna que existe, además de para el tema de casinos ilegales, pornografía infantil, etc.

Las redes sociales están siendo, en primer lugar, como objeto del delito, en segundo lugar como plataforma de provisión de selectivos, como herramienta de distribución de *malware*, o herramienta de comunicación, reclutamiento y apoyo, tanto al ciberterrorismo como al crimen organizado. También como instrumento de cambio, de hecho Anonymus está utilizando, y algún que otro también, las redes sociales para que sean un instrumento de cambio de la sociedad. Algunos se están apuntando a ello, sobre todo desde el punto de vista económico, como es el tema de la prueba virtual cifrada, que implica que los módulos no se comportan exactamente igual. Esto lo emplea el crimen organizado ya que cuando se ataca un modulo y se siguen las trazas para llegar a la cabeza, realmente no se alcanza dentro de ese mar de confusiones.

En cuanto al medio, las *Botnets* (redes de bots) son unas redes infectadas que se manejan por control remoto desde un ordenador central implicado en todo tipo de actividades. Desde el punto de vista político, terrorista, del crimen organizado, del lanzamiento de páginas *topping hit*, es un elemento que también empieza a ser utilizando fundamentalmente en el contexto de las ciber. Pero no solamente son los ordenadores, también son los router y los teléfonos móviles.

256

El impulso de las redes sociales lleva a que sean consideradas también como objetivo. Hay un caso de LinkedIn en el que en una página web rusa se produjo el robo de 6,4 millones de contraseñas, y lo mismo ocurrió con la NBC en Facebook o en Twitter.

¿Medio de distribución de *malware*? Ésta es la única *bookface* que se dedica a distribuir lo que es el *flashware* previamente, a distribuir *malware* por esa vía a través de Twitter o Facebook mediante una noticia.

El caso de los grupos sociales que usan Facebook, Twitter o diferentes redes, realmente lo que hacen es pedir que la gente se incorpore y que lleven a cabo una serie de iniciativas con vistas a que la acción que están poniendo en marcha tenga éxito.

Y en cuanto a la tendencia de ciberejércitos, estos van evolucionando. Es decir, los ciberpatriotas o seguidores de anónimos, o los *hacker*, van progresando en lo que ha sido este año el ciberejército programado, es decir, se han detectado ataques a la Universidad de Cambridge por el ejército histórico de Siria, o de Rumanía contra Francia y Reino Unido por determinadas cuestiones, o Pakistán contra India y al contrario, etc. Son manifestaciones muy corrientes, y de hecho en el año 2012 hubo 815.000 ataques*.

*Fuente: Zona H

En la ciberguerra está el caso de Agne, que estuvo muy dirigido hacia lo que fue Irán y aquí es donde se autoriza por parte de la ciberguerra y el nuevo hardware, inventado por los norteamericanos contra las centrales nucleares. En el caso del móvil es diferente, y como ejemplo está este mensaje de Anonymous:

“Españoles, somos Anonymous, el día 16 de febrero de 2012 en la manifestación protesta del instituto Luis Vives de Valencia otra vez ha habido duras cargas policiales. El día anterior, 15 de febrero, se han vuelto a producir similares situaciones siendo esta vez seis los detenidos. Estas y estos jóvenes han sido detenidos cuando participaban de la protesta masiva contra la brutal carga policial que el miércoles tuvo lugar también en el mismo sitio que se saldó con la detención de un menor.

Ambas carreras han sido en palabras de la mayoría de personas que estaban allí totalmente injustificadas y ejercidas contra estudiantes que en su mayoría tenían entre 13 y 17 años. Los procedimientos los mismos, pelotas de goma contra las personas, no se puede tolerar ningún tipo de abuso policial en la tarea de velar por el orden en protestas ciudadanas, menos aun en protestas pacíficas que reclaman unos derechos que están amparados en nuestra propia constitución e inaceptables si las víctimas de estos abusos son menores de edad.

257

Desde Anonymous avisamos a la Policía de España que es inaceptable que las cargas policiales se sigan sucediendo una detrás de otra con una agresividad cada vez mayor, por ello exigimos la dimisión inmediata de la Delegada del Gobierno Paula Sánchez de León ante una situación de violencia que está fuera de control. La Policía está para velar por el orden y no para abusar de la fuerza, no dejemos que esto se quede en el olvido, es intolerable. Desde Anonymous hacemos un llamamiento al mundo para atacar a su web estrella.

Policía de España, ya estamos hartos de esos abusos, de palizas sin control, de intimidaciones, de sus porras, de sus botas con punta de acero, de que no se identifiquen cuando van a usar la fuerza, vuestras acciones son inaceptables, es hora de actuar no les tenemos miedo, ustedes deben tenerlo ahora, les advertimos que cesen con tales brutalidades contra la gente indefensa, contra estudiantes, contra menores de edad, contra gente que lucha por sus derechos, etc. no descansaremos. Gentes del mundo levantaos, no tened miedo, apoyen a esta lucha contra la policía, han cambiado las tornas y ahora jugamos nosotros, hablamos en nombre de España, Colombia, Venezuela, Guatemala, Honduras, México, El Salvador, Argentina, Republica Dominicana, Perú, Chile, Bolivia, Uruguay, Costa Rica, Cuba, Ecuador, Nicaragua, Puerto rico y toda Latinoamérica, somos Anonymous, somos legión, no olvidamos, no perdonamos, Policía de España, te esperamos”.

El comunicado lo que está transmitiendo es muy claro, por ello hay que incidir sobre si los Cuerpos de Seguridad son o no víctimas, y si están preparados para dar la respuesta adecuada, no solamente en cuanto a la propia defensa sino en cuanto a decir lo que realmente les compete en relación con los ciudadanos, la defensa de los derechos y libertades. Y es en ese sentido en el que se encamina el desarrollo de la propuesta o del programa “Policía 3.0”, que ya se está llevando a cabo por parte del Ministerio del Interior y la Dirección General de la Policía, encargadas de incrementar la conciencia de la gente sobre los riesgos y, desde luego, sin obviar el papel tan importante que se lleva a cabo por Unidades especializadas en la investigación de este tipo de hechos.

258 A cuenta de lo observado a lo largo de este tiempo, el mensaje va un poco más allá. Se deben combinar las vertientes de anticipación y prevención con la de respuesta. Las razones serían, por una parte, la actuación a la demanda social, aunque ésta en este caso sea ya porque no hay una petición unánime, a diferencia de lo que está ocurriendo o lo que puede ocurrir en el caso de que asociaciones de vecinos que se levantan y empiezan a tener reuniones con el Comisario de Distrito porque se ha incrementado el número de robos o porque las personas que van al mercado no están seguras, etc. en este caso no, es totalmente diferente, pero se observa que, de manera silenciosa, van avanzando numerosas, infinidad de modalidades delictivas que están ocasionando un serio daño a todos.

Por otra parte, la naturaleza y la persistencia de la amenaza tienen múltiples percepciones y objetivos, como se ha podido observar.

También hay que contar que siempre va a existir una cifra oscura que no se puede contabilizar. De hecho, en su momento se pusieron en marcha iniciativas, como la denuncia telefónica o vía internet, con vistas a hacer aflorar ese tipo de conocimiento y dar una mejor respuesta desde el punto de vista de la prevención, y mejorar la eficacia Cuerpo Nacional de Policía. Eso llevaría a concentrarse en un escenario en el que se tendrían que producir cambios asociados, fundamentalmente, a los procesos, tanto desde el punto de vista operativo como desde el punto de vista de la formación, y este último es esencial; o bien cambios de naturaleza estructural, no solamente lo que son las cooperancias de determinados órganos o la creación Unidades. De hecho, la Dirección General de la Policía está en esa línea y ha habido un cambio reciente en la Brigada de Investigación Tecnológica, que se convierte en Unidad de Inteligencia Tecnológica dentro de la Consejería General de información, con lo que eso conlleva.

En cambio, desde el punto de vista normativo es necesario llegar al conocimiento del impacto de la ciberdelincuencia en la economía o en su

estructura empresarial y social. Y hay que gestionar el conocimiento con vistas a especializar el desarrollo de procedimientos de investigación, teniendo en cuenta lo compleja que es el análisis de este tipo de hechos, que trascienden las fronteras nacionales.

En el tema del cambio hay dos reflexiones: el del individuo y el de la proyección. El cambio en el individuo normalmente va asociado al desarrollo de programas de formación, o de concienciación en este caso, y es cuestión de estructurarlos bien. Desde el punto de vista del cambio en el diseño organizativo hay otro componente sobre la estructura, los puestos de trabajo, los sistemas de deflexión etc.

La acción de desarrollo de iniciativa tiene dos grandes componentes: la anticipación o reflexión y la respuesta. En estos ámbitos también interviene la prevención, que va asociado al campo de la Seguridad Nacional y protección.

En la seguridad privada, que es otra competencia que tiene la Dirección General de la Policía, concordante con el desarrollo de la Ley de Protección de Infraestructura Física cuyo sentido fundamental es el de prevenir ataques dirigidos contra esa infraestructura, desde el punto de vista del empleo de las nuevas tecnologías se les encomienda función de supervisión y, por tanto, requieren además de unos conocimientos superiores a los que actualmente tienen, para ver en qué medida pueden supervisar los planes, tanto de centrales nucleares como de cualquier otra institución.

259

La entidad u organismo que esté sujeta al desarrollo de esa Ley o desde el punto de vista de la protección, Unidades de protección que están a cargo de la defensa de la integridad personal de aquellas personas sujetas a protección, como pueden ser miembros del Gobierno o cualquier otro.

¿Qué ocurre con el perfil en redes sociales respecto de la familia, de agenda o de cualquier otra noticia que está a la vista de todo el público y sobre el que se puede atentar?, ¿puede hacerse? Es necesario empezar a cambiar el chip, en lo que hace referencia tanto a la captación y al tratamiento de la información, desde luego con vistas a la acción preventiva.

Y en ese sentido también se habla del ámbito de la investigación, tanto desde el punto de vista de Policía Judicial como de otras acciones. Unas forman parte del ámbito competencial de la Policía Judicial, otras de la Comisaría General de información y otras de la Comisión de Extranjería-tráfico de seres humanos y otra serie de hechos significativos-. El ámbito de Policía Científica se corresponde con la analítica forense, la profundidad

de las acciones y la aportación a la autoridad judicial sobre indicios que permitan condenar a los detenidos.

La propuesta es la creación de un Centro Nacional de Prevención y Respuesta.

¿Qué ocurre con la información sobre el conocimiento de los hechos delictivos que están ocurriendo o han ocurrido y que afecta a los derechos de personas y de los que los Cuerpos de Seguridad no tienen conocimiento?, es porque a las entidades financieras les resulta muchísimo más barato acallar ese tipo de datos, puesto que les supone un gran coste el empleo de equipos de asesores para solucionarlos. Eso implica que no se conoce el volumen de fraude porque, indudablemente, tiene un gran impacto en la confianza de los ciudadanos. Eso es un escenario en el que el ciudadano está totalmente desprotegido.

Los Cuerpos de Seguridad no tienen capacidad para proteger al ciudadano porque no tienen la estructura adecuada, y eso ocurre en muchos países. Por tanto, hay que empezar a adoptar medidas para corregir eso, teniendo en cuenta que siempre se irá un paso por detrás de los criminales.

MESA REDONDA:

REDES SOCIALES Y DELITOS SEXUALES

ALFONSO SAN ROMÁN IBARRONDO

Fiscal Delegado de Criminalidad Informática de Madrid

Se juzgaba a un hombre que mató a sus padres y al terminar el juicio, en su turno de última palabra, pidió clemencia alegando que era huérfano. Este hecho lo contaba Abraham Lincoln, que antes que político fue abogado, describiendo el tiempo de gran confusión en que le tocó dirigir su país¹. Este tipo de incomprensibles alegaciones se realizan en los Tribunales cuando se juzgan algunos delitos informáticos. He aquí dos casos reales. El primero se produjo en un juicio en el que se acusaba a una persona por posesión y distribución de archivos de pornografía infantil compartida a través de las redes P2P. El acusado alegó que no sabía ni que lo compartía ni el contenido de los archivos. La realidad comprobada del mero examen de la distribución de carpetas y archivos del disco duro de su ordenador era que buscaba, mediante un programa peer to peer, y los por su nombre relativo a pedofilia y movía esos archivos a carpetas donde los clasificaba por su temática concreta (palizas, violaciones, etc.).

261

El segundo ejemplo de estas situaciones paradójicas se produjo en el curso de un juicio celebrado por *child grooming*². Al inicio del juicio, que

1.- "He reminds me of the man who murdered both his parents, and then when sentence was about to be pronounced pleaded for mercy on the grounds that he was an orphan." Abraham Lincoln.

2.- INTECO define el grooming como "un acoso ejercido por un adulto y se refiere a las acciones realizadas deliberadamente para establecer una relación y un control emocional sobre un niño o niña con el fin de preparar el terreno para el abuso sexual del menor."

se prolongó durante varias semanas, la defensa aportó una información de INTECO sobre el *sexting*³. Durante las jornadas del juicio se aludía siempre al *sexting*. Finalmente declaró un perito de parte, médico de profesión, que explicó que los hechos podían ser considerados como *sexting*. Se citan estos ejemplos porque, en algunas ocasiones, se intenta confundir a los Tribunales aprovechando la novedad de este tipo de delitos. Así no es infrecuente que quien demuestra con los hechos ser conocedor de la informática por el hardware y software que maneja, por la configuración personalizada y avanzada de los programas que utiliza, por la sofisticación de la herramientas informáticas instaladas en su equipo, etc., pretenda que apenas tiene conocimientos informáticos y que no sabe bien cómo sucedieron los hechos. Volviendo al hecho narrado por Lincoln, sería como si al asesino de sus padres se le aplicara una atenuación por el hecho de ser huérfano.

PEDOFILIA Y PEDERASTIA

Tanto la pedofilia como los delitos contra la libertad sexual en su conjunto han existido desde antiguo. Se ha estudiado si la aparición de las nuevas tecnologías, especialmente Internet, ha favorecido o no este tipo de delitos. Mi opinión es que sí. Internet ha favorecido estas conductas por los siguientes motivos:

- 1) Permite la comunicación entre pedófilos/pederastas de todo el mundo.
- 2) Se apoyan mutuamente sobre ideas falsas que sustentan una especie de filosofía que permitiría este tipo de relaciones como algo natural.
- 3) Comparten ideas sobre cómo atraer a sus potenciales víctimas.
- 4) Pueden elegir a sus víctimas usando técnicas de selección (ingeniería social, data mining, etc.) para detectar los perfiles más propensos. Para ello, acceden a los chats de adolescentes y a las redes sociales.
- 5) Incluso pueden seguir a grupos enteros reuniendo a las potenciales víctimas por distintos criterios (localidad, colegio, edad, etc.).
- 6) Facilidad para disfrazar su identidad, género, edad y, por supuesto, intenciones.
- 7) Posibilidad de establecer una relación de larga duración para lograr su objetivo.

3.- INTECO define el *sexting* como “la difusión o publicación de contenidos (principalmente fotografías o vídeos) de tipo sexual, producidos por el propio remitente, utilizando para ello el teléfono móvil u otro dispositivo tecnológico.”

- 8) Acceso a espacios privados de la víctima (domicilio, lugar de estudio, etc.), donde existe una menor vigilancia por parte de padres y cuidadores.
- 9) Pueden, de forma sencilla y asequible, dificultar la trazabilidad de su rastro digital utilizando diversas técnicas y servicios informáticos (VPN, programas que permiten la navegación más anónima, uso de redes ajenas, etc.).

LEY PENAL Y JURISPRUDENCIA. ALGUNOS ASPECTOS DE LA INVESTIGACIÓN Y ENJUICIAMIENTO DE LAS CONDUCTAS PEDÓFILAS

El pedófilo de la era anterior a Internet se encontraba aislado y sus acciones debían ser muy cautelosas para evitar ser descubierto. Además, las legislaciones nacionales establecían una intensidad muy distinta en cuanto al reproche de estas conductas. Hoy mismo, fuera de Europa y algunas otras zonas del planeta, la pedofilia es admitida y no constituye delito alguno.

También conviene echar la mirada atrás para adquirir un poco de perspectiva histórica. Hasta hace pocos años no era infrecuente el considerar la pedofilia como una cuestión privada. Para ser sinceros, ha sido la Unión Europea y otros organismos internacionales los que han espoleado el cambio legislativo en esta materia. Se han emitido directivas y resoluciones muy exigentes para que se plasmara en las legislaciones penales de los países miembros una legislación severa en orden a reprimir el tráfico y tenencia de este material⁴.

263

4.- La resolución del Parlamento Europeo relativa a la protección y derechos del niño de 20 de noviembre de 1997 recoge en su número 5º la necesidad de “prohibición total de la producción, del comercio, del transporte y de la tenencia de material que incite a los abusos sexuales contra niños.”

La Decisión 2000/375/JAI, de 29 de mayo de 2000, relativa a la lucha contra la pornografía infantil en Internet, señala una serie de medidas que deben ser obligatorias para los proveedores de Internet, entre las que debe destacarse la información a las autoridades acerca del material pornográfico infantil que se difunda a través de ellos, la retirada del material, salvo que las autoridades decidan otra cosa, la conservación de datos del tráfico de acuerdo con la ley y durante el tiempo que prevean las leyes nacionales y la creación de sistemas de control para combatir la producción, tratamiento, posesión y difusión de material pornográfico infantil.

La Decisión Marco 2004/68/JAI del Consejo, de 22 de diciembre de 2003, relativa a la lucha contra la explotación sexual de los niños y la pornografía, tiene como objetivo armonizar las legislaciones penales de los Estados miembros en relación con estos delitos. A tales efectos contiene una definición de qué debe entenderse por pornografía infantil en su artículo 1 y establece en sus artículos 2, 3 y 4 los comportamientos que deben ser castigados, incluyendo la producción de pornografía infantil, la distribución, difusión o transmisión de pornografía infantil, el ofrecimiento o facilitación por cualquier otro medio de pornografía infantil, y su adquisición o posesión.

Al mismo tiempo, como reacción, se ha producido una presión de los pedófilos para que sus acciones se vean como algo normal. Esta presión es fuerte y bien organizada. Las redes sociales permiten a estas comunidades (es el caso de los “boylovers”⁵) organizar eventos sociales y reuniones anuales.

La terminología pornografía infantil y pornografía de adultos no es del todo precisa. Da a entender que son como especies del mismo género. En cualquier caso, la pornografía es una actividad lícita en nuestra sociedad. Mientras que la posesión y tráfico de pornografía infantil es un delito, además de una injusta explotación de personas y que ocasiona perjuicios en el normal desarrollo de los menores que lo sufren, causando un daño muchas veces irreparable.

La distinción entre pornografía infantil y pornografía, en el ordenamiento español se concreta, en una primera aproximación, a que la primera se elabora con menores de 18 años o incapaces y que la segunda se produce con mayores de edad. Sin embargo, la cuestión del concepto y alcance de la pornografía infantil no es pacífica⁶. Además, la jurisprudencia ha mantenido que la imagen del desnudo de una persona menor de edad no adquiere, por sí mismo, carácter pornográfico. El carácter pornográfico deriva de la actitud sexual reproducida en el material de que se trata⁷. En cualquier caso, con carácter general, no suelen plantearse dudas sobre cuando una imagen es o no pornografía infantil.

5.- El llamado «movimiento del “amor” hacia los niños» pretende que la pedofilia sea tenida como una opción más en la sociedad. Se trata de un movimiento muy activo en la Red. Desde el punto de vista de la lucha contra la pedofilia se ha considerado que promueve y facilita compartimientos delictivos. Se han desarrollado varias iniciativas para bloquear las páginas de este movimiento con la base legal de que atenta contra el mandato constitucional de protección de la infancia y la juventud.

6.- Una definición de pornografía infantil se encuentra en el Convenio sobre la Ciberdelincuencia, realizado en Budapest el 23 de noviembre de 2001 (BOE de 17.9.2010), firmado y ratificado por el Reino de España. En el artículo 9.2 define la pornografía infantil como todo material pornográfico que contenga: a) un menor comportándose de una forma sexualmente explícita, b) una persona que parezca un menor comportándose de una forma sexualmente explícita, y c) imágenes realistas que representen a un menor comportándose de una forma sexualmente explícita.

El punto 3 del citado artículo explica que por “menor” deberá entenderse toda persona menor de 18 años si bien permite que cualquier Estado parte pueda establecer un límite de edad inferior, que será como mínimo de 16 años.

7.- La sentencia de la Sala Segunda del Tribunal Supremo número 782/2007, de fecha 3.10.2007 explica esta cuestión y aboga por examinar las imágenes no de forma aislada unas o de otras o desvinculadas de una conducta relevante. El Tribunal tiene en cuenta que se enfocaban principalmente los genitales de los menores, lo cual, unido a la posesión del resto del material ocupado en poder del condenado y a los demás datos que demostraban la gestión de páginas pornográficas conteniendo imágenes de menores, permitió inferir razonablemente el carácter pornográfico del material.

Ocasionalmente se producen casos en que surge la duda. Recientemente se señaló un juicio por tenencia y distribución de pornografía infantil. Se acusaba a una persona que había compartido un archivo de pornografía infantil. En su equipo solo se halló una imagen que representaba a un adulto y una mujer que aparentaba ser menor manteniendo sexo oral. La supuesta menor era, en realidad, una actriz de cine pornográfico conocida por hacerse pasar por menor pero que, en realidad, tenía más de 20 años. La literalidad del Código Penal parece excluir el delito en este caso por cuanto no se ha utilizado la imagen de ningún menor.

El fin de la norma arroja luz sobre cuándo hay delito y cuando no. La determinación del bien jurídico protegido es clara en el caso de la elaboración de pornografía infantil, ya que se trata de un menor concreto utilizado por el delincuente para producir el material pornográfico. La cuestión no es tan sencilla cuando se trata de enjuiciar las conductas de quienes, sin haber participado en la elaboración del material ilícito, lo distribuyen o, simplemente, lo poseen para su consumo. Tradicionalmente se venía manteniendo que el bien jurídico protegido era, en principio, la protección de la indemnidad y libertad sexual de los menores. Se ha planteado que si la descarga o posesión de estos archivos afecta a la indemnidad sexual de los menores, por qué motivo no se castiga también la visualización de los mismos archivos sin descarga de los mismos⁸. La única respuesta que puede darse es que a día de hoy esta visualización no es delito.

265

En las redes sociales circulan imágenes que pueden considerarse pornografía infantil. Cuando la imagen ha sido obtenida subrepticamente o directamente sustraída al menor, el delito se habrá perpetrado. Cuestión distinta es cuando el menor ha consentido la realización del archivo. La jurisprudencia se ha planteado, ante esta situación, considerar el bien jurídico protegido no tanto la indemnidad sexual del menor, que más arriba se apuntaba, como su dignidad como menor e, incluso, su derecho a la propia imagen⁹.

8.- Streaming

9.- La sentencia de la Sala Segunda del Tribunal Supremo número 262/2012 de fecha 3.4.2012 recoge en su Fundamento Jurídico primero que “las conductas descritas en el artículo 189 tienen en común que el sujeto pasivo es un menor de 18 años (o incapaz) y que su consentimiento no es válido al existir una presunción legal en el sentido de que no concurren condiciones de libertad para el ejercicio de la sexualidad por parte de estos, cuando dicho ejercicio implica su utilización por terceras personas con fines pornográficos o exhibicionistas, lo que implica que un sector doctrinal considera, en cuanto a cual sea el bien jurídico protegido, que no es tanto la indemnidad sexual de la personalidad del menor, como su dignidad como menor o su derecho a la propia imagen, lo que justifica esa irrelevancia del consentimiento de los menores de 18 años que deciden intervenir en la elaboración del material pornográfico, incluso sin mediar abuso de superioridad o engaño, cuando ese consentimiento, por el contrario, sí sería válido para la práctica de relaciones sexuales cuando no mediasen tales circunstancias.”

Esta consideración justifica la irrelevancia del consentimiento de los menores de 18 años que deciden intervenir en la elaboración del material pornográfico, incluso sin mediar abuso de superioridad o engaño. La solución jurisprudencial parece adecuada, pero resulta chocante que un menor de más de 13 años pueda consentir la práctica de actos sexuales¹⁰⁻¹¹. En la práctica suele hallarse la solución más acorde con los derechos y bienes jurídicos en conflicto.

La proporcionalidad debe regir la investigación criminal. Debe evitarse cualquier tipo de sobreactuación, lo que es compatible con la tolerancia cero que debe presidir la lucha contra este tipo de delincuencia. Como ejemplo: es el caso de una investigación sobre direcciones IP desde las que se comparten archivos pedófilos. Se ha resuelto la IP y se ha ido al domicilio correspondiente, normalmente a primera hora de la mañana, ha abierto la esposa y le ha dicho a la comisión judicial que debía ser un error, que ellos no eran delincuentes. Lo que ha sucedido es que el hijo se había descargado un archivo pedófilo por error. El hecho es, por supuesto, real. Las consecuencias personales, familiares y sociales son obvias. Pero las consecuencias no terminan aquí. Además del estigma social para el encartado en su familia y en su vecindario, existe otro efecto colateral, el judicial. Los jueces deben comprobar, para condenar a una persona: uno que ha cometido un hecho tipificado y dos que existe dolo, esto es, ánimo de delinquir. En casos como el relatado han absuelto al no quedar probada la intención de bajarse pornografía infantil. Algo no se ha hecho bien cuando ha llegado hasta la fase de enjuiciamiento un hecho más que dudoso.

Además, en estos casos, se ha llevado la investigación como distribución de pornografía infantil por un solo archivo. La solución a esta posibilidad de error es poner en marcha la maquinaria policial y judicial únicamente cuando haya varios indicios, lo que se traduce en varios archivos descargados. Estas últimas consideraciones se hacen en cuanto a los que se bajan y comparten archivos ilícitos mediante programas para compartir archivos. No es aplicable al que cuelga en una red social una sola imagen o video pedófilo. En este último caso el dolo es claro.

10.- España es uno de los países con edad más baja en cuanto al consentimiento sexual (13 años, artículo 183 CP).

11.- En otros países europeos ambas edades (edad de consentimiento sexual y edad para participar en actividades de pornografía infantil) coinciden: Francia, 15 años; Alemania, 14 años; y Reino Unido, 16 años.

El artículo 189 del Código Penal¹² castiga distintas conductas dentro del genérico título de “Delitos relativos a la prostitución y corrupción de menores”. Este tipo de conductas han experimentado un considerable aumento con el uso de las nuevas tecnologías de la información y el conocimiento. Este artículo contiene un tipo básico que estaría constituido por el párrafo primero, una conducta atenuada recogida en el párrafo segundo¹³, y unos subtipos agravados establecidos en el párrafo tercero. Además, el citado artículo contiene otros tipos penales y establece una serie de medidas que podrán ser impuestas a los responsables de estos delitos y a las organizaciones dedicadas a su comisión.

Hay que recalcar la importante pena con la que se castigan los supuestos agravados del párrafo tercero del artículo 189 del Código Penal. Baste decir que ha habido una elaboración jurisprudencial que ha perfilado con mucha precisión cuándo serán aplicables cada uno de los subtipos agravados. Así se distingue entre seis supuestos de agravación: dos referidos al material pornográfico, dos a las condiciones del sujeto activo y los otros a los actos de elaboración del material o utilización de los menores o incapaces¹⁴.

12.- Los dos primero párrafos del precepto citado son:

“Artículo 189.1. Será castigado con la pena de prisión de uno a cinco años:

- a) El que capture o utilizare a menores de edad o a incapaces con fines o en espectáculos exhibicionistas o pornográficos, tanto públicos como privados, o para elaborar cualquier clase de material pornográfico, cualquiera que sea su soporte, o financiare cualquiera de estas actividades o se lucrare con ellas.
 - b) El que produjere, vendiere, distribuyere, exhibiere, ofreciere o facilitare la producción, venta, difusión o exhibición por cualquier medio de material porno- gráfico en cuya elaboración hayan sido utilizados menores de edad o incapaces, o lo poseyere para estos fines, aunque el material tuviere su origen en el extranjero o fuere desconocido.
2. El que para su propio uso posea material pornográfico en cuya elaboración se hubieran utilizado menores de edad o incapaces, será castigado con la pena de tres meses a un año de prisión o con multa de seis meses a dos años.”

13.- En el caso de la mera tenencia de pornografía infantil del artículo 189.2 no son de aplicación las agravaciones contenidas en el párrafo tercero del mismo artículo.

14.- “3. Serán castigados con la pena de prisión de cinco a nueve años los que realicen los actos previstos en el apartado 1 de este artículo cuando concurra alguna de las circunstancias siguientes:

- a) Cuando se utilicen a niños menores de 13 años.
- b) Cuando los hechos revistan un carácter particularmente degradante o vejatorio.
- c) Cuando los hechos revistan especial gravedad atendiendo al valor económico del material pornográfico.
- d) Cuando el material pornográfico represente a niños o a incapaces que son víctimas de violencia física o sexual.
- e) Cuando el culpable pertenezca a una organización o asociación, incluso de carácter transitorio, que se dedicare a la realización de tales actividades.

De los tres más frecuentes, conviene dar unas notas rápidas que permitan conocer la última jurisprudencia:

- a) “Se utilicen menores de 13 años” (art. 189.3.a). Solo será aplicable la agravación cuando se utilicen a menores y no cuando sólo se distribuye o difunde el material elaborado por terceros¹⁵.
- b) “Los hechos revistan un carácter particularmente degradante o vejatorio” (art. 189.3.b). Se trata de un subtipo poco aplicado. Existen casos de child grooming en los que el delincuente busca no sólo que la víctima acceda a realizar el material pornográfico infantil, sino que persigue la humillación de la misma con prácticas degradantes para su dignidad¹⁶.
- c) “Cuando el material pornográfico represente a niños o a incapaces que son víctimas de violencia física o sexual” (artículo 189.3.d). No es necesario haber participado en la elaboración del material, basta con realizar cualquiera de las conductas del número 1 del artículo 189. Además de los casos en que existe violencia física (niños atados, golpeados, etc.) o sexual (violaciones, múltiples penetraciones, etc.), existe una reciente sentencia que aplica esta agravación cuando exista desproporción entre los órganos sexuales de adulto y niño¹⁷.

f) Cuando el responsable sea ascendiente, tutor, curador, guardador, maestro o cualquier otra persona encargada, de hecho o de derecho, del menor o incapaz.”

15.- Así la sentencia de la Sala Segunda del Tribunal Supremo número 795/2009, de fecha 28.5.2009 concreta que este subtipo agravado sólo puede integrarse con “las acciones previstas en la letra a) del apartado 1º, pero no necesariamente con todas las descritas en la letra b), pues la difusión o posterior utilización de imágenes producidas por otro no significa usar o utilizar a los menores, sino difundir los soportes ya elaborados en los que sí se han utilizado menores de 13 años en persona, de forma que sería necesario establecer, en cada caso, en relación con la letra b) del apartado 1º, si ha concurrido o no esta utilización.”

16.- La sentencia de la Sala Segunda del Tribunal Supremo número 803/2010 de fecha 30.9.2010 aplicó este subtipo agravado que “nada tiene que ver con la vejación inherente al acceso carnal, el cual en sí mismo, tratándose de menores, podría considerarse como degradante o vejatorio, sino a la especial naturaleza de los hechos que acentúa esa connotación peyorativa y que han de ser ejecutados con la finalidad de ocasionar una especial sensación de humillación a la víctima.” Se trata de imágenes que, además del componente sexual, describen una situación escatológica que produce sentimientos de asco, repugnancia y es especialmente envilecedor para el menor por la sensación de humillación que produce.

17.- La sentencia de la Sala Segunda del Tribunal Supremo número 184/2012, de fecha 9.3.2012 justifica la agravación cuando “la desproporción es tan evidente como en el caso de autos, tratándose de una niña de cuatro años penetrada vaginal y analmente en repetidas ocasiones por un pene adulto en erección...”

Estos subtipos agravados están castigados con penas de prisión muy graves. Sin embargo, en algunas ocasiones ha ocurrido que no se han aplicado estos subtipos agravados por una concatenación de causas que a continuación se exponen. La investigación policial suele concluir con la recolección de las evidencias digitales, bien por la ocupación de un soporte de memoria o equipo informático, bien por la traza electrónica que ha dejado determinada comunicación en la Red. En cualquier caso, es necesario hacer un informe pericial de esas evidencias. En ocasiones, la cantidad de material intervenido es importante por lo que su estudio puede ser laborioso. El informe pericial suele hacerlo un funcionario policial que, si no visiona la totalidad del material incautado o no usa un criterio jurídico adecuado para exponer los hallazgos realizados, puede obviarse el material más grave en el informe. En otras palabras, el funcionario policial no resalta en su informe que hay material que pudiera dar lugar a la aplicación de un subtipo agravado. El Fiscal estudia ese informe pericial pero no visiona directamente el material intervenido y formula su acusación por el tipo básico. El Juez tiene en cuenta el escrito de acusación fiscal y tampoco ve el material ocupado, estando, además, constreñido por el principio acusatorio. El resultado es una sentencia que no refleja la gravedad de la conducta realizada por el delincuente sino una inferior.

Por lo que se refiere a la pederastia, cuando el delincuente sexual ejecuta actos físicos contra la libertad sexual de los menores, se produce un concurso de delitos entre los acaecidos en el mundo virtual y los producidos en la realidad física.

269

LAS CONDUCTAS DE ACOSO CON FINALIDAD SEXUAL

Las conductas de acoso deben recibir en una sociedad avanzada una especial consideración por parte de los poderes públicos. La práctica diaria en los Juzgados y Tribunales nos da una visión de la importancia del fenómeno que, si bien no es nuevo, se ha desarrollado de forma considerable con las nuevas tecnologías. Estas tecnologías permiten que prácticamente cualquiera pueda convertirse en acosador o en acosado. Los notorios casos de acoso a autoridades, personas conocidas de los medios de comunicación, del espectáculo o el deporte, no hacen sino remachar que no hay nadie a salvo de sufrir este tipo de persecución. Además, las consecuencias pueden llegar a ser graves. Esto se demuestra por las denuncias interpuestas por parte de estas personas conocidas o con importantes responsabilidades públicas o privadas. Cuando el objetivo del acoso se dirige a menores o incapaces y la finalidad del mismo es de tipo sexual, el daño potencial a bienes jurídicos crece de forma considerable¹⁸. Los menores carecen de la experiencia vital que exige enfrentarse a este tipo de

18.- La Constitución española en su artículo 20.4 establece como límite a los derechos y libertades en este precepto reconocidos, la protección de la juventud y la infancia.

fenómenos, y pueden ser una presa fácil para los acosadores. Estos suelen aprovecharse del uso y conocimiento de herramientas informáticas que les permiten tener, ya de inicio, una ventaja sobre las víctimas.

El acoso a menores con finalidad sexual o *child grooming* es, desde mi punto de vista, uno de los delitos que se ha visto favorecido por el masivo uso de las redes sociales. Por red social entendemos un círculo de conocidos. Pues bien, determinados programas implementados en la Red facilitan que estos conocidos puedan mantener una casi continua intercomunicación. En este sentido se emplea aquí red social. El conocido *Messenger*, además de un programa de mensajería instantánea, también puede ser considerado, en ese sentido amplio, como una red social. En realidad, si estudiamos las sentencias judiciales sobre *child grooming* se puede comprobar que en los hechos que relatan la mayoría de ellas el medio empleado por el acosador fue precisamente este programa creado por Microsoft¹⁹, por mucho que normalmente el canal por el que entraron en contacto acosador y víctima suele ser una red social de las muchas que utilizan los jóvenes y adolescentes.

270 El *child grooming* ha sido tipificado “ex novo” por la Ley Orgánica 5/2010²⁰. Se trata de un paso relevante en la progresiva incorporación de los llamados delitos informáticos en el Código Penal. Merece una mención destacada que en la Exposición de Motivos de la citada ley orgánica se alude por primera vez en la ley penal española al *child grooming*²¹. El hecho de que el legislador introduzca este nuevo tipo penal significa que adelanta el reproche penal a actos que, anteriormente a esta Ley, no eran delito. Por lo que se refiere a todos los demás delitos que se cometen con ocasión del acoso, el estado de cosas no ha variado. Se trata de un paso importante, por cuanto tipifica los actos iniciales del acoso, anteriormente impunes, pero insuficiente porque se

19.- MSN Messenger fue creado en el año 1999 y experimentó una considerable implantación en nuestro país entre adolescentes y jóvenes.

20.- “Artículo 183 bis. El que a través de Internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de trece años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los arts. 178 a 183 y 189, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento, será castigado con la pena de uno a tres años de prisión o multa de doce a veinticuatro meses, sin perjuicio de las penas correspondientes a los delitos en su caso cometidos. Las penas se impondrán en su mitad superior cuando el acercamiento se obtenga mediante coacción, intimidación o engaño.”

21.- “La extensión de la utilización de Internet y de las tecnologías de la información y la comunicación con fines sexuales contra menores, ha evidenciado la necesidad de castigar penalmente las conductas que una persona adulta desarrolla a través de tales medios para ganarse la confianza de menores con el fin de concertar encuentros para obtener concesiones de índole sexual. Por ello se introduce un nuevo artículo 183 bis mediante el que se regula el internacionalmente llamado “*child grooming*”, previéndose, además, penas agravadas cuando el acercamiento al menor se obtenga mediante coacción, intimidación o engaño.”

refiere sólo a menores de 13 años, que son una pequeña parte de las víctimas de estos delitos de acoso a menores.

Las fases del delito de *child grooming* responden en la mayoría de las ocasiones a un patrón que se ha revelado eficaz para los pederastas y pedófilos. Estas son las etapas del acoso:

- 1) **Planificación.** Dos son los puntos relevantes de esta etapa: la averiguación de los lugares en que se va a entrar en contacto con las potenciales víctimas (algunas redes sociales son propicias para entrar en contacto con menores de edad) y las herramientas de todo tipo que se van a utilizar para iniciar la aproximación. Las herramientas pueden ser de tipo informático. Es el caso de troyanos o virus para conocer las claves de las cuentas de correo o de redes sociales. También se suelen utilizar archivos multimedia para hacer creer a la víctima que está comunicándose con otro menor²².
- 2) **Contacto con el menor.** Se trata del momento clave. El adulto, haciéndose pasar por quien no es, normalmente otro menor, trata de establecer lazos de amistad con el menor. En ocasiones estos contactos pueden prolongarse durante días e incluso meses. De esta forma se individualizan las posibles víctimas, normalmente las más vulnerables. En ocasiones, esta supuesta amistad y contacto virtual prolongado son suficientes para conseguir los objetivos del delincuente, esto es, la remisión de imágenes de contenido sexual o el encuentro sexual.
- 3) **Acoso al menor hasta doblegar su voluntad.** Cuando el fin perseguido no se obtiene de forma amigable, el acosador despliega todas sus habilidades. Se produce normalmente una lucha desigual agravada porque el acosador intenta aislar a su víctima para que no solicite ayuda en su entorno familiar o entre sus amistades. Entre las amenazas más comunes se encuentra la intimidación a la víctima con que se va a publicar en determinados sitios de Internet o bien imágenes o bien datos ya cedidos voluntariamente por la víctima, o bien éstos u otros bajados de sitios públicos en los que los había subido la propia víctima pero después de haberlos modificado, de tal forma que su posible publicación produzca temor en la víctima y le lleve a acceder a los requerimientos del acosador. Existe otro método más sofisticado en el caso de que el acosador utilice herramientas informáticas para controlar las cuentas que utiliza la víctima (de correo, en las redes sociales, etc.). En los casos más extremos el acosador puede hacerse con el control

22.- Por ejemplo, un video en el que aparece una joven desnudándose al tiempo que se invita al interlocutor, un chico adolescente, a que haga lo mismo a través de la webcam.

del equipo informático y de las cuentas de la víctima, incluso aunque aquélla formatee el disco duro o trate de cambiar las credenciales. Llegado a este punto el acosador puede llevar a cabo una labor de aniquilación de la voluntad de la víctima con resultados muy graves.

Con ocasión del *child grooming* se suelen perpetrar otros delitos. Se han expuesto los relativos a la pornografía infantil que, en muchas ocasiones, son el fin primordial del delincuente. Frecuentemente, para lograr ese propósito, el acosador realiza otras acciones que debiliten la originaria voluntad de la víctima de no acceder a las peticiones realizadas por aquél. Estas acciones pueden constituir delitos autónomos. Se ha mencionado el supuesto de sustracción de cuentas de correo o de redes sociales. La cuestión ha sido tratada en varias ocasiones por la jurisprudencia y la doctrina de las Audiencias Provinciales²³. También ha habido pronunciamientos judiciales sobre la utilización de virus y troyanos²⁴, herramientas usadas por el acosador para controlar el equipo informático de la víctima y realizar su labor de debilitamiento de su voluntad²⁵.

23.- Tres sentencias de Audiencias Provinciales.

La sentencia de la Audiencia Provincial de Barcelona número 72/2008, de fecha 18.1.2008 sostiene que la entrada inconstituida en la aplicación de correo electrónico de otra persona y el recorrido por las diferentes bases de datos que el sistema contiene, incluso sin abrir ningún mensaje, puede ser penalmente típica, ya que con ella se está produciendo una intromisión en la intimidad.

La sentencia de la Audiencia Provincial de Zaragoza número 317/2009, de fecha 7.4.2009 que mantiene que el delito contra la intimidad se consuma tan pronto el sujeto activo accede a los datos, esto es, tan pronto los conoce y los tiene a su disposición.

Y la sentencia de la Audiencia Provincial de Asturias número 152/2005, de fecha 29.6.2005 que afirma que constituye este delito la entrada en el correo electrónico de la perjudicada, obteniendo datos personales de la misma y su entorno.

24.- La diferencia fundamental entre un troyano y un virus, consiste en su finalidad. Para que un programa sea un “troyano” sólo tiene que acceder y controlar la máquina anfitriona sin ser advertido, normalmente bajo una apariencia inocua. Al contrario que un virus, que es un huésped destructivo, el troyano no necesariamente provoca daños porque no es su objetivo.

25.- La sentencia de la Audiencia Provincial de Madrid número 329/2009, de fecha 26.11.2009 considera que la creación y utilización de un “troyano” mediante el cual, una vez descargado por los usuarios, sin saberlo al estar oculto en otros archivos, lograba acceder a datos de tipo personal sin conocimiento ni autorización de éstos constituye el delito de descubrimiento y revelación de secretos.

En estos supuestos se comete un delito de revelación de secretos tipificado en el artículo 197 del Código Penal²⁶. Téngase en cuenta que, en estos casos, será de aplicación el subtipo agravado del párrafo sexto del citado artículo que agrava la pena cuando se vean afectados datos de carácter personal que revelen, entre otros, la vida sexual de la víctima o ésta sea menor de edad o incapaz. El delito de revelación de secretos tiene una naturaleza semipública, es decir, requiere denuncia de la persona agraviada o de su representante legal. En estos casos, al ser la víctima menor de edad, puede denunciar el Ministerio Fiscal. Si es mayor de edad será preciso que se muestre parte y denuncie.

El mismo significado de acosar²⁷ nos indica que es la libertad uno de los bienes atacados en el *child grooming*. Por ello, es frecuente que se cometan delitos como amenazas y coacciones. En este punto, hay que resaltar que la amenaza suele ser condicional, esto es, se pide a la víctima que realice una acción (encender la webcam, desnudarse, realizar determinados actos, etc.) y se le dice que en caso contrario se llevara a cabo una acción que la víctima quiere evitar (por ejemplo, difundir una fotografía comprometida o una conversación o datos personales entre sus contactos o seguidores de una red social o en un sitio de Internet de acceso público). Estas amenazas tendrán, en principio, la consideración de delito y no de falta²⁸. Es importante destacar que si la condición se llega a cumplir, la pena a imponer será la del delito de amenazas condicionales, agravada cuando la condición se cumple y reagravada por haberse amenazado por escrito, por teléfono o por cualquier medio de comunicación o de reproducción²⁹. Se resalta esta concreta pe-

273

26.- Los dos primeros números de dicho artículo están redactados como sigue:

“197. 1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Igualmente se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.”

27.- La RAE define acosar como “perseguir, apremiar, importunar a alguien con molestias o requerimientos.”

28.- La sentencia de la Audiencia Provincial de Segovia número 27/2010, de fecha 8.9.2010 califica de delito de amenazas condicionales el supuesto de amenaza con colgar en Internet fotos de una persona desnuda obtenidas voluntariamente durante una relación sentimental.

29.- La pena a imponer en estos supuestos será la de prisión de 3 años y un día a 5 años.

nalidad porque, frecuentemente, será la pena más grave que se imponga en los delitos de *child grooming*. Esto tiene importancia porque, en los casos de haberse cometido varios delitos, la pena a imponer por el delito de amenazas puede ser la más grave y determina el máximo de cumplimiento efectivo³⁰.

Por último, mencionaré el tipo delictivo contra la integridad moral tipificado en el artículo 173.1 del Código Penal³¹, que refleja muy bien lo que suele ocurrir con ocasión del *child grooming*. Se trata de un delito compatible con los otros delitos mencionados más arriba. Algunas sentencias están aplicando este delito para las situaciones creadas por la publicación de datos personales en Internet y las redes sociales³². En los significados de “integridad” del diccionario de la Real Academia Española, el segundo alude a la “pureza de las vírgenes”. Las víctimas de este delito pierden anticipadamente esa especie de inocencia o confianza en que el adulto no va a ser cruel con un menor, que va a respetar esa norma de la ley no escrita de la vida por la cual los niños y los adolescentes deben ser protegidos y respetados por los adultos. Este sentimiento, de haber sido utilizado de forma sucia por el acosador es la manifestación que muchas víctimas de *child grooming* suelen hacer en los Tribunales en los pocos casos en que estos delitos llegan a juicio. Algo que no se permitiría a la puerta de un centro educativo se realiza en Internet sin que se pueda evitar. Las víctimas que denuncian estos delitos no inician un camino fácil. Se las mira con recelo.

Es como si hubieran recibido el acoso por haber entrado en las redes sociales. Se recalca, una y otra vez, que si no hubiera visitado esos sitios de Internet no habría tenido problemas. Se les exige una madurez que no tienen que tener a su edad.

30.- Por aplicación del artículo 76 del Código Penal. Si se repasan las penas por los delitos mencionados en este trabajo (revelación de secretos, elaboración o distribución de pornografía infantil básica, coacciones, contra la integridad moral e injurias) resulta que la pena de estas amenazas condicionales hechas por escrito, teléfono u otro medio de comunicación, puede ser el delito más castigado. Esto es así, al menos, para hechos anteriores a la entrada en vigor de la reforma operada por L.O. 5/2010, que ha aumentado la penalidad de la elaboración o distribución de la pornografía infantil básica hasta los cinco años de prisión.

31.- “173. 1. El que infligiera a otra persona un trato degradante, menoscabando gravemente su integridad moral, será castigado con la pena de prisión de seis meses a dos años.”

32.- La sentencia de la Audiencia Provincial de Valencia número 304/2011, de fecha 18.10.2011 condena por delito contra la integridad moral a quien utilizó, sin consentimiento alguno, datos personales, no sólo los que aparecen en cualquier consulta por Internet: teléfono, dirección, nombre, apellidos, sino también relativos a su vida personal, su condición de soltera, de vivir sola, de trabajo y horarios, haciéndolo en una página de eminente contenido sexual. Esta sentencia mantiene que “la integridad moral se configura como una categoría conceptual propia, como un valor de la vida humana independiente del derecho a la vida, a la integridad física, a la libertad en sus diversas manifestaciones y al honor.”

Las consecuencias del *child grooming* no son ninguna minucia: miedo a salir a la calle, retraimiento, dejar de acudir a clase, trastornos de la personalidad, intentos de suicidio, etc. Las víctimas sólo usaron las nuevas tecnologías para relacionarse y conocer nuevos amigos. Usaron Internet como muchos otros lo emplean para utilizar diversos servicios, como la banca electrónica, y no por ello son merecedores de sufrir un delito, como el *phishing* bancario. En los delitos informáticos se explotan, normalmente, las vulnerabilidades de sistemas y redes. En este delito se explota la vulnerabilidad de quien ya se cree con capacidad de hacer frente al acoso pero que, en realidad, no deja de ser un niño o adolescente. En la lucha contra el acoso a menores en Internet se va por el buen camino, pero todavía lejos de darle la importancia que estas conductas ya reciben en otros países que las persiguen desde hace tiempo. En España, tímidamente, se ha introducido en el año 2010. La buena noticia es que, poco a poco, los responsables de la persecución del delito están llegando a ese mundo de las redes sociales en que venía imperando la ley del más fuerte, es decir, la impunidad.

REDES SOCIALES Y DELITOS SEXUALES

MANUEL ALCAIDE ALCAIDE

**Inspector Jefe del Cuerpo Nacional de Policía.
Jefe de la Sección de Delitos Sexuales y Servicio de Atención
a la Mujer (SAM) de Madrid**

Hay que quitarse de la mente la idea esta de que los delitos tecnológicos son, exclusivamente, los que se dirigen contra los equipos informáticos. Hay un Convenio sobre Ciberdelincuencia, firmado en Budapest, que define en su preámbulo como ciberdelitos varias cuestiones, entre ellas el abuso de los sistemas, redes y datos para cometer infracciones. Según esta definición, prácticamente dentro de poco todos los delitos se podrían casi clasificar como delitos informáticos porque, hoy en día, pocos quebrantamientos se cometen sin utilizar las telecomunicaciones, al menos, un correo electrónico. En este caso concreto se podrá comprobar que en los delitos contra la libertad sexual de adultos también se usa este tipo de herramientas por parte del delincuente. Es decir, en las agresiones contra la libertad sexual que afectan a adultos y en las cuales Internet se utiliza como instrumento, se abusa de esas nuevas tecnologías para cometer los delitos.

277

La mayoría de las personas piensan que los agresores sexuales tienen que tener un aspecto desagradable, ser feos, impotentes, etc., y que comente sus actos en zonas oscuras y poco transitadas, que lo hacen en serie, que solo tienen antecedentes por delitos contra la libertad sexual, que son enfermos mentales, que no tienen relaciones sexuales estables y lógicas y que, por ello, se convierten en este tipo de delincuentes sexuales. A todos esos mitos que ya existían, y que también afectan a la delincuencia a través de Internet cometida sobre adultos, se une uno nuevo, que es un traslado mental que se ha hecho de los peligros que hay para los menores a los adultos. Esta amenazada de los menores es objetiva, pero los medios de comunicación, ya sean Internet como tradicionales, tratan de establecer que la Red es un peligro continuo.

En cuanto a datos, según la Brigada Provincial de Policía Judicial de Madrid, en el años 2011 hubo 654 casos, 654 víctimas, 346 detenidos y 69 imputados. Lo que en estos casos se observa es que la vía pública no es el lugar preponderante para realizar sus fechorías; que las edades en los delitos sexuales están muy distribuidas, aunque la mayoría están de 25 años hacia abajo; que la hora del hecho no siempre es de noche, entre las 00:00 y las 06:00 se producen un 28 por ciento de las agresiones sexuales; que en la relación con la víctima solamente es desconocido en un 45 por ciento de los casos; y que en 2010 hubo cuatro casos en los que había una relación telemática previa. En ese año seis casos, que de 654 víctimas es, aproximadamente, un 1 por ciento.

278

Sobre el agresor, estos no suelen ser enfermos ni su aspecto físico es extraño, en la mayoría de los casos es de lo más normal. En el 46 por ciento de las situaciones, el delincuente sexual no era desconocido para la víctima, es un familiar, un profesor, etc., una persona que la conoce. El 14 por ciento de la violencia sexual se comete dentro del ámbito familiar. En la violencia sexual no existe un lugar seguro, se produce en cualquier espacio, en el domicilio, en un descampado, en la vía pública. El agresor sexual no tiene un perfil de víctima definido, a menudo basta con que encuentre a una persona y la “pille” en ese momento. Y en algunas ocasiones, los agresores sexuales de niños, que muchos piensan que son muy exclusivos, también atacan a adultos. Esto es una experiencia de datos objetivos sobre 654 casos.

Existen numerosos agresores sexuales ocasionales, oportunistas, no todos son en serie. Son gente que no iba a cometer esa agresión pero, cuando se les da la oportunidad, por ejemplo situaciones en las que ese agresor ha consumido alcohol, pues la realizan. Y muchos tienen antecedentes por otros delitos, sobre todo violentos: robos con violencia o con intimidación.

Muchos de los violadores en serie llevan una vida de lo más normal, como por ejemplo el del trabajador que tenía su mujer y cuando le sucedía con ella un problema y no estaba muy a gusto pues se dedicaba a violar por todo Madrid.

De siete millones de usuario, que es el 20 por ciento de la población adulta de España que está registrada en las páginas web para citas, hay tres millones que están en redes eróticas. En Madrid se han producido un 1 por ciento de delitos sexuales, respecto a los totales. Es una relación muy escasa. En este caso no hay que demonizar Internet. Hay un gran número de sites de encuentros: Sé travieso, Casual Club, Badoo, etc. Cuando la Policía ha accedido con perfiles ficticios a esta última, prácticamente “le tiran los tejos” en el primer momento y, normalmente, esos adultos no mantienen relacio-

nes sexuales hasta la segunda cita y el 3 por ciento acaba en éxito. Como ya se ha indicado, de los siete millones de usuarios sólo se han encontrado un 1 por ciento de delitos sexuales. Es un hecho.

Aun así, hay un 1 por ciento que debe ser digno de estudio. Entre los ejemplos, obtenidos de noticias aparecidas en Internet, está el artículo “Detenido el presunto violador de Moncloa”, que en una referencia pequeña señalaba que contactaba con sus víctimas a través de los foros de Internet. Cuando se le va a juzgar, en el titular se especifica que la Audiencia Nacional juzga a un violador en serie de prostitutas a las que contrataba en Internet, es decir, se está ya demonizando desde los titulares, porque la opinión pública lo que recibe es: Internet, Internet, Internet. Efectivamente, esa persona contactaba con prostitutas pero, ¿y si estos anuncios los hubiera obtenido en la prensa escrita tradicional? Hasta hace poco, los agresores con esas conductas acudían al *ABC* y en sus páginas de citas obtenía la información, quedaban con esa mujer y cometían los delitos. La diferencia está en que no aparecía en los medios escritos ese lugar de obtención de la información, porque si hubiera sido así estos se habrían echado tierra encima. ¿Cómo van a titular: “La Audiencia juzga a un violador en serie de prostitutas a las que contrataba a través de las páginas de contactos del *ABC*”? Internet se demoniza.

279

Hay otros casos en los que, efectivamente, se ha utilizado Internet y, además, ésta ha sido una herramienta básica. En este caso es una persona que se detuvo en Cuenca. Los violadores en general no tienen porque ser personas con unas características físicas especiales, pero en este caso se va a indicar lo más destacado de su aspecto físico: era una persona con acondroplasia. Éste contactaba por Internet y se hacía pasar por un chico de 20 años, cuando conseguía el vínculo con esas mujeres mayores de edad les pedía el favor de que tuvieran relaciones sexuales con un familiar suyo que estaba a punto de suicidarse. Conseguía que las chicas tuvieran una cita con él mismo, que tenía más de cuarenta años y que era el supuesto tío de la persona que había contactado con ellas por la Red y lograba barbaridades con unas conductas bastante agresivas. En este caso se realizó un abuso de las nuevas tecnologías para llevar a cabo ese delito.

Hay que destacar que los periodistas, la sociedad, están demonizando Internet, y todo hay que contarlo en su justa medida. Hay una serie de peligros, hay una serie de cuestiones que hay que estudiar y que hay que evitar porque no se puede demonizar todo.

También hay casos de mujeres que ponen sus *books* en LinkedIn para trabajar como modelos. Hay personas que tienen la facilidad de hacerse pasar por supuestos empresarios del sector, hasta de cine porno, para lograr

que esas víctimas caigan en sus redes, forzarlas y mantener unas relaciones no consentidas. En 2011 hubo unos seis casos de ese tipo, y en 2012 se incrementó un poco, hasta alcanzar el 1,5 de los delitos sexuales de unos 600, que es lo que se espera alcanzar en 2012. Algo ínfimo comparado con los casos de pederastia.

Habría que imitar ciertas leyes de Estados Unidos que, en algunos Estados, obligan a cualquier condenado por delitos sexuales a comunicar a las redes sociales que está condenado, ya que tiene que aparecer en su perfil “Condenado por delito sexual”, y si es con menores debe mostrarse la referencia: “con menores”. ¿Habría que llegar a esto?

Para finalizar se explica otro caso investigado por la Policía Nacional. Se trata de un chico de 15 años que publica el siguiente anuncio: “Doy sexo a cambio de teléfono iPhone a hombre. Hombre de 19. Hago todo lo que me pidas: follo, chupo, hago mamadas, etc.” Se trataba de un caso de prostitución voluntaria de un menor, pero los que acudían se aprovechaban del chaval. Se investigó y se detuvo a varias personas. ¡Hasta dónde llega la dependencia de las redes sociales!, ¡hasta dónde llega la dependencia de las nuevas tecnologías!



POWERPOINT

MANUEL ALCAIDE ALCAIDE

**Inspector Jefe del Cuerpo Nacional de Policía.
Jefe de la Sección de Delitos Sexuales y Servicio de Atención
a la Mujer (SAM) de Madrid**



CUERPO NACIONAL DE POLICIA

DELITOS CONTRA LA LIBERTAD SEXUAL EN CITAS TELEMÁTICAS DE ADULTOS



25
aniversario

Cursos de Verano 2012
Universidad Complutense
San Lorenzo de El Escorial



Santander
UNIVERSIDADES


POLICIA 3.0

Manuel ALCAIDE


Inspector Jefe, Jefe de la Sección S.A.M. de la Brigada Provincial de Policía Judicial de Madrid



COMPETENCIAS S.A.M MADRID EN LIBERTAD SEXUAL



1. **TODO DELITO CONTRA LA LIBERTAD / INDEMNIDAD SEXUAL COMETIDO EN MADRID CAPITAL SIN IMPORTAR EDAD, NI CONDICIÓN DE VÍCTIMAS / AUTORES, EXCEPTO:**
 - DISTRIBUCIÓN PORNOGRAFÍA DE MENORES A TRAVÉS DE INTERNET ---> GRUPO VIII BPPJ (ÁMBITO MADRID), B.I.T. (ÁMBITO NACIONAL)
 - REDES DE PROSTITUCIÓN Y TRATA DE SERES HUMANOS PARA EXPLOTACIÓN SEXUAL ---> B.P.E.F.-U.C.R.I.F. (UNIDAD CONTRA LAS REDES DE INMIGRACIÓN Y FALSEDAD DOCUMENTAL) Y U.C.R.I.F. CENTRAL
2. **LABOR DE ANÁLISIS:** Tratamiento de toda denuncia por delitos contra Libertad Sexual de la región policial de Madrid, con fin ESTADÍSTICO, y para DESCUBRIR DELITOS CONEXOS por características del autor, similar modus operandi, zonas de actuación, etc.



¿ENTONCES, POR QUÉ ESTAMOS AQUÍ EN UN CURSO SOBRE CIBERDELINCUENCIA?

El Convenio sobre Ciberdelincuencia del Consejo de Europa" (Budapest el 23-NOV 2001), ampliado por protocolo adicional en el año 2.003 y ratificado por España en el año 2010, define en su Preámbulo como "ciberdelitos" los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como EL ABUSO DE DICHOS SISTEMAS, REDES Y DATOS.

Comprobaremos que además de para conductas que atentan contra diversos derechos de los menores, EXISTE UN ABUSO para aprovecharlos en DELITOS CONTRA LA LIBERTAD SEXUAL DE ADULTOS.



EL MITO DEL PELIGRO





MITOS HISTÓRICOS SOBRE AGRESORES SEXUALES



- LOS AGRESORES SEXUALES TIENEN ASPECTO DESAGRADABLE, SON FEOS E IMPOTENTES
- LAS AGRESIONES SEXUALES SE COMETEN POR INDIVIDUOS DESCONOCIDOS
- LOS VIOLADORES ATACAN SIEMPRE EN ZONAS OSCURAS Y POCO TRANSITADAS
- LOS VIOLADORES EN SERIE SIEMPRE ATACAN AL MISMO TIPO DE VÍCTIMAS
- TODO DELINCUENTE SEXUAL LO ES EN SERIE, TODOS SON REINCIDENTES
- LOS DELINCUENTES SEXUALES SOLO TIENEN ANTECEDENTES POR DELITOS CONTRA LA LIBERTAD SEXUAL
- LOS AGRESORES SEXUALES SON ENFERMOS MENTALES
- LOS AGRESORES SEXUALES, LO SON POR NO TENER RELACIONES SEXUALES NORMALES, NI PAREJA ESTABLE

5



EL NUEVO MITO

TRASLADO MENTAL, A LAS CITAS DE ADULTOS, DEL PELIGRO OBJETIVO DE EXISTENCIA DE UNA ALTA TASA DE DEPREDADORES SEXUALES DE MENORES EN INTERNET.

Peligros de las redes de citas y contactos

A pesar de las ventajas que puedan tener las redes de contactos para encontrar una pareja, se deben conocer sus riesgos

Por ANTONIO DELBANDO | Última actualización: 9 de junio de 2018 | 15:51

No hay comentarios

👍 👎 🗨️ 📄 📧 📧 📧 📧 📧 📧

Hoy en día, utilizar las redes sociales y las plataformas especializadas en contactos es una de las nuevas vías para encontrar pareja. Estas

La gran guía de sitios de encuentros

Existen sitios de encuentros para encontrar pareja, relaciones profesionales, contactos para volantes para la primera cita de la vida, pero también

Home | Contactos para volantes | Noticias | Prensa | Contacto | Webmaster

Peligros de las citas por Internet

A esta altura, seguramente ya te habrás convencido de las enormes ventajas de conocer gente online, amistades, citas, diversión, y quizás hasta el amor de tu vida. Pero, ¡cuidado! No todo es color de rosas. No es que esto haga de este modo de conocer gente una técnica menos recomendable en este juego, estar al tanto de los riesgos implicados, y saber cómo actuar para defenderse de ellos. De tener mucha suerte puedes salirte con la tuya, pero si no, puedes caer en desilusiones ni a peligros fácilmente evitables, conociendo las reglas y en manejo de ellas, y así, podrás sacarle el máximo provecho.

En primer lugar es importantísimo tener presente que la Internet es sólo un medio para acercarse a alguien, y no un fin en sí mismo. La idea no es tener un romance online, que se prolongue en el tiempo indefinidamente sin llegar a conocerse personalmente. Este es un gran riesgo que se corre si no se tienen claras las cosas desde un principio. Si la persona vive lejos, por ejemplo, puede darse un supuesto romance virtual basado en una IDEALIZACIÓN del otro. Y si la atracción es tan fuerte como para lograr vencer las barreras espaciales y finalmente encontrarse en persona, puede pasar que la química fallé, que las expectativas desmedidas generadas no se comiencen, al descubrir que quien venía del otro lado era una persona real, con sus defectos y meritos, en vez del príncipe azul, o princesa dorada que se había imaginado, creado a través de las fantasías y la proyección de los propios deseos. Esto puede resultar terriblemente frustrante y doloroso, más allá del tiempo y las ilusiones que se pueden desperdiciar con una dinámica así.

ICita a degas – pero seguro!

Los consejos de seguridad más importantes para antes y durante la primera cita

Como es sabido, la búsqueda de pareja en Internet tiene ventajas: concipie independientemente del tiempo y espacio se pueden conocer personas de todo el mundo – mucho más eficiente que en una discoteca.

A primera vista la idea de conocer gente online parece muy atractiva, pero ¿qué hay detrás?

De tener mucha suerte puedes salirte con la tuya, pero si no, puedes caer en desilusiones ni a peligros fácilmente evitables, conociendo las reglas y en manejo de ellas, y así, podrás sacarle el máximo provecho.

283



DESCENSO A LA REALIDAD





SIN PHOTOSHOP

CON PHOTOSHOP

CON SILICONAS

7

ANÁLISIS ESTADÍSTICO 2011 - VÍCTIMAS / AUTORES

LUGAR DEL HECHO		EADAES		HORA DEL HECHO	
DOMICILIO	40 %	18 - 25	26 %	00:00 - 06:00	28%
VIA PÚBLICA	34 %	25 - 35	26 %	18:00 - 24:00	20 %
ESTABLECIMIENTO PÚBLICO	12 %	- 18	38 %	06:00 - 12:00	19 %

2011 : 654 VÍCTIMAS - 346 DETENIDOS + 69 IMPUTADOS
 184 VIOLACIONES, 203 AGRESIONES, 229 ABUSOS Y 8 "OTROS"

EL 55 % DE LAS VÍCTIMAS SON MENORES DE 25 AÑOS.
 SE MANTIENE LA PROPORCIÓN DE AUTOR CONOCIDO Y DESCONOCIDO, CASI AL 50%.

RELACION CON VÍCTIMA		RELACIÓN TELEMÁTICA PREVIA	
DESCONOCIDO	46 %	2010	4 CASOS
CONOCIDO	30 %	2011	6 CASOS
FAMILIAR	14 %	2012 (6 MESES)	5CASOS
SENTIMENTAL	6 %		
LABORAL	4 %		

PORCENTAJE: 0,75% 2010 - 1 % 2011 - 1,5% 2012



CASUÍSTICA REAL S.A.M. - MADRID



- NO SON ENFERMOS Y SU ASPECTO EN LA MAYORÍA DE LOS CASOS, COMPLETAMENTE NORMAL.
- EN EL 46 % DE LOS CASOS, EL DELINCUENTE SEXUAL NO ERA DESCONOCIDO PARA VÍCTIMA Y EL 14% DE LA VIOLENCIA SEXUAL SE COMETE DENTRO DEL ÁMBITO FAMILIAR
- EN LA VIOLENCIA SEXUAL, NO EXISTE UN LUGAR SEGURO, SE PRODUCE EN CUALQUIER ESPACIO: DOMICILIO, DESCAMPADO, VÍA PÚBLICA.... Y SOLO EL 48 % DE LAS AGRESIONES SEXUALES SE COMETEN ENTRE LAS 18:00 Y LAS 06:00 HORAS
- EL AGRESOR SEXUAL NO TIENE PERFIL DE VÍCTIMA DEFINIDO, A MENUDO BASTA CON ENCONTRAR UNA, E INCLUSO ALGUNOS AGRESORES DE NIÑOS, TAMBIÉN ATACAN A ADULTOS
- EXISTEN NUMEROSOS AGRESORES SEXUALES OCASIONALES U OPORTUNISTAS
- MUCHOS TIENEN ANTECEDENTES POR OTROS DELITOS (SOBRE TODO R.V.I.)
- MUCHOS DE LOS VIOLADORES EN SERIE LLEVAN UNA VIDA NORMAL Y TIENEN PAREJA ESTABLE

[illegible]



¿Y SI LAS HUBIESE CONTRATADO A TRAVÉS DE ANUNCIOS DE PRENSA?

La Audiencia juzga a un violador en serie de prostitutas a las que contrataba en internet

Comunidad de Madrid • actualidad • Crimen

Detenido el presunto violador de Moncloa

La Policía ha detenido al presunto autor de una serie de violaciones, y tres agresiones sexuales, cometidas en el distrito de Moncloa.

El acusado contactaba con una víctima a través de la página de Internet de moncloa.com, donde se ofrecían servicios sexuales. Tras varias reuniones, el hombre se presentó en la vivienda de la víctima, donde la violó y la agredió sexualmente. La víctima denunció el hecho a la Policía, que lo detuvo tras una investigación de varias semanas.

La Audiencia Provincial de Madrid juzga el martes a un hombre con antecedentes penales por violación y que está acusado ahora de reincidir en sus agresiones en 2010 con dos prostitutas tras contactar con ellas por internet, y ante las que se hizo pasar por policía amenazándolas con una pistola. El procesado, Basilio Luis G.U., se enfrenta a 32 años y 4 meses de cárcel por los delitos de agresión sexual, violación, robo con violencia y una falta de lesiones, según el escrito provisional del fiscal.

23.03.2012

12

ESTO SI QUE NO SE PODRÍA HACER SIN INTERNET = ENGAÑO IMPOSIBLE

elcorreo.com

Edición: Bickala | Ir a Edición Araba/Alava | Personalizar

Portada Local Deportes Economía Más Actualidad Gente y TV Ocio Participa Blogs Servicios y Hemeroteca

Política Mundo Sociedad Cultura Videsolidaria Salud Tecnología e Internet Final de la violencia de ETA

Estás en: Bickala - El Correo.com > Noticias Más Actualidad > Noticias Sociedad > Detenido en Cuenca un violador que contactaba con sus víctimas a través de las redes sociales

Detenido en Cuenca un violador que contactaba con sus víctimas a través de las redes sociales

Entablaba cibervozos con jóvenes haciéndose pasar por un chico de 20 años y después les ofrecía realizar un 'book' de modelaje.

15.11.11 - 13:35 - EUROPA PRESS | CUENCA

Comentarios | Twitter | Facebook | Google+ | LinkedIn | StumbleUpon | Dribbble | SoundCloud | YouTube | RSS

Agentes de la Policía Nacional han detenido hoy en Tarancón (Cuenca) a un violador que contactaba con jóvenes y menores de edad a través de las redes sociales y que se hacía pasar por un chico de 20 años, cuando su edad era de 40, para entablar el primer contacto. Según ha informado la Jefatura Superior de Policía, tras ganarse la confianza, las persuadía para tomarles fotografías desnudas a través de la webcam a modo de prueba para un futuro 'book' de modelo.


De hecho, el delincuente, que según han indicado fuentes de la investigación utilizaba 'Badoo' como red habitual para sus contactos, llegó a simular ser el tío del supuesto joven de 20 años.

Cuenta AZUL 3,40%

Desde el 1 de diciembre de 2012. Para más información, visita el link.

[Diversidad]

[illegible]



POR ÚLTIMO: CASO REAL MENOR 15 AÑOS ¿DÓNDE VAMOS A LLEGAR?

milanuncios

PUBLICAR ANUNCIOS | PROFESIONALES MIS ANUNCIOS | |

VER ANUNCIOS.com > CONTACTOS > CONTACTOS HOMBRES

Ref: 44270009 Contactos hombres en madrid (MADRID) 3 días

DOY SEXO A CAMBIO DE DETELEFONO IPHONE A HOMBRE

HOMBRE DE 19. DOY sexo a cambio de un telefono iphone. pago lo que me pides follochupo hago mmamadas a cambio de un telefono movil andrid con internet soi ardiente en la cama . Edad 19 años

Contactar

- Enviar a amigos
- Enviar a mi selección
- Denunciar

Estadísticas

- 50 veces listado ?
- 0 vieron el teléfono
- 0 envios de email
- 0 envios a un amigo

SIN FOTO

EL BUSCAMIENTOS

Categoría: **Contactos** **Contactos hombres** en toda España

Que contengan las palabras

Edad: desde hasta ordenar por fecha fecha publicación

RECOMENDADO

1. Contactos mujeres sexo gratis en pineda	1. Contactos mujeres mujer sexo	1. Contactos madras sexo en las palmas
1. Contactos mujeres mujer sexo en madrid	1. Contactos mujeres sexo noche en madrid	1. Contactos sexo madrid
1. Contactos mujeres mujer paga sexo	1. Contactos mujer sexo gratis	1. Contactos mujeres mujer paga sexo en las palmas
1. Contactos mujeres mujer sexo gratis	1. Contactos mujeres mujer sexo gratis	

REDES SOCIALES Y DELITOS SEXUALES

BEATRIZ RAMOS IGLESIAS

**Inspectora del Cuerpo Nacional de Policía.
Jefa del Grupo II, de la Brigada de Investigación Tecnológica,
de Protección al Menor**

¿Qué es el turismo sexual infantil?

El turismo sexual infantil implica que turistas adultos, ya sea de procedencia nacional o extranjera, exploten sexualmente a menores de edad mediante una prestación económica o favor de alguna clase. Es un asalto horrendo y vergonzoso a la dignidad y los derechos de los niños, y es una forma de violencia y abuso infantil.

289

¿Por qué existe el turismo sexual infantil?

El entorno del turismo sexual en general (motivos del turista, intereses económicos, destinos turísticos orientados al sexo, estilos de publicidad, etc.), proporciona fuertes estímulos en las personas con inclinación a explotar sexualmente a los niños en sus viajes.

Las poblaciones de los países afectados, casi en su totalidad, atraviesan problemas económicos, los cuales son utilizados por el explotador para introducirlos a un circuito de explotación: la oferta y demanda de sexo. Aquí, la “mercancía más valiosa” es aquella que el turista sexual demanda y por la que está dispuesto a pagar altas sumas de dinero.

¿De dónde proviene el turista sexual infantil?

El flujo se produce, principalmente, desde el mundo económicamente desarrollado (Europa occidental, Norteamérica, los Países Escandinavos,

Asia, Australia, Países del Golfo) hacia los países pobres del Sudeste asiático, África y Latinoamérica. Además, individuos acomodados de naciones menos desarrolladas económicamente como México, Argentina y la India, también realizan turismo sexual. Asimismo, hay un reducido número de destinos en países desarrollados (Ámsterdam o Estados Unidos -Nueva Orleans y Las Vegas-). Muchos países receptores están bajo presiones económicas y políticas para que promuevan el turismo con el fin de generar divisas.

¿Quién es el turista sexual?

Es aquella persona, nacional o extranjera, que visita una ciudad, provincia o poblado, con el objetivo de contratar servicios sexuales con niños o niñas menores de edad.

¿Existe algún código ético sobre el turismo que desaprobe este tipo de delito?

Sí, el artículo 2 del Código Ético Mundial del Turismo (1999) de la Organización Mundial del Turismo señala: “La explotación de seres humanos, en cualquiera de sus formas, especialmente la sexual, y en particular cuando afecta a los niños, vulnera los objetivos fundamentales del turismo y constituye una negación de su esencia. Por lo tanto, conforme al derecho internacional, debe combatirse sin reservas con la cooperación de todos los Estados interesados, y sancionarse con rigor en las legislaciones nacionales de los países visitados y los de los autores de esos actos, incluso cuando se hayan cometido en el extranjero”.

¿Qué puede hacerse para combatir el turismo sexual infantil?

- Apoyar las campañas existentes en su contra que viene desarrollando el Ministerio de Comercio Exterior y Turismo (MINCETUR) español.
- Impulsar nuevas campañas en los lugares donde aún no se estén desarrollando acciones para frenar este delito, mediante una estrategia que incluya la participación activa de los sectores empresariales, formales e informales, ligados al turismo.
- Realizar charlas de prevención en las ciudades o zonas que cuenten con un índice alto de turismo nacional o extranjero.
- Mejorar los niveles socio-económicos de la población afectada, y promover un mayor acceso a la educación y la salud, principalmente de los niños, niñas y adolescentes.

- Sancionar drásticamente al explotador sexual de menores o “beneficiario” de esa explotación, al igual que al usuario o cliente.

LA REALIDAD MUNDIAL

Cada año se producen más de 600 millones de viajes turísticos internacionales. Un 20 por ciento de estos viajeros buscar sexo en sus desplazamientos, de los cuales un 3 por ciento confiesa tendencias pedófilas. Esto supone más de tres millones de personas que viajan por el mundo buscando sexo con niños¹.

El turismo sexual infantil afecta a más de dos millones de niños, niñas y adolescentes en el mundo, los cuales son obligados a ejercer la prostitución o a trabajar en pornografía. Sus practicantes son también los mayores consumidores de pornografía infantil, y proceden, fundamentalmente, de Estados Unidos, Alemania, Reino Unido, Australia y Japón².

El turismo sexual infantil es el principal motor de la mal llamada “prostitución infantil” (es decir, de la Explotación Sexual Comercial Infantil). Ésta se ha desplazado del sudeste de Asia, donde las penas se han endurecido, hacia Latinoamérica, por su legislación permisiva y altos niveles de corrupción³.

291

El turismo sexual infantil es un fenómeno que en estos últimos años se ha extendido por todo el mundo, en especial ha migrado de Asia a Latinoamérica. Éste se halla estrechamente ligado al tráfico de menores y a la pornografía infantil⁴.

1.- Fuente: Organización Internacional de Migraciones y Turismo

2.- Fuente: Organización Internacional del Trabajo (OIT)

3.- UNICEF y de la Organización Internacional del Trabajo (OIT)

4.- Fuente: Estudio “Explotación Sexual Infantil” – Plan de acción para Europa

1. DEFINICION DEL PROBLEMA

Los nacionales españoles y de otros países desarrollados viajan al extranjero para mantener relaciones sexuales con niños que se encuentran en situaciones de extrema pobreza, aprovechando su vulnerabilidad.

Los principales destinos son países donde el acceso a los menores es muy fácil porque:

- Los padres actúan en connivencia con las organizaciones de pederastas, vendiendo o alquilando a sus hijos menores de edad a cambio de dinero para subsistir
- El precio para acceder a un menor es muy bajo
- El riesgo de ser detenidos es nulo

La experiencia policial en este campo apunta como los principales destinos: Camboya, Tailandia, Filipinas, Costa Rica, México y los países del Este de Europa.

292

El proyecto HAVEN nació en el seno de Oficina Europea de Policía (EUROPOL), dentro del Fichero AWF-TWINS, dedicado a la lucha internacional contra la distribución de pornografía infantil por Internet. El proyecto HAVEN proporciona un escenario común para la lucha contra el turismo sexual relacionado con el abuso de menores en situación de pobreza. Se trata de perseguir al autor de la explotación, independientemente de su nacionalidad y del país en el que se ha consumado el delito. Por su parte, España tiene la responsabilidad de prevenir a otros Estados del riesgo que supone para sus menores la estancia de estos pederastas en sus territorios. Por este motivo, la Policía Nacional efectúa controles periódicos de los vuelos donde viajan personas con antecedentes por delitos sexuales, de prostitución y corrupción de menores.

En ocasiones, se ha logrado la extradición de autores españoles de delitos sexuales sobre menores cometidos en otro país, en concreto en Camboya, imputando no solo el delito de abusos sexuales sobre menores sino por la producción y distribución de pornografía infantil.

2. LA INVESTIGACIÓN ON-LINE

Los pedófilos han creado sus propias comunidades en Internet, donde no solo intercambian pornografía infantil, sino que además los usan para

comerciar información sobre donde deben viajar para abusar de menores y crear material pedófilo inédito. Los autores de estos delitos emplean turoperadores on-line que diseñan los viajes. Los pederastas comunican directamente con otros pedófilos que están en el destino turístico para que les proporcionen acceso a los menores y abusar de ellos. Después graban los abusos y los distribuyen o venden por Internet, es el llamado Cyber-Sex Tourism.

3. CARACTERÍSTICAS DEL PEDERASTA VIAJERO

Normalmente son hombres de mediana edad, entre 35 y 70 años, que habitualmente se desplazan solos o en compañía de un menor. Su pasaporte reflejará entradas en países que son escala obligada en el itinerario hacia sus destinos, siendo los más frecuentes: el Sudeste Asiático, Latinoamérica, Europa del Este, Filipinas y el sur de África.

Llevarán artículos sospechosos: medicamentos relacionados con el sexo, tipo Viagra, preservativos, golosinas, películas de Disney, juguetes, ropa para niños, etc.

Mercancía relacionada con medios de comunicación: cámara de vídeo y fotográfica, CD-ROM, DVD, revistas, literatura ligada a la pornografía infantil, correos electrónicos y cartas personales, ordenador portátil, etc.

293

4. ESPECIALIDADES EN LA INVESTIGACIÓN

Una vez que un ciudadano español ha sido identificado en el extranjero como autor de un delito relacionado con turismo sexual de menores, hay que tener en cuenta las siguientes consideraciones:

- La posible destrucción de pruebas por parte de autor/es
- Poner a salvo a las víctimas
- Recopilar las pruebas
- Conseguir la extradición del agresor

Es posible que el autor de los hechos intente llamar a su casa para destruir pruebas y evidencias del delito, por este motivo hay que intentar incomunicarlo. Hay que mantener a la víctima fuera de su entorno familiar, pues es habitual que su familia sea cómplice del delito.

El detenido puede borrar el rastro de cualquier operación bancaria que demuestre la evidencia del delito, así que hay que lograr bloquear sus cuentas.

Es preferible estar presente durante su custodia policial en el momento de la detención, porque es habitual que intenten sobornar a los policías de los países donde se ha cometido la agresión.

Es posible contactar con asociaciones de ayuda a la infancia; ONGs que estén presentes en la zona para que proporcionen ayuda social y apoyo psicológico a la víctima.

Se deben tener muy en cuenta las costumbres y tradiciones locales para comprender y no ofender a la víctima.

Hay que recuperar evidencias físicas del delito: pruebas médicas de los abusos o violaciones; recopilar toda la documentación relacionada con la operación; y explorar a la víctima y tomar declaración a los testigos.

Hay que conservar las posibles evidencias físicas: cámaras, fotografías, CD's, preservativos, juguetes y ropa de niño, ordenadores, teléfono móvil.

Se deben conservar todas las posibles pruebas documentales:

- Pasaporte, formularios extranjeros de acceso al país, visados, posibles grabaciones en hoteles, en la aduana, etc., fotografías del hotel y de los menores, certificados de nacimiento
- Recibos o resguardos de transferencias de dinero (Western Union)
- Resguardos de alquiler de vehículos

Hay que tomar declaración a la víctima y los testigos, estos últimos empleados de hotel, de policías de ese país, etc. Es fundamental que se ratifiquen en el juicio oral para poder acusar al autor por abuso sexual, y no solo por producción y distribución de pornografía infantil.

5. LA CRECIENTE INDUSTRIA DEL TURISMO SEXUAL CIBERNÉTICO

Se trata de producir y distribuir pornografía infantil a través webcams. Los autores de estos delitos usan cámaras web y salas de chat para grabar y difundir espectáculos de sexos, protagonizados por menores que se encuentran en otros países.

Los clientes de estas salas de chat pagan por visualizar cada uno de estos shows. A través de webcams sites conocen a otros clientes pedófilos. Los pagos se efectúan a través de banca on-line.

¿Por qué son tan populares?

- Son fáciles de utilizar
- Se obtienen altos márgenes de beneficio
- Son difíciles de investigar por la policía

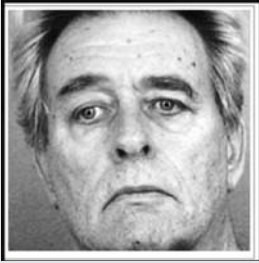
El resultado es que aumenta peligrosamente el número de niños explotados sexualmente y nuevas víctimas de abuso.

¿Cómo investigar la distribución de pornografía infantil a través de webcams?

- Hay que seguir el rastro de los pagos, el dinero
- Localizar a los autores de los abusos sexuales y de las víctimas en países extranjeros
- Examinar los equipos informáticos investigados
- Recuperar los correos electrónicos
- Investigar los posibles viajes al extranjero realizados por el objetivo

6. CASOS REALES RESUELTOS

DONALD MATHIAS



- Fue condenado a 20 años de prisión
- En Filipinas abusó de dos menores, de 11 y 12 años de edad
- Las víctimas le denunciaron porque las obligaba a mantener relaciones sexuales con él
- La madre de las menores y Donald Mathias intercambiaron cientos de correos electrónicos relativos a las actividades sexuales entre el estadounidense y sus hijas, y pactaron que grabarían lo abusos para luego distribuirlos en Internet
- Pagaba por adelantado sus servicios a través de Western Union
- Cuando abusó de las niñas, éstas no tenían más de cinco años
- Admitió su culpabilidad en el juicio

JOHN WRENSHALL



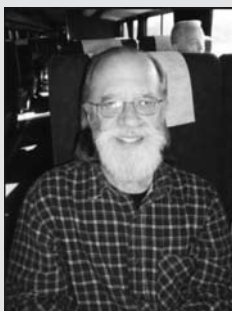
- Nacionalidad canadiense
- Fue detenido en el Aeropuerto de Londres por fomentar el turismo relacionado con el abuso de menores encubierto en viajes de negocios
- Facilitaba los contactos con los menores
- Trabajaba como profesor en la Escuela de Idiomas de Bangkok
- Pudo ser detenido como consecuencia de la declaración de un pederasta también detenido, quién explico el “modus operandi” de la empresa de John Wrenshall

WAYNE NELSON CORLISS



- Es ejemplo de una investigación que se inicia identificando al protagonista de una serie de fotografías distribuidas en Internet, y en las que Wayne Corliss abusaba de tres varones menores asiáticos
- Se le acusa de abuso sexual a menores, producción y distribución de pornografía infantil en la Red

THOMAS PENDLETON



Fue condenado a 30 años de prisión por violación de un menor de 14 años

- Viajaba desde Filadelfia, en Estados Unidos, a Alemania para mantener relaciones sexuales con la víctima, que vivía en un orfanato
- Firmó un contrato con el orfanato para que el menor le acompañara durante un mes con la excusa de llevarlo de viaje. En ese tiempo el niño sufrió los abusos

297

KENT FRANK

- Fue detenido por abusar de tres menores en Camboya, previo pago para que le permitieran grabar durante los abusos y distribuir el material en la Red

<p>Abuse a child in this country, go to jail in yours.</p> <p>Stop child sex tourism.</p> <p><small>In 2004, World Vision joined forces with national governments, law-enforcement agencies and other organizations to combat child sex tourism through the Child Sex Tourism Prevention Project.</small></p>	<p>Miami Man Sentenced to 40 Years in Prison for Sex Tourism and Child Pornography Offenses in Cambodia</p> <p>Miami, Florida July 31, 2007</p> <p>According to a U.S. Department of Justice news release, Miami resident Kent Frank was sentenced to 40 years in prison on sex tourism and child pornography charges. The judge also ordered Frank to pay a \$25,000 fine and serve 15 years of supervised release.</p>
--	---

Save the Children, en su informe “Rompamos las cadenas de la esclavitud infantil”, explica que este nuevo “tipo” de turismo es la práctica de abusadores que escogen, deliberadamente, destinos donde saben que pueden pagar para mantener relaciones sexuales con niños, violándoles y forzándoles a posar para ser fotografiados en posturas sexualmente humillantes.

Estas actividades se desarrollan gracias a los clientes “locales” de los “paraísos del sexo”, y de los denominados “turistas sexuales”. Desde 1980, cuando ONGs internacionales adoptaron esta definición para denunciar el tipo de turismo que se estaba desarrollando, el turismo sexual ha crecido tan rápidamente que hoy es en un negocio lucrativo en el cual están involucradas miles de personas.

Anualmente, supone una fuerte contribución al empleo y una importante entrada de ingresos en los países donde se desarrolla. Incluso las autoridades gubernamentales reciben beneficios económicos, unas veces legales –tasas de licencia e impuestos de los hoteles, bares, restaurantes y casas de juego– y otras ilegales, procedentes de sobornos, asegura la Fundación Renacer, que lucha contra la explotación sexual infantil en Colombia, país en el que la cifra de niños explotados sexualmente media los 20.000.

298

7. MATRIMONIO FORZOSO

Se habla de matrimonios forzosos cuando, al menos, uno de los miembros de la pareja no da su consentimiento y es obligado a casarse. En el citado informe, esta misma organización asegura que, en la próxima década, 100 millones de niñas contraerán matrimonio antes de cumplir 18 años, obligadas por sus padres u otros familiares. Ellas son siempre las más afectadas por esta esclavitud infantil, y quienes sufren las consecuencias más severas: intimidación, secuestros, violaciones y asesinatos. Una niña o una mujer obligada a casarse se convierte en una esclava, forzada a vivir y dormir con su marido, y confinada a permanecer en el interior del hogar; negándoles la educación, poder trabajar fuera de casa y convertidas en dependientes totales de sus maridos.

8. LAS CAUSAS DE SIEMPRE

La pobreza crónica es una de las razones más importantes para que los niños estén en riesgo de explotación. Las crisis económicas, el aumento del desempleo y factores sociales y políticos contribuyen a un aumento sin precedentes en la explotación sexual infantil. Las guerras y los desastres naturales son períodos claves en la intensificación de los índices de explotación sexual, como medida desesperada de supervivencia. Las organizaciones

que atacan esta práctica ilegal aseguran que el número de niños explotados sexualmente con fines comerciales va en aumento, y la prostitución infantil los atrapa, cada vez, a más temprana edad. Falsas creencias, como la de no contraer enfermedades de transmisión sexual como el VIH/SIDA si se mantienen relaciones sexuales con niños y niñas, favorecen este aumento.

9. LAS CONSECUENCIAS

Una vez introducido en el mercado del sexo, las posibilidades de encontrar fuentes de ingreso alternativas son casi nulas para el menor involucrado: la falta de una formación adecuada, las posibles enfermedades contraídas o el estigma social que implica haber trabajado en el comercio sexual suponen grandes obstáculos para reinsertarse en la sociedad con un trabajo digno, afirma Save the Children.

La explotación sexual tiene un impacto devastador para cualquier menor. Permanecen bajo el control total de sus abusadores, son utilizados como mercancías, sufren violaciones y palizas y, en ocasiones, son torturados. Viven con un alto riesgo de sufrir problemas de salud, física y mental de larga duración, como el VIH/SIDA. Rara vez reciben algo de dinero, tan sólo comida y un sitio para dormir para que puedan seguir trabajando. Incluso aquellos que regresan a casa se enfrentarán a una tremenda estigmatización, especialmente porque no han ganado dinero o han estado involucrados en el mundo de la prostitución.

299

10. PARA TENERLO PRESENTE

“Somos los niños y niñas del mundo. Somos las víctimas de la explotación y el abuso. Somos niños y niñas de la calle. Somos niños y niñas de la guerra. Somos las víctimas y los huérfanos del VIH-SIDA. Se nos niega una educación de buena calidad, así como buenos servicios de salud. Somos las víctimas de la discriminación política, económica, cultural, religiosa y del medio ambiente. Somos los niños y niñas cuyas voces no se oyen. Es hora de que nos tomen en cuenta. Queremos un mundo adecuado a las necesidades de los niños y niñas, porque un mundo adecuado a nuestras necesidades es un mundo adecuado a las necesidades de todos”⁵.

5.- Mensaje de los niños en la Sesión Especial a favor de la Infancia de la ONU, New York (Estados Unidos), 8 de mayo de 2002.

11. LOS NIÑOS DANZANTES DE AFGANISTÁN: LOS BACHA BAZI⁶

“En un mundo de hombres, en el que las mujeres carecen de consideración y son tratadas como objetos, como ocurre en las tribus pastunes de Afganistán, los niños son raptados para sustituir a las mujeres en algunas fiestas tribales. Normalmente son comprados a sus padres y ofrecidos a hombres maduros y ricos, que los disfrazan de mujer para bailar y satisfacer sexualmente a sus dueños. Actúan en fiestas en las que las mujeres no pueden estar presentes y de alguna manera ellos las sustituyen. Son los Bacha Bazi”.



Los niños son raptados o comprados antes de llegar a la pubertad. Una vez en cautiverio se les viste de mujer, se les obliga a comportarse como tal y, generalmente, deben satisfacer las necesidades sexuales de los varones que lo soliciten. Si no aceptan son violados y, en muchas ocasiones, asesinados.



6.- Fuente consultada: artículo publicado en L'armari Obert

La tradición proviene del mundo persa. Para ellos en el paraíso estaban los ghilman, esperándoles para dar satisfacción. Eran unos eunucos feminizados, premio para los hombres justos. La realidad era que muchos generales, reyes y potentados tenían por costumbre tener jóvenes esclavos a su entera disposición. (Para ampliar información: <http://leopoldest.blogspot.com/2011/08/los-ghilman-mitologia-y-realidad.html>).

A finales del siglo XIX esta costumbre fue prohibida, trasladándose a los montes de Afganistán y el Turkestán. Los bacha bazi que se adaptaban podían acceder después a tener una situación privilegiada en el mundo de los negocios, pero muchos no tenían tanta suerte y eran asesinados por negarse a servir o abandonados al perder la juventud. La inmensa mayoría se veía abocado a un final trágico. Con el régimen talibán esta costumbre fue prohibida, pero hoy día la situación no ha cambiado.

El diario *The Guardian* lo explicaba así:

“La práctica de tomar a los muchachos jóvenes para que actúen como bailarines en fiestas privadas que se conoce como bacha bazi (literalmente “chico para jugar”) es una tradición afgana con raíces muy profundas. Bajo el régimen talibán se prohibió esta práctica, pero ahora se ha vuelto hacia atrás y se ha extendido, pues florece también en las ciudades, incluida la capital, Kabul, y es común en las bodas, sobre todo en el norte. Los bailarines bacha son a menudo niños violados cuyas familias las han repudiado. Sus “dueños” o “maestros” pueden ser hombres solteros o casados, que los mantienen en una forma de esclavitud sexual, como concubinas. Los bachas suelen ser liberados a la edad de 19 años, cuando pueden casarse y reclamar su condición de “macho”, aunque el estigma de haber vivido como una bacha es difícil de superar. Las autoridades afganas y los grupos de derechos humanos son conscientes de la difícil situación de los niños bacha, pero parecen incapaces de detenerlo.”



En Afganistán la transexualidad es tolerada, es mas fácil hablar o ver a un transexual que a una mujer, siempre dentro del burka y huyendo de cualquier presencia masculina. En cambio la homosexualidad es perseguida cruelmente.

Información de interés:

Documental “Los muchachos de Danza de Afganistán” Emitido por TVE el 20 de noviembre de 2010. <http://vodpod.com/watch/4185357-bacha-bazi-or-boy-play->

Video sobre los Bacha Bazi: <http://www.youtube.com/watch?v=zNUxq8rI6IM&am;NR=1>:



QUINTO PANEL

EL USO DE LAS REDES SOCIALES EN LA EMPRESA

MANUEL CARPIO CÁMARA
Director de Seguridad de la Información y
Prevención del Fraude de Telefónica

El tema de las redes sociales en la empresa actual, para qué se usan, qué errores son los que se han cometido y que no deberían producirse cuando se incorporan las redes sociales a los negocios, cuáles son las preocupaciones de seguridad que esto conlleva, y la Política de Uso Aceptable, la UPA, que es la piedra angular en la que ha de basarse la incorporación y uso de las redes en la empresa, son asuntos clave.

305

En el año 2012, Google encargó a la consultora internacional Millward Brown un estudio para conocer cómo se percibía en las empresas el uso de las redes sociales, cómo les estaban ayudando y qué intenciones albergaban las corporaciones de ámbito europeo para la adopción de las redes sociales como otra fórmula para potenciar el business. Las encuestas se realizaron en países europeos y la muestra estuvo constituida por 2.700 profesionales y directivos de las más importantes empresas del Viejo Continente. Entre las conclusiones, se señalaba que los directivos de las organizaciones italianas y españolas eran los más proclives a adoptar el uso de las redes sociales dentro de sus entidades empresariales. Esto no sorprende demasiado ya que la telefonía móvil, cuando comenzó su andadura, hace 15 años, mostró que los países del área mediterránea eran más proclives a la socialización, también dentro de la empresa, y a la utilización de esos medios de comunicación social. España e Italia tienen una enorme penetración de terminales móviles y, en general, todos los países latinos la tienen, mucho más que los países nórdicos, y no era de extrañar que el uso de las redes sociales también fuera

algo parecido. En realidad es otro medio más de comunicación social. Por lo tanto, no sorprendían las cifras.

Según ese mismo informe, el 77 por ciento de los encuestados que trabajaban en el sector multimedia, en el sector creativo, ya usaban las redes sociales de forma habitual. Les seguía, a corta distancia, las empresas retail, de gran consumo, de bienes básicos, de distribución, etc. En última posición se ubicaban las entidades de transporte, cuyos profesionales y directivos no usaban habitualmente las redes sociales, solo el 57 por ciento.

306 A esos directivos también se les preguntó cómo podían ayudar las redes sociales a sus empresas. En ese caso, básicamente indicaban que se ahorra tiempo en lectura y envío de correos electrónicos, y también que se ahorra en viajes. En un momento en el que la restricción de costes estaba y está tan de moda, en todas las empresas el uso de redes sociales es una buena opción para mantener esa integración necesaria de la organización, promover esa gestión del conocimiento, que es muy importante, y el ahorro de costes en viajes y en tiempo en esos desplazamientos. Otra respuesta que señalaban es que las redes sociales podían ser un impulso al negocio, dado que mantiene a la entidad en contacto con los clientes. Muchas empresas están abrazando las redes sociales porque sus clientes se están yendo a las redes sociales. Si los clientes se desplazan a otras formas de comunicación, los proveedores de servicios se tienen que trasladar con los hábitos de los clientes, es evidente que es así. Esto también plantea una serie de problemas que son interesantes, y que se verán más adelante, como por ejemplo: ¿es un comercial dueño de su perfil una red social de un comercial si ese perfil lo tiene asociado a su correo empresarial? En Estados Unidos ya se están produciendo litigios por la propiedad de los perfiles en las redes sociales, ya que cuando el comercial se va de la empresa se quiere llevar a sus clientes pero no está definido de quién es ese perfil. Ésta es una de las novedades que se está produciendo en la empresa con respecto a las redes sociales, y hay que ir adaptándose a estas circunstancias.

El estudio tenía tres campanadas u ofrecía tres hallazgos:

- El primero es que, contra todo pronóstico, los directivos *senior* eran más proclives al uso de las redes sociales dentro de la empresa, frente a los jóvenes: un 71 por ciento ante un 39 por ciento
- Sobre cómo va a afectar al crecimiento del negocio, el 59 por ciento de los encuestados señalaban que estaban convencidos de que el uso de las redes sociales iba a incrementar el volumen de negocio –el 76 por ciento de las empresas que están adoptando las redes sociales están cre-

ciendo a nivel de dos dígitos, es decir, hay una correlación muy fuerte entre las empresas de alto crecimiento, según lo que refleja el estudio-. El 53 por ciento de los encuestados indicaba que las empresas que no abracen las redes sociales para los dos puntos anteriormente mencionados no van a sobrevivir. Probablemente no porque las utilicen o no, sino porque serán compañías que se irán quedando en un ambiente arcaizado, y eso, lógicamente, no augura nada bueno

- La tercera gran campanada del informe aparecía cuando preguntaban a los propios profesionales sobre ellos mismos, sobre cómo veían su proyección profesional en el mercado laboral. En este caso, se mostraba una clara correlación entre profesionales de éxito, entendido éste en cuanto nivel salarial y de promoción profesional dentro de la empresa, de valoración en el mercado, entre los que usan redes profesional y los que no. El que existan esas correlaciones entre empresas de alto rendimiento y profesionales de alto rendimiento y el uso de redes sociales no significa que una cosa lleve a la otra. El hecho de estar en redes sociales es indicativo de otra serie de atributos, tanto en la empresa como en el trabajador, que les hacen especialmente exitosos en los tiempos que corren

¿Para qué se están usando en las empresas las redes sociales? Fundamentalmente para dos cosas:

- Para colaboración entre empleados
- Para monitorización de trabajadores. En este caso se refiere a qué cuando una persona abre una red social a Internet desde su empresa, lo que está haciendo es algo serio, ya que está desplegando las puertas de los datos de su empresa –datos de carácter personal sobre sus clientes y otras áreas–, al mundo exterior, y eso conlleva una serie de riesgos. Poner la empresa en una red social no significa enchufarla, hay que adecuarla a la casa antes de enchufarla a una red social

En ese sentido, en Estados Unidos hay, actualmente, dos tipologías de litigios relativos a la monitorización de trabajadores: los relacionados con la contratación y aquéllos en los que el empleado está ya trabajando en la empresa. En el primer tipo el caso típico es cuando una persona tiene su perfil en Facebook. La compañía que lo va a contratar accede y hace su amigo, con lo que pasa a conocer cosas de ese candidato que, quizás, no vienen a cuento para la contratación, pero se entera, y decide no contratarle. Cuando esa persona conoce que no ha pasado a formar parte de la plantilla por algo que encontraron en su perfil, pone una demanda a la compañía y entran en

litigio, ya que la organización ha invadido su intimidad y no estaba todavía dentro de la empresa. El otro caso habitual es el del empleado de Recursos Humanos que emplea la información en las redes del personal para despedirle.

Todas estas situaciones están muy bien tasadas en Estados Unidos: qué cosas se pueden y qué cosas no se pueden tener en cuenta a la hora de contratar, a la hora de tener una relación laboral con un empleado, etc. Hay acciones que están prohibidas: discriminación por raza, por tipo de amistades, etc., y su empleo ha llevado a los tribunales muchos litigios por supuesta discriminación por datos encontrados en los perfiles de las redes sociales.

El segundo problema fundamental se comete porque no existen unas buenas prácticas y unas buenas políticas publicadas sobre cómo ha de hacerse una correcta contratación e investigación del mercado laboral, principalmente por parte de los *headhunters*. Cuando el empleado está trabajando, hay una relación laboral entre éste y la empresa, y si el trabajador usa las redes para hablar de su empresa y ésta ve que tiene un comportamiento que no es adecuado para la entidad entonces le despide. Este despido se declara improcedente, ya que no está regulado en las normativas internas de la compañía cuál es el uso que sus colaboradores deben hacer de las redes sociales, bien de forma privada hablando de la empresa o bien dentro de la empresa.

Otro error gravísimo de las empresas es tratar de averiguar qué está pasando dentro de las mismas, inmiscuyéndose de forma subrepticia en los perfiles de los empleados, haciéndose pasar por amigos. Esto es una mala práctica, y por ello es fundamental que las entidades dispongan de una Política de Uso Aceptable (PUA). Un ejemplo de ello es el caso de L. Simonetti. Esta azafata de Delta Airlines tuvo una desgracia personal en 2003 -su madre murió de cáncer- y entró en depresión. Su psicólogo o su psiquiatra le aconsejó que abriera un blog y que contara su vida, y así lo hizo. Lo llamo “Diario de una Azafata Disfuncional” y contaba sus viajes como azafata, daba consejos a los viajeros, pero sin nombrar a la aerolínea. El blog fue un éxito pero Delta Airline la despidió de forma improcedente, dado que esa actitud no formaba parte de la cultura de empresa y no estaba indicado en ningún sitio qué debía de hacer el empleado ante las redes sociales. Se convirtió en un escándalo mediática y Delta Airlines, muchos años después, terminó pagándole a L. Simonetti una cantidad no revelada.

Otro caso real fue el de un empleado que le dijo a su jefe que su familia en Nueva York había tenido un grave problema y que debía irse urgentemente pues era un caso de vida o muerte. A continuación, la urgencia familiar aparece en Facebook y el jefe le dice: “Oye, espero que no haya sido

nada lo de tu padre. Ah, por cierto, preciosa varita”. Esto demuestra que los errores no solo los cometen las empresas, también los empleados.

Contra esos equívocos, hay que ejercer buenas prácticas. La más importante es tener una Política de Uso Aceptable (PUA) y, si es posible, referida específicamente a las redes sociales. Pero, de forma general, previa a la contratación, la recomendación es que la entidad disponga de una parte neutral que realice las búsquedas sobre los medios de comunicación social, es decir, un proveedor externo que lleve a cabo el proceso de selección basado en temas de redes sociales, y esa acción ha de ser neutral y no discriminatoria. Por ejemplo, si se va a contratar a una persona para trabajar en Madrid, no se puede ir a buscar candidatos en los perfiles de Facebook del Real Madrid, o no contratar a un candidato porque en su perfil señala que es seguidor del Fútbol Club Barcelona y el contratador es forofo del Real Madrid. La neutralidad y la no discriminación han de ser parte de la política establecida por la empresa. Ha de analizar la información sobre los candidatos de forma uniforme. Y, por supuesto, no hacerse amigo de ellos o hacerse pasar por sus amigos para fisgonear en sus perfiles. Otra equivocación es indicarle al candidato quiénes son los otros competidores que están en liza, porque lo que va a hacer a continuación el candidato es ver qué cosas tienen ellos en sus perfiles que no tiene él y luego puede llevar a los tribunales a la empresa por discriminación.

309

También la organización tiene que explicar a sus colaboradores que la red social no está para que unos hablen mal de otros. Una cosa muy interesante que se ha establecido en Estados Unidos es la obligación de que el equipo no puede hablar mal de la compañía en la red social no si antes no lo han comunicado a su departamento de Recursos Humanos. Hay que explicarles que si tienen un problema deben transmitirlo a su jefe, dado que acudir primero en la red genera un mal clima laboral. Esto también debe estar plasmado en la Política de Uso Adecuado (UPA).

Es también interesante el uso del correo de la empresa para inscribirse en las redes sociales, dado que hay personas que lo emplean. La identidad en Internet hoy día es el correo electrónico, los nicks no valen nada, dado que lo que realmente identifica a las personas es una dirección de correo electrónico, porque son irrepetibles, y también lo es la dirección que asigna la empresa a cada empleado, y que es un recurso de la entidad. De modo que, que cuando el empleado usa su dirección en las redes comienza el problema. Tanto si acepta invitaciones de otras personas como si se va de la empresa. En ese último caso, la compañía de baja esa dirección de correo y el empleado ya no puede acceder a ella, ni a los contactos que en ella tenía asignados. Es clave gestionar de qué manera se van a usar las direcciones de

correo electrónico a la hora de darse de alta en las redes sociales para hacer *business*.

En cuanto a los supervisores y agentes, hay una recomendación muy importante: nunca hay que pedir ni obligar a un subordinado a que se haga su amigo o a que le entregue sus claves. En todo caso, que sea él quien acepte a su jefe como amigo.

También está el asunto de las comunicaciones protegidas dentro de la empresa, que en Estados Unidos está regulado por ley. El argumento de la protección del ejercicio de los derechos sindicales dentro de la corporación y su relación con las comunicaciones dentro de la empresa es muy importante, y afecta a las redes sociales. Además, hay muchas compañías que son multinacionales, y que tienen que tener en cuenta el máximo común denominador de todas las legislaciones de los países en los que están presentes. Eso se regula también mediante una Política de Uso Aceptable (PUA).

310 Es muy importante a su vez dejar claro a los trabajadores en el momento del despido en qué condiciones van a poder utilizar las redes sociales, qué cosas se van a permitir y qué cosas no cuando hable en las redes sociales de la compañía de la que deja de formar parte. Esto también es fundamental a la hora de firmar los finiquitos, y esta poco regulado en las empresas españolas privadas.

Existe una contrapartida al informe de Millward Brown. Es la encuesta del Instituto Ponemon para la empresa norteamericana Websens, un fabricante mundial de uno de los líderes de seguridad para aplicaciones web en el mundo de Internet. La muestra es de 4.600 entrevistas entre responsables de informática y comunicaciones de las mayores empresas del mundo y trata sobre los problemas de seguridad que implica el uso de las redes sociales dentro de las entidades. Lo primero que se desprende es que los trabajadores pierden 40 minutos diarios de su tiempo chateando con los amigos en aquellas empresas que tienen redes sociales. El caso más sangrante sería Australia, donde a nivel global el estudio dice que se ahorrarían 5.000 millones de dólares al año si quitaran el uso de las redes sociales en las corporaciones.

Lo que está pasando es algo muy sencillo. ¿Redes sociales en la empresa?: sí, pero según de qué manera. Como todo en la vida. Redes sociales sí para los objetivos de negocio.

Uno de los conflictos más importantes que para un responsable de seguridad en una empresa tienen las redes sociales es la cuestión de la ingeniería social. Es una técnica muy conocida, ancestral, ya la usaba Kevin Mitnick, el

primer hacker de sistemas telefónicos a principios de los 90, cuando llamaba por teléfono haciéndose pasar por un tipo de mantenimiento de la red telefónica para que le dieran acceso al ordenador central y hacer llamadas gratis. Es ingeniería social, y es engañar al destinatario y hacerle pensar que se trata de otra cosa. Los empleados, inconscientemente, van a caer en ese tipo de engaños, que son muy efectivos en Internet. De ahí, la necesaria y urgente monitorización que se indicaba anteriormente mediante sistemas de inteligencia de seguridad. La seguridad que existe pero no se nota. Ésta está dando actualmente grandes frutos en la prevención de este tipo de situaciones.

También hay que hablar en el uso de las redes sociales en la empresa de la culpa “in vigilando”, un concepto que, básicamente, significa que cuando un empleado tiene un error a sabiendas, por ejemplo porque maneja información confidencial, y lleva a la empresa a un problema, el que va a la cárcel es el secretario general o el apoderado o el administrador de la empresa por culpa “in vigilando”, si se demuestra que así ha sido, dado que no ha controlado el uso que de la red social estaba haciendo ese colaborador y con ello se han cometido delitos societarios.

Las empresas tienen que crear una Política de Uso Aceptable (PUA) que es todo lo que la compañía le dice al trabajador en el momento de la contratación, y que le entrega en un anexo, y que son las obligaciones que contrae con la empresa, entre otras cosas en el uso de los recursos que la organización pone a sus disposición. Estos recursos son: la fotocopidora, el teléfono, la PDA, el ordenador, el uso de las claves de acceso a su equipo, etc. También le tiene que informar sobre las políticas sanitarias, es decir, cómo debe emplear esos recursos.

311

También está el tema de la monitorización. Según datos de la Organización Mundial de la Salud, el 2 por ciento de la población mundial es psicópata. La labor del área de seguridad interna es controlar que esas personas, que no se puede evitar que sean así, metan a la empresa en un lío. Por eso hay que monitorizar el uso que de estos recursos hacen los equipos.

LA AUTORREGULACIÓN COMO SISTEMA DE PROTECCIÓN DE LA SEGURIDAD EN LAS REDES SOCIALES: EL CASO DE TUENTI

ÓSCAR CASADO OLIVA
Director de la Asesoría Jurídica de Tuenti.
Grupo Telefónica

313

Tuenti es una empresa española que el Grupo Telefónica adquirió en el año 2010. Esta red social está sometida a la legislación española, de modo que, a diferencia de otras redes sociales, tiene una serie de obligaciones, de responsabilidades según la legislación de este país y, de cara a la colaboración que tiene con las Fuerzas y Cuerpos de Seguridad del Estado español, muchas veces la relación es más sencilla y más fácil por el sometimiento a la Ley de España.

La web 3.0 es aquella en la que el usuario es el protagonista, es activo y genera la información. Antes se adquiría Internet para leer páginas, el periódico, el correo electrónico, pero en la actualidad es el usuario el que sube la información a las redes sociales, y eso ha producido un cambio de paradigma muy importante, con una serie de implicaciones.

Cualquier negocio digital, y Tuenti es uno de ellos, está basado fundamentalmente en 3 pilares:

- Una tecnología excelente
- El usuario
- La privacidad, como elemento básico para el éxito de un negocio digital

La combinación de esos tres elementos es fundamental para el éxito de cualquier servicio en Internet. Hay casos, como Google Street View, que ha tenido fallos de seguridad, como por ejemplo la captación de las imágenes de las personas por la calle o las matrículas de los coches, y debido a esos problemas en materia de privacidad no han tenido el éxito que esperaban. Por lo tanto, la privacidad genera seguridad y confianza en el usuario en el entorno Internet.

ENTORNO. INTERNET YA ES UNA REALIDAD

El 68,5 por ciento de la población española es internauta; están 13,6 horas semanales conectados; 68 son los minutos que dedican a las redes sociales; 9 de 10 toman parte en redes sociales; el 96 por ciento de los jóvenes se conectan diariamente a la Red (68 minutos/día), y en materia de ingresos publicitarios la Red ya es el tercer medio en inversión con 799 millones de euros.

Para Tuenti, Internet en el futuro será social y móvil. La Red es ya un entorno colaborativo o participativo, es un canal multidireccional abierto que permite lograr la máxima interacción entre las personas, ofreciendo posibilidades de colaborar, de expresarse, de participar y buscar a otros, por tanto es una herramientas diseñadas para crear espacios que facilitan la comunicación y el intercambio social, es el denominado *Social Networking*.

Según los datos antes expuestos, España es, junto con Estados Unidos y Brasil, uno de los países del mundo donde más se utilizan las redes sociales. A los cifran anteriormente expuestas habría que añadir: el 30 por ciento del tiempo que los usuarios españoles pasan en Internet lo dedican a las redes sociales; el 82 por ciento utilizan herramientas *social media* de una forma habitual; el 40 por ciento las consultan a diario; el 96 por ciento de los adolescentes entre 14 y 24 años se ha registrado alguna vez en una red social; y el 75 por ciento de quienes operan en redes sociales opina que es el medio más divertido, frente al 14 por ciento que hace considera lo mismo sobre la televisión.

La tres C que definen a una red social son:

- Comunicación, es decir, poner conocimientos en común
- Comunidad, encontrar e integrar comunidades afines
- Cooperación, hacer cosas juntos

TUENTI

La convivencia entre el mundo de la televisión y el mundo de Internet es una realidad, en el caso de España el 25 por ciento de los usuarios españoles está conectado a Internet mientras ve la televisión.



315

Un ejemplo es este gráfico, que muestra el uso de Tuenti –en donde cada día se intercambian 400 millones de mensajes durante la final del Mundial de Sudáfrica en ¿2010?: cuando dio comienzo el partido, el número de personas conectadas era muy alto; al comenzar la primera parte, cayó totalmente el uso de Tuenti; en el descanso empezó a subir de nuevo, lo que significó que en ese periodo los usuarios comentaron la primera parte, empezaron a enviarse mensajes, subieron fotografías; en la segunda parte el uso volvió a descender; se incrementó nuevamente en la prórroga; descendió en el descanso; y al final del partido empezó a remontar nuevamente.

Tuenti es el mayor site web y móvil que existe hoy día en España: el 15 por ciento del tráfico web de ese país pasa por Tuenti, lo que significa 40.000 millones de páginas vistas al mes (los periódicos Marca o El Mundo tienen unas 4.000 millones de páginas). Desde hace unos meses ha pasado a ser internacional, con una gran presencia en Latinoamérica, y con un cambio de imagen en la aplicación móvil y la página web. La entidad está

formada por 260 empleados de 21 nacionalidades, de los cuales el 50 por ciento son ingenieros. Este impresionante equipo humano atiende, en el caso de la Guardia Civil y de la Policía, todos los requerimientos, los oficios y los mandamientos, una media de 15.000 denuncias diarias, que también incluyen las de los usuarios particulares y entre las que se encuentra: pornografía infantil, acosos, amenazas, etc.

Las tres principales características que diferencian a Tuenti de otras redes sociales son:

- Modelo de acceso por invitación o teléfono móvil verificado

Tuenti ha comprobado que el 90 por ciento de las conversaciones se realizan con 20 personas, nadie tiene 300 amigos. Por eso Tuenti ha separado el concepto de “contacto” del de “amigo”, y en un entorno privado ha creado una plataforma con un modelo de acceso por invitación o por teléfono verificado. Eso significan perfiles reales, personas reales, no nicknames, ni pseudónimos, que se ocultan detrás de esa identidad con, probablemente, no muy buenas intenciones.

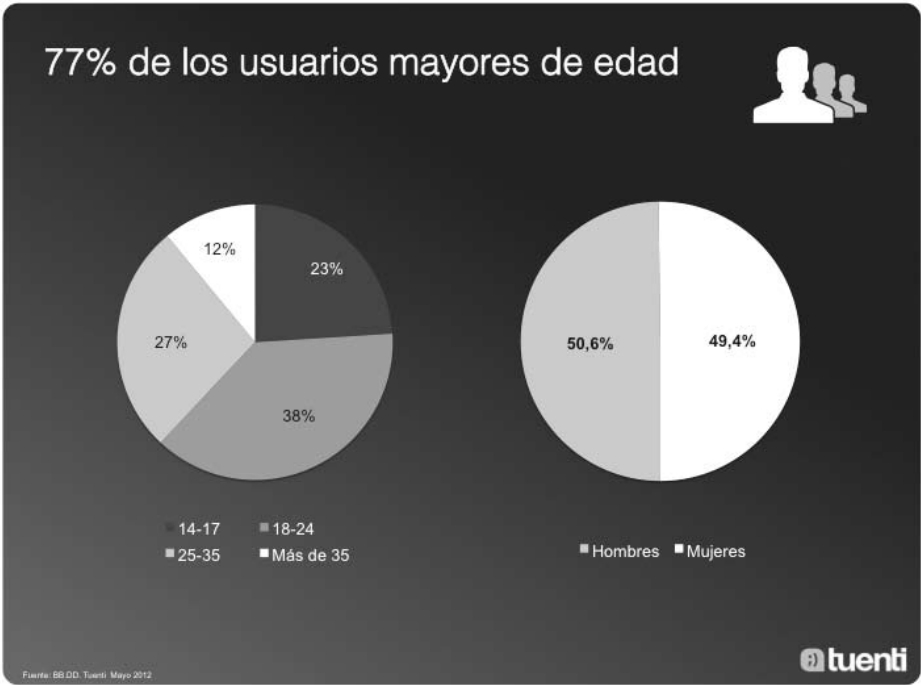
316

- La información personal de los usuarios no se indexa en ningún buscador, y ésta es la principal característica de la privacidad de esta red social. En el momento en que una red social indexar los contenidos en un buscador la información se pierde, se disemina por la red y el usuario ya no sabe dónde han ido sus datos
- Gente real, información real, relaciones reales

Tuenti tiene 14 millones de usuarios en España, Facebook 15 millones y medio en ese país y 1.000 millones en el mundo. Tuenti cuenta con una media de 100 minutos diarios, la media de Facebook es de 20-25 minutos. Eso significa que el usuario de Facebook entra, físgonea, ve lo que ha hecho un amigo, la fiesta de aquél y sale. El de Tuenti utiliza esa red como un medio de comunicación alternativo a la voz y al SMS. El 77 por ciento de sus usuarios son mayores de edad, en contra de lo que muchas veces se comenta de que es una red social solo para menores, y esta edad media es cada vez mayor.



317



Cobertura superior al 93% entre 14 y 35 años



Usuarios +14 años

13,3MM

Penetración **34%**



Usuarios 14-35 años

11,8MM

Penetración **93%**

Fuente: BB.DD. Tuenti. Mayo 2012, IRE Abril 2012

 **tuenti**

318

Sitio móvil y Apps

+40% de los usuarios de web acceden también vía móvil

5 MM usuarios mensuales

Más de un millón de fotos subidas por móvil al mes

Aplicaciones disponibles para iPhone, Java, Android y Blackberry

Más de 25.000 personas instalan la App de Tuenti en sus terminales cada día

•m.tuenti.com

1,7 MM usuarios únicos mensuales

Más de 300 MM páginas vistas/mes

Más de 250.000 usuarios únicos día

Más de 3 MM de impresiones a lo largo del día (home y profile).



Fuente: BB.DD. Tuenti. Marzo 2012

 **tuenti**

REDES SOCIALES, PRIVACIDAD Y MENORES: EL GRAN RETO JURÍDICO Y EDUCATIVO

La edad mínima para acceder a una red social o cualquier servicio de la sociedad de la información son 14 años. El control de acceso es uno de los problemas que encuentra Tuenti en su día a día, y la gran preocupación de los propios padres. Ante esta situación: ¿cómo controla Tuenti la longevidad de sus usuarios? En este momento no existe un mecanismo técnico viable de verificación, por lo que esta condición se resuelve mediante un acuerdo alcanzado con la Agencia de Protección de Datos en virtud del cual la red social de Telefónica se compromete a abordar una media de unos 1.500 perfiles al día sospechosos de ser menores de 14 años. Cuando duda de un usuario le solicita su Documento Nacional de identidad (DNI) y, en caso de no facilitarlo, la compañía borra su perfil, cumpliendo así con el artículo 13 del Reglamento de Protección de Datos.

Las redes sociales que consideran que no deben regirse por las normativas española ni europea de protección de datos, no llevan a cabo estos protocolos de seguridad. Esto provoca desventajas competitivas, desequilibrios a la hora de competir en el mercado global que es Internet, en el que quiebra el principio de territorialidad en la aplicación de las leyes. Se trata de un problema de derecho y redes sociales o derecho y tecnología, y es normal que esta última vaya dos o tres pasos por delante del derecho, lo que genera muchos conflictos. Es un reto para los abogados que se dedican a este campo buscar soluciones creativas para intentar cumplir la Ley.

319

La edad de acceso a Internet es cada vez menor, de hecho existe un reglamento en la Comisión Europea que va a rebajar la edad a 13 años, dado que los nativos digitales cada vez acceden antes a Internet.



POWERPOINT

ÓSCAR CASADO OLIVA
Director de la Asesoría Jurídica de Tuenti.
Grupo Telefónica

Curso de Verano de El Escorial

Policía 3.0: Redes Sociales y la nueva dimensión de la seguridad

San Lorenzo de El Escorial, 13 de julio 2012



Oscar Casado Oliva
Director Jurídico y de Privacidad



322



LA AUTORREGULACIÓN COMO SISTEMA DE PROTECCIÓN DE LA SEGURIDAD EN LAS REDES SOCIALES: EL CASO DE TUENTI

Internet colaborativo

Canal multidireccional abierto que permite lograr la máxima interacción entre los usuarios y les ofrece nuevas posibilidades de colaboración, expresión y participación.

Internet social

Social Networking: Herramientas diseñadas para la creación de espacios que faciliten la creación de comunidades de intercambio social.

Redes sociales: ¿conversamos?

- 30%** Tiempo en Internet que dedicamos a las redes sociales.
- 82%** De los internautas españoles utiliza social media de forma habitual.
- 39%** De los usuarios de redes sociales las consulta a diario.
- 96%** De jóvenes entre 14 y 24 se han registrado alguna vez en una red social.
- 75%** De usuarios de redes sociales opina que es el medio más divertido, frente al 14% que opina lo mismo sobre la TV.

Fuente: 1. Nielsen Online; 2. EISA; 3. Mediascope

Redes Sociales

Formas de interacción social en las que se establece un intercambio dinámico entre personas, grupos e instituciones con el propósito de lograr:

- ✓ Comunicación: poner conocimientos en común
- ✓ Comunidad: Encontrar e integrar comunidades afines
- ✓ Cooperación: Hacer cosas juntos



Tuenti hoy

El mayor site web y móvil de España

Compañía tecnológica 100% española

260 empleados de 21 nacionalidades, 50% ingenieros

3 oficinas en Madrid y Barcelona

15% del tráfico web de España pasa por Tuenti cada día

Una de las principales compañías de Internet en Europa

La información personal de los usuarios no se indexa en ningún buscador. Sólo perfiles reales.

tuenti

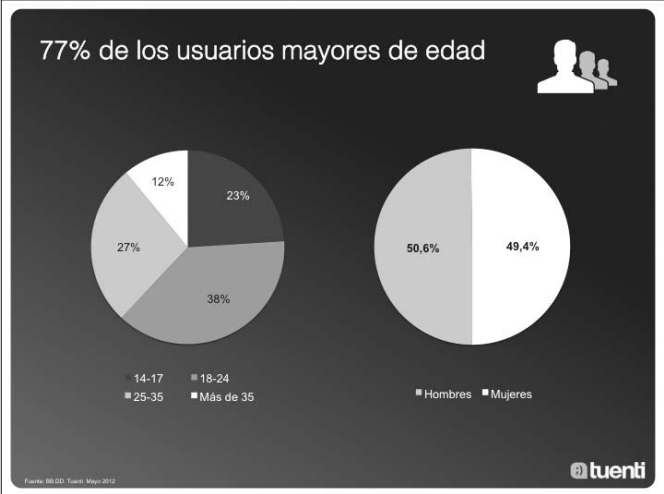
Plataforma social de comunicación

Modelo de acceso por invitación o teléfono móvil verificado.

La información personal de los usuarios no se indexa en ningún buscador.

Gente real, información real, relaciones reales.

tuenti



Sitio móvil y Apps

+40% de los usuarios de web acceden también vía móvil

5 MM usuarios mensuales

Más de un millón de fotos subidas por móvil al mes

Aplicaciones disponibles para iPhone, Java, Android y Blackberry

Más de 25.000 personas instalan la App de Tuenti en sus terminales cada día

m.tuenti.com

1,7 MM usuarios únicos mensuales

Más de 300 MM páginas vistas/mes

Más de 250.000 usuarios únicos día

Más de 3 MM de impresiones a lo largo del día (home y profile).





Fuente: BBDO, Tuenti, Mayo 2012

326


03

Redes sociales, privacidad y menores: El gran reto jurídico y educativo

El usuario es el protagonista

Los usuarios son los que aportan sus contenidos, suministran información, la comparten con otros. En definitiva, la creación y explotación de la información y los contenidos en Internet está ahora en manos de todos y cada uno de los ciudadanos, ya sea como autores y/o como usuarios de esa información y contenidos.





La importancia de los datos en la era digital

“Data is the new gold of the Digital Economy”

(Nellie Kroes, Vice-President of the European Commission responsible for the Digital Agenda. January 2012)



La importancia de los datos en la era digital

“The great threat in the digital age comes from companies that use our data to enrich themselves — buying and selling our most intimate details for their own corporate benefit”

(Viviane Reding, Vice-President of the European Commission. EU Justice Commissioner. January 2012)



¿Qué es la privacidad?

“Derecho a que te dejen en paz” (Louis Brandeis, Magistrado del TS de EEUU en 1890)

Derecho a decidir qué partes de nuestra esfera vital pueden ser accesibles para otros y controlar la extensión, la manera y el momento de usar esa información.



La Privacidad no es el problema sino la solución

Actualmente el mayor reto al que se enfrenta la privacidad es el del desarrollo tecnológico y el auge de las redes sociales.

Las redes sociales han cambiado en parte la realidad de las relaciones entre los responsables del tratamiento de los datos y los titulares de los mismos.



PROCESO DE REVISIÓN DE LA LEGISLACIÓN COMUNITARIA DE PROTECCIÓN DE DATOS

Pay for Privacy (Pagar por privacidad)

Información y datos personales = PIEZA CLAVE SOBRE LA QUE PIVOTAN LAS REDES SOCIALES Y PRINCIPAL FUENTE DE RIQUEZA



Mecanismos jurídico – informativos para garantizar la privacidad

POLÍTICAS DE PRIVACIDAD

- ☐ Lenguaje sencillo y comprensible
- ☐ Fácilmente accesible y visible
- ☐ Permite a los usuarios conocer efectivamente el uso de sus datos personales cuando utilizan cualquier servicio vinculado al uso de internet.
- ☐ El consentimiento debe ser siempre específico para la finalidad informada.




TRANSPARENCIA, SENCILLEZ Y CLARIDAD

Mecanismos técnicos para garantizar la privacidad

PANEL DE PRIVACIDAD

- ❑ Interfaz sencilla y fácil de manejar
- ❑ El usuario puede configurar el grado de privacidad con el que quiere relacionarse en la red social.
- ❑ El usuario puede controlar en todo momento la privacidad de su perfil y sus diferentes elementos: fotos, tablón, recepción de mensajes y/o la visibilidad de números de teléfono.



TRANSPARENCIA, CONTROL Y ELECCIÓN

Privacy by Design & Privacy by Default

La privacidad debe estar presente desde el principio en el desarrollo de cualquier servicio que vaya a tratar datos personales.

Incorporar desde el principio la privacidad en la tecnología.

Las configuraciones por defecto no deben permitir el acceso a la información a terceras personas.



329

Control de los datos personales (I)



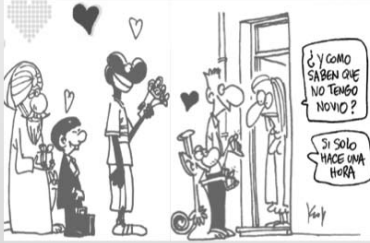
Toda la información presente en una red social debe ser propiedad del usuario y como tal, tiene derecho a controlar la recogida, uso y revelación de cualquier información sobre sí mismo.



Control de los datos personales (y II)

La base de la protección de datos en Europa es el **poder de disposición de los datos personales** (derecho a la autodeterminación informativa): Cada persona debe decidir y controlar quién, cuándo y por cuánto tiempo están disponibles sus datos en Internet.

Es decir, que los usuarios de las redes sociales no pierdan el control sobre la información que les concierne y que tengan a su alcance **medios** que les permitan garantizar dicho control.



tuenti

Confianza del usuario



"Data Security and Privacy concerns impacting what people buy, where they do business".

"Consumer loyalty depends on privacy and data security" (Edelman study, March 2012)

Necesidad de fomentar la confianza de los usuarios en Internet:

- Transparencia
- Garantía de la privacidad
- Seguridad de su información
- Consentimiento específico para el tratamiento concreto

tuenti

A modo de reflexión...

Para poder disfrutar de la libertad de Internet, debemos recordar y potenciar una actuación diligente de todas las partes intervinientes:



USUARIOS, pensando en qué información queremos compartir en la red



PRESTADORES DE SERVICIOS, informando y atendiendo el ejercicio de nuestros derechos en materia de protección de datos



MEDIOS DE COMUNICACIÓN, siendo conscientes de los límites de la libertad de expresión e información



BUSCADORES DE INTERNET, colaborando con las autoridades.

Todo ello en aras de no olvidarnos de aplicar la regulación en materia de protección de datos de forma responsable.



04

Sistemas de autorregulación de redes sociales: El caso de Tuenti

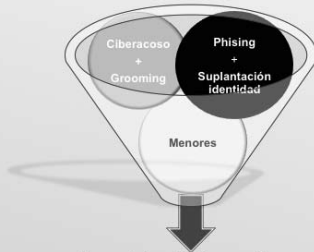
Sistemas de autorregulación

- ❑ La autorregulación surge con la idea de dar respuesta a la necesidad de **regular los contenidos y servicios de Internet**, mediante procedimientos para detectar y retirar contenidos ilícitos, proteger a los menores y garantizar su privacidad, sin, por supuesto, suplir a la legislación vigente, sino complementándola.
- ❑ **Desarrollo de sistemas y modelos de autorregulación** en este nuevo entorno que garanticen la protección de los derechos de las personas sin obstaculizar el desarrollo de las nuevas tecnologías.
- ❑ En Tuenti estamos convencidos de un **modelo basado en la autorregulación** donde los usuarios son quienes gestionan y detectan cualquier contenido inapropiado, perfil sospechoso o falso, suplantación de identidad o cualquier otro material o conducta ilegal y son ellos mismos quienes los denuncian a través de los **mecanismos y herramientas de reporte que TUENTI les facilita**.

Soporte al usuario

❑ En Tuenti ofrecemos a nuestro **equipo de Soporte al Usuario** una formación permanente en materia jurídica y sobre protección de datos de carácter personal de forma que estén preparados para contestar cualquier cuestión a la mayor brevedad y con la máxima precisión.

Protocolo de seguridad para combatir los delitos más comunes



privacidad@tuenti.com



Herramientas de protección

❑ TUENTI facilita mecanismos muy sencillos de utilizar para denunciar aquellas conductas o contenidos que vulneran la Ley y/o nuestras Condiciones de uso. El sistema de reporte de TUENTI es extremadamente sencillo y permite a los usuarios denunciar perfiles o contenidos ilícitos a TUENTI con sólo 4 clicks.

❑ En Tuenti es posible denunciar al equipo de Soporte:

- 1) Perfiles
- 2) Fotos
- 3) Cualquier otro asunto de consulta a través de nuestra sección de ayuda o escribiendo a privacidad@tuenti.com



1) Denuncia de perfiles

Paso 1: A través del perfil de un usuario pulsar el botón "Denunciar usuario", en la parte inferior de la página.



Paso 3: Emerge una nueva ventana con las distintas categorías en las que es posible realizar una denuncia (insultos, amenazas, suplantación, perfil falso, contenido ilegal, ofensivo, etc.).



Paso 2: Emerge una ventana nueva en la que se dan unas indicaciones sobre las denuncias y se aceptan las condiciones de uso para certificar la denuncia como verdadera.



Paso 4: Seleccionar la categoría correspondiente y escribir al menos 50 caracteres que justifiquen y expliquen tu denuncia (para evitar denuncias falsas).



LA AUTORREGULACIÓN COMO SISTEMA DE PROTECCIÓN DE LA SEGURIDAD EN LAS REDES SOCIALES: EL CASO DE TUENTI

2) Denuncia de fotos

Paso 1: Abrir la foto que queremos denunciar y pinchar sobre la rueda de Opciones, a la derecha de la imagen, y elegir la opción "Denunciar".



Paso 3: Emerge una nueva ventana con las distintas categorías en las que es posible realizar una denuncia sobre una fotografía (imágenes violentas, ofensivas, pornografía).



Paso 2: Al igual que con los perfiles, emerge una ventana nueva en la que se dan unas indicaciones sobre las denuncias. Se deben de aceptar las Condiciones de uso para que la denuncia se pueda procesar.



Paso 4: Escoger la categoría correspondiente y justificar la denuncia con más información en el cuadro de texto (sin límite mínimo de caracteres).



Centro de Ayuda y Seguridad



333

Compromisos suscritos





05

Sistemas de autorregulación en la Unión Europea

PRINCIPIOS DE LA UE PARA UNAS REDES SOCIALES MÁS SEGURAS
(Febrero 2009)

A grid of logos for various social media and technology companies, including Arto, Bebo, Dailymotion, Facebook, MySpace, Google, Hyves, Microsoft, One, Nasza Klasa, Netlog, Skyrock.com, Sula, Yahoo!, Zap, Rate.ee, Tuenti, Stardoll, and others. The Tuenti logo is visible in the bottom right corner.

PRINCIPIOS DE LA UE PARA UNAS REDES SOCIALES MÁS SEGURAS
(Febrero 2009)

- 1º) **Suscitar la sensibilización** sobre los mensajes orientados a la formación en materia de seguridad y las políticas de usos admitidos en usuarios, padres, docentes y otros responsables de la tutela de menores de manera que figuren de forma destacada, clara y adaptada a la edad del destinatario.
- 2º) Procurar garantizar que los **servicios ofrecidos son adecuados a la edad** del usuario a quien se dirigen.
- 3º) Capacitar a los usuarios mediante **herramientas y aplicaciones tecnológicas**.
- 4º) Facilitar **procedimientos de utilización sencilla para informar sobre conductas o contenidos** que supongan una vulneración de las condiciones de servicio.
- 5º) **Responder a las notificaciones** relativas a conductas o contenidos ilícitos
- 6º) Dotar de recursos y promover que los usuarios utilicen **procedimientos seguros en el tratamiento de la información personal y la privacidad**.
- 7º) Evaluar los **medios disponibles para la investigación de conductas o contenidos ilícitos o prohibidos**.



COALITION TO MAKE INTERNET A BETTER PLACE FOR KIDS
(Diciembre 2011)

❑ **Signatory companies:** Apple, BSKyB, BT, Dailymotion, Deutsche Telekom, Facebook, France Telecom - Orange, Google, Hyves, KPN, Liberty Global, LG Electronics, Mediaset, Microsoft, Netlog, Nintendo, Nokia, Opera Software, Research In Motion, RTL Group, Samsung, Skyrock, Stardoll, Sulake, **Telefonica**, TeliaSonera, Telecom Italia, Telenor Group, **Tuenti**, Vivendi and Vodafone.

❑ **Objetivos y acciones:**

- ✓ Facilitar mecanismos sencillos de reporte de denuncias.
- ✓ Implementar configuraciones de privacidad adecuados a la edad del usuario.
- ✓ Usar la Clasificación de Contenidos.
- ✓ Ofrecer herramientas de control parental.
- ✓ Mejorar los procedimientos de eliminado de contenidos de abusos a menores.





CLAUSURA

JOSÉ CABANILLAS SÁNCHEZ
Director General de la Fundación Policía Española
y Director del curso

En este Curso se ha repasado, durante los últimos cuatro días, uno de los problemas más característicos de los últimos tiempos, que va a marcar probablemente toda una época, es la aparición de la era digital y, dentro de ella, el advenimiento de las redes sociales. Este tema ha sido revisado desde el punto de vista del impacto social que representan los aspectos jurídicos. Se ha señalado que es necesaria su implantación dentro de las Administraciones Públicas. Se han analizado las dificultades que representa en procesos como los de la globalización, en sus ámbito legal, de cara al terreno técnico que suponen el fenómeno de las redes sociales y la interrelación entre las personas, la convivencia en el ámbito del ciberespacio, que no tiene fronteras y que, por lo tanto, choca con los conceptos clásicos de la territorialidad de las leyes y de los procesos penales y, en este sentido, cómo desde Europa, determinadas instituciones están intentando avanzar en ello. Y también se ha analizado como la Policía está trabajando ante este problema.

339

Alfonso San Román Ibarrondo, Fiscal Delegado de Criminalidad Informática de la Fiscalía de Madrid, me ha indicado que en este fenómeno la Policía tiene que ser, como en anteriores ocasiones, la punta de lanza, porque detrás irán el resto de instituciones de corte penal. Es necesario porque, probablemente, y no sé si se cumplirá lo que Ulrich Beck dijo en su momento en relación con la sociedad del riesgo, que el comportamiento de las personas en esta nueva época, una vez desaparecida la época industrial, que sería el postmodernismo o la segunda modernidad, va a estar centrado, fundamentalmente, en el individualismo y en la globalización, en contra de lo que era el hombre-masa en el período anterior.

El individuo que participa en las redes sociales ha sido definido como el que se encuentra constantemente como desgranando maíz, y que está exclusivamente en ese mundo de individualidad incluso cuando tiene a pocos

metros a aquel con el que se está comunicando, exclusivamente a través de esas redes sociales. Esta actitud podría llevarnos, quizás, al problema de que los seres humanos pudiéramos perder la capacidad del habla, si únicamente nos comunicamos “cliqueando”. Otros plantean de las redes sociales puedan ser cambiadas por Whatsapp u otros medios. Todo ello es cuestión de futuro, y la Policía tiene que estar ahí porque es una realidad y la misión del Cuerpo es, básicamente, la de cumplir con los ciudadanos.

También se ha explicado como, desde la Dirección General de la Policía, a través de los representantes de relaciones sociales, están trabajando en estas redes sociales, con lo cual ya se va avanzando y que, en cierto modo, son pioneros en este ámbito dentro de las Administraciones españolas.

Se ha expuesto los problemas que existen y la necesidad de participar en ellos y, sobre todo, la inmensa mayoría considera que la ventaja de este Curso es que no solamente se oye a los ponentes sino que, posteriormente, se plantean cuestiones, se establecen diálogos, se transmiten sensaciones y opiniones. En este caso, las noticias cuentan que ha sido muy enriquecedor y muy importante.

MERCEDES MOLINA IBÁÑEZ
Vicerrectora de Transferencia de la Universidad
Complutense de Madrid.
Directora General de la Fundación General de
la Universidad Complutense de Madrid

Quisiera agradecer de una manera muy sincera y, a la vez, muy institucional, la presencia del Cuerpo Nacional de Policía en los Cursos de Verano de la Universidad Complutense de Madrid.

La Universidad, partiendo de una gran vocación de sus miembros, de quienes la integramos, y pidiéndonos las responsabilidades que, como a todos, nos deben demandar, sobre todo, quien nos financia y a quienes debemos hacer el servicio, lógicamente ha de pensar que el papel que está haciendo es verdaderamente importante para la sociedad de hoy y la de mañana. Ya decía Cicerón en alguna de sus obras que el mejor y mayor servicio que podemos prestar al Estado es educar a la juventud. Ahora habría que decir que educar a todas las edades por ese proceso de formación a lo largo de toda la vida, exige los vertiginosos cambios a los que todos estamos precisamente sometidos.

341

En la Universidad seguimos trabajando por aquellas funciones que dentro de nuestra universidad son esenciales, y estos Cursos de Verano forman parte del tercer pilar de la Universidad: la transferencia del conocimiento, pero que está muy unido a los otros dos: la investigación y la docencia. Laín Entralgo decía en alguna conferencia o entrevista que le hicieron que la universidad para dar de sí tiene que ser en sí. Si no tiene algo que decir, si no tiene algo que transmitir, y no lo valora la sociedad, difícilmente se podría proyectar.

Hemos interpretado siempre este foro de Cursos de Verano como un espacio de reflexión. Es un ámbito del conocimiento, porque es aquí donde, precisamente, se toma el conocimiento en muy diferentes campos y facetas: desde la investigación en una química básica a una acción con repercusión

clave en la sociedad como es la actividad del Cuerpo Nacional de Policía, detrás de las cuales hay también una investigación, un saber, unos problemas que descubrir, unas soluciones que plantear, igual que hacemos los científicos, en muy diferentes campos. Y ustedes van avanzando precisamente en función de los interrogantes y en función de los logros que a partir de esas preguntas van haciendo.

Yo he estudiado la globalización desde otros procesos porque soy geógrafa, y precisamente, cuando decían que el territorio se iba a desdibujar yo veo que el territorio tiene, cada vez, más peso, y que lo global es cada vez más individual. Hay globalización en la difusión de la información pero, ¿quién genera esa información?, ¿quién la procesa?, ¿quién la asume?, y ¿quién la transforma? Hablamos de globalización, pero no todo el mundo es controlado por todos a nivel internacional. Departimos de globalización de derechos y valores, y aquí vivimos en un paraíso de derechos frente a territorios mundiales que carecen de los más elementales. Es decir, hablamos de que la Red iba a desdibujar las fronteras pero hoy predicamos del territorio del capital, del de la innovación y de la investigación, del de la mano de obra o del consumo. Y ya en algunas prendas no se dice “Hecho en” sino “Diseñado en”.

342

También dentro de la globalización, las nuevas tecnologías, que han generado por una parte una gran vinculación social, decaen o hacen caer al individuo en el individualismo.

Esos fenómenos que están apareciendo en Japón, del joven que se aísla, que solo se comunica a través de la Red, que están creando verdaderos problemas en las familias, la sociedad, de convivencia, incluso de comportamientos suicidas, que se van extendiendo individualmente pero que se hacen colectivos en un territorio que siempre ha tenido, pese a esa idea de colectividad, una presencia del individualismo grande.

En la Universidad se dice siempre que las ideas tienen que estar por encima de las ideologías. Cuando hay algo que verdaderamente tiene interés se debe mantener, pero también hay que cambiar y adaptarse a aquellas innovaciones que le exigen estar a la altura de lo que la sociedad le exige, igual que la Policía está al servicio de la sociedad. Que estas palabras sirvan de reconocimiento público, no ya como Vicerrectora, sino como una simple ciudadana que está muy contenta de tenerlos aquí. Mi gratitud como ciudadana a la labor que realizan y a su esfuerzo constante porque la seguridad, que también es una forma de garantía de derechos, la tengamos avalada y, lógicamente, presente en nuestro camino.

La Universidad Complutense puede y debe colaborar con el Cuerpo Nacional de Policía, y le tiendo la mano para tener una sesión de trabajo, porque hay grupos de investigación en el campus que están trabajando también en temas de seguridad vinculados, precisamente, a actuaciones territoriales y también en relación con la Red.

Hay dos cosas que se han dicho en este curso que se deben destacar: la información para corregir y para prevenir. No solo hay que perseguir el delito, que además en algunas acciones de la Red es terrible, y con grupos sociales tremendamente vulnerables, como son los niños, sino que también hay que informar a las familias, a los padres, a los centros.

En los foros como este Curso, aparte de la multidisciplinariedad, también se genera la multiactividad de muy distintos campos de trabajo, que pueden aportar y recoger ideas en sus diferentes trabajos, y el sistema educativo tiene que recibir información y formación en todos estos espacios.

Quiero expresarles, en nombre del Rector y en el mío propio, mi gratitud más sincera por contar con nosotros, a la Fundación por supuesto, a otros patrocinadores y a nuestro sponsor general, que es el Banco de Santander. Gracias a ellos podemos ejercer estas funciones tan importantes de transferencia, que sino nuestra Universidad pública no podría realizar. Pero también ellos confían en nosotros porque respondemos. Volviendo a las palabras de Laín, damos en sí porque somos en sí, y eso nos lo reconocen.

IGNACIO COSIDÓ GUTIÉRREZ
Director General de la Policía

Sra. Vicerrectora de la Universidad Complutense de Madrid, Director de Logística del Cuerpo Nacional de Policía, Director del Curso y Director también del Instituto de Estudios de la Policía, Comisario Cabanillas, alumnos, al ver el programa de este curso pensé que me apetecía más venir como alumno que como clausurante, porque realmente es un curso atractivo, de enorme nivel y con unos temas que me despiertan mucha curiosidad e interés. En todo caso, el papel que me toca es el de clausurarlo y lo voy a hacer con brevedad. Después de las intervenciones, ponencias y conferencias que aquí se han impartido poco voy a poder aportar, pero es un honor, personalmente como Director de la Policía, pero también para el conjunto del Cuerpo Nacional de Policía, estar en estos Cursos de Verano de la Universidad Complutense. Una Universidad que es un claro referente en España de los cursos de verano, que abre un espacio para la reflexión, el diálogo y el debate con el sosiego que da el estío y el no tener los exámenes ni las obligaciones propias de un curso académico, lo que es especialmente de agradecer.

345

De los 25 años de historia de estos Cursos de Verano el Cuerpo Nacional de Policía ha estado presente en 14. Es un verdadero honor y privilegio estar hoy aquí. Y si hemos podido participar es gracias a unos patrocinios que tengo obligación de reconocer públicamente. Más allá del patrocinio general del Banco Santander, en nuestro caso es Telefónica la que cada año, también éste, nos permite organizar este curso. Y deseo agradecerlo de forma especial porque en estos momentos de crisis económica no es fácil encontrar a alguien que esté dispuesto a respaldar este tipo de iniciativas.

Quiero extender mi reconocimiento a la Fundación Policía Española, que siempre nos da apoyo en todas las actividades, muy especialmente en las de formación, que lleva a cabo el Cuerpo Nacional de Policía. Y dentro

de la Fundación, creo que lo ha dicho ya la Vicerrectora pero me sumo con todo entusiasmo a esa felicitación, al Comisario José Cabanillas, quien me consta ha trabajado con enorme entusiasmo, dedicación y, a la vista de los resultados, eficacia, para la buena finalización de este curso.

Particular gratitud quiero mostrar a los alumnos que habéis asistido al curso. En ocasiones observamos cómo a magníficos programas, con ponentes de muchísima altura, les falla lo más importante: tener un buen número de alumnos y, además, alumnos de calidad y realmente interesados. Creo que éste ha sido uno de los cursos con más matrículas y, por lo que me han comentado los ponentes, ha habido interés, participación, coloquio, debate, que es lo que le da interés y calidad a una formación de esta naturaleza. Muchas gracias por haber participado, a los que sois miembros del Cuerpo Nacional de Policía porque en vuestra carrera (veo a varios Comisarios Principales aquí sentados) nunca se deja de aprender y siempre hay un gran interés por la formación como una manera de servir mejor a la sociedad, a los ciudadanos y a la Policía. Y a los que habéis venido de fuera, por haber querido participar en un curso organizado por el Cuerpo Nacional de Policía.

346 Voy a ser breve, pero dejadme decir dos o tres cosas. En primer lugar, si hay algún proyecto que a mí me gustaría que definiera la política de la Dirección General de los próximos años, al menos, en los que yo tenga la responsabilidad de dirigir esta institución, es el de una Policía inteligente. En España siempre hemos dicho: “la Policía no es tonta”. La Policía es inteligente, así ha sido históricamente, la inteligencia ha sido consustancial a la labor de investigación policial. Cuando hablo de la Policía inteligente (el inglés creo que refleja mejor este concepto: Smart Police) estamos hablando de cómo integrar todo el potencial de cambio tecnológico tan acelerado que ha vivido la sociedad en los últimos años a la función policial. Hablamos de una Policía 3.0, que es el nombre comercial que hemos dado a este proyecto. Queremos que la labor de información que hace la Policía, la investigación criminal, la seguridad ciudadana sean inteligentes, que utilicemos mejor el potencial que todas estas tecnologías, todo el mundo cibernético o de Internet, nos permiten para prestar un mejor servicio a los ciudadanos, que es de lo que se trata.

Cuando uno asume la responsabilidad de dirigir el Cuerpo Nacional de Policía siente una cierta frustración. La Policía funciona y funciona bien, tenemos una buena Policía, todos los días hay buenos servicios. Por eso hay que huir de una tentación que tenemos los políticos: querer descubrir todas las mañanas el Mediterráneo, y cambiar cosas que funcionan y no tenemos ninguna necesidad de modificar. Sobre la base de esa Policía eficaz, muy bien valorada por los ciudadanos y con un enorme prestigio internacional,

tenemos que tener una voluntad de transformación, de hacer mejor las cosas porque lo más peligroso para una organización es morir de éxito, creer que porque las cosas funcionan van a seguir funcionando siempre. El mayor peligro es quedarse quietos en un entorno social, económico, tecnológico, internacional, tan cambiante y dinámico. Precisamente el éxito del Cuerpo Nacional de Policía se debe a que siempre ha tenido una voluntad de adaptación a las nuevas realidades sociales y delictivas o criminales a las que tiene que enfrentarse. Por eso el proyecto de Policía 3.0 es un plan de transformación sobre el reconocimiento de que tenemos una gran Policía.

La Policía sufre también la crisis económica. Tengo a mi derecha al Subdirector General de Logística, que es el que maneja los presupuestos y, por tanto, el que más consciencia tiene de cómo nos están afectando las restricciones presupuestarias. Esta crisis, más que un inconveniente o un freno, debe ser un motor, un incentivo para el proceso de transformación que queremos poner en marcha, porque a más inteligencia, más eficiencia en el uso de los recursos, que siempre son escasos. No se trata solo de tener muchas patrullas de policía en la calle, sino de que estén en el momento adecuado, en el lugar oportuno y con la capacidad de actuación necesaria para prestar el servicio a los ciudadanos. Y eso, básicamente, pasa por una planificación y por la utilización de la tecnología y de la inteligencia en la planificación de los servicios de seguridad ciudadana. Por tanto, diría que incluso el contexto de crisis que estamos viviendo nos obliga a poner en marcha este proyecto de Policía Inteligente o de Policía 3.0.

347

Y dentro de este proyecto, es fundamental el papel de las redes sociales, que es transformador del mundo virtual, cibernético. Estamos en una evolución de ese mundo y las reflexiones, ponencias y debates que habéis tenido aquí nos van a ser de mucha utilidad para orientar este proyecto, cuyo liderazgo corresponde a Luis de Eusebio, que ha participado como alumno del curso y que ha tomado muy buena nota de todo lo que se ha dicho.

Me gustaría hablar de las redes sociales como un elemento claramente positivo, un factor de un enorme potencial social, económico, diría incluso que político. En algunos procesos las redes sociales han jugado un papel determinante, Eduardo Baeza nos habló de la campaña Obama y de cómo las redes están transformando también la acción política.

Las redes sociales también entrañan riesgos, muy especialmente para sectores vulnerables de la sociedad, específicamente la infancia. El profesor Antonio Troncoso hizo una buena disección de cuáles son esos riesgos, en general para todos los ciudadanos, en su derecho a la intimidad, en la protección de su honor, etc., pero muy particularmente para los niños, para la

infancia. Sin embargo, debemos huir de la criminalización de las redes sociales, suponen inseguridades como también entraña riesgo el coger un coche y hacer un viaje. Prestan un gran servicio, entrañan un riesgo. Lo importante es tener consciencia de éstos y tomar las medidas de precaución necesarias para minimizarlos. En la Policía estamos muy pendientes de los peligros.

Las redes sociales son también un enorme potencial para la Policía, para las Administraciones Públicas en general, a efectos de prestar un mejor servicio a la sociedad, a los ciudadanos, que es de lo que se trata. Juanjo Esteban participó en el programa, y dio una buena visión de cómo desde el Cuerpo Nacional de Policía estamos utilizando estas redes sociales para ofrecer una mejor asistencia a los ciudadanos.

Yo puedo decir con mucha satisfacción que el Cuerpo Nacional de Policía hoy ocupa una posición de liderazgo, tanto en la lucha contra la ciberdelincuencia como en la presencia y utilización de las redes sociales para realizar mejor nuestra función policial. En el primer campo somos punteros. Tenemos a varios expertos del Cuerpo Nacional de Policía trabajando ahora mismo en la creación del Centro del Cibercrimen de Europol. Nuestra Brigada de Delincuencia Tecnológica cuenta con pocos recursos pero es una de las unidades más eficientes del Cuerpo, y hace frente a una amenaza considerada por Europa y por todos los países del mundo occidental como uno de los principales desafíos de seguridad a afrontar.

Hace poco, en una conferencia de directores de policía europeos, nos daban unas cifras muy significativas. El incremento en el número de delitos en Internet en el año 2011 había sido de casi un 70 por ciento, no hay ningún otro ámbito de la actividad donde la delincuencia esté creciendo tan rápidamente. Estamos hablando de 400 millones de víctimas y de un coste de 300.000 millones de dólares como consecuencia de toda esta delincuencia tecnológica.

Por tanto, es uno de los grandes desafíos que tenemos que afrontar, y estamos haciendo un gran trabajo. He traído también solamente dos cifras, no quiero aburrir. En el año 2011, la Brigada de Delincuencia Tecnológica (insisto, con muy pocos efectivos) ha llevado a cabo casi 800 investigaciones y ha detenido a casi 700 personas por delitos de estafas, de pornografía infantil, de amenazas, de injurias, etc. muchos tipos delictivos. Necesitamos potenciar nuestras necesidades de investigación en este ámbito porque la delincuencia crece más rápido que nuestra capacidad para hacerle frente.

Muy recientemente celebramos otra formación estival, en este caso con una parte de la industria tecnológica de nuestro país, y el representante del

Federal Bureau of Investigation (FBI) llegaba a la misma conclusión. Es decir, tanto el FBI como el Cuerpo Nacional de Policía en estos momentos están en un proyecto de duplicar sus capacidades para hacer frente a este tipo de delincuencia, que insisto, es uno de los grandes riesgos que afronta la sociedad del futuro.

Les hablaba de una segunda dimensión: la utilización de las redes sociales para mejorar el servicio que prestamos a las personas. También tenemos un claro liderazgo en este campo, Juanjo Esteban les dio todos los datos. La cifra crece día a día, pero ahora mismo tenemos 220.000 seguidores en Twitter. El día que superamos a la Moncloa me preocupé por no morir de éxito. Somos la institución pública en España con mayor número de seguidores, con diferencia. Y, aunque no tenemos todavía creada la figura del “social media manager”, contamos con un gran equipo, que es el principal responsable de este éxito vertiginoso, pues en lo que llevamos de año 2012 se ha triplicado el número de *followers*. En pocas ocasiones tiene uno la satisfacción de obtener una respuesta de los ciudadanos tan positiva. Ya digo, es uno de los resultados de los que estoy más orgulloso en los seis meses que llevo como Director. Lo digo con sinceridad, y el mérito no es mío, sino de ese equipo que gestiona diariamente y presta este servicio a los ciudadanos.

349

Si lo miramos en un contexto internacional, somos la segunda Policía del mundo, después del Federal Bureau of Investigation (FBI) en número de seguidores. La distancia hace que nos vaya a costar alcanzar el liderazgo mundial, pero somos los segundos. Y somos también la Policía de la Unión Europea con mayor número de seguidores y, por tanto, con mayor presencia en las redes sociales. Eso también es un orgullo, no solamente para el Cuerpo Nacional de Policía, sino también para toda España.

Interesa destacarlo: no es solo marketing. La presencia en redes sociales no trata únicamente de transmitir una idea de modernidad o de estar en el mundo tecnológico. Tiene dos utilidades que son muy, muy importantes. La primera es tener un canal abierto de información a los ciudadanos de un potencial extraordinario. No tenemos dinero en estos momentos, lamentablemente, para poner una página en *El País*, *ABC* o en cualquier otro periódico de tirada nacional, pero el impacto que logramos con campañas a través de nuestras redes sociales es muchísimo mayor que el conseguido a veces con medios tradicionales. Ya me gustaría que complementáramos, porque también es verdad que hay todo un público al que no llegamos sino es a través de esos medios tradicionales. Lo que quiero destacar es que tenemos un potencial enorme en las redes sociales para comunicarnos con la gente, para informar al ciudadano, para que por ejemplo, las persona tome conciencia de cuáles son los riesgos que tiene cuando está utilizando un *Smartphone*.

No podríamos vivir ya sin ellos, cuando estamos más de cinco minutos sin recibir un mensaje o una llamada empezamos a preocuparnos, pero también hay vulnerabilidades y tenemos que ser conscientes de ellas.

La segunda ventaja es que es una comunicación bidireccional, es decir, que no se trata solamente de que nosotros podamos comunicarnos con el ciudadano, sino estamos contestando del orden de 300 mensajes diarios que a través de redes sociales nos envían pidiéndonos información o algún tipo de dato. Por tanto, es una comunicación mucho más potente que la que antes éramos capaces de mantener.

350 Pero ni siquiera es solo una utilidad en términos de información, que ya es muy importante y muy potente, es una utilidad en términos operativos. A través de redes sociales, se lo explicaría Juanjo Esteban, pusimos en marcha campañas como la Tweetredada, en la que se recibieron 3.000 informaciones relevantes para las investigaciones en la lucha contra la droga. Nuevamente se puso de manifiesto el enorme potencial de las redes sociales para articular algo tan vital para la Policía como la colaboración ciudadana, que ante una sociedad cada vez más compleja y con más riesgos es un eje esencial de nuestra política. Es decir, o conseguimos implicar más a la gente en su propia seguridad o será muy difícil que podamos dar una respuesta adecuada a los desafíos de seguridad que tenemos planteados para el futuro. Y estas redes son un instrumento maravilloso para poder articular, de una forma muy accesible para el ciudadano y al mismo tiempo muy económica para nosotros, todo ese potencial de ayuda social. Después del éxito de la Tweetredada en la lucha contra la droga, estamos pensando en otra para algo que también preocupa mucho y daña enormemente la convivencia: el vandalismo, un fenómeno tremendamente complicado, al que con la asistencia de la gente vamos a poder dar una respuesta más eficaz.

El curso, por las ideas, por la calidad de las ponencias e intervenciones que se han producido, nos ha enriquecido mucho y nos va a ayudar a perfilar todo este proyecto de policía inteligente, de Policía 3.0 que queremos impulsar desde la Dirección General de la Policía. Así que, mi agradecimiento a la Universidad y a todos ustedes por habernos ayudado a ser un poco mejores, que es el objetivo con el que nos levantamos todos cada mañana.

