ÍNDICE

I

Contexto sociológico de ciberacoso o daños más frecuentes para los menores en la red

La labor de campo hecha por ciertos organismos fiables[1] sobre la seguridad jurídica de las redes sociales evidencia que el menor, efectivamente, es en lo virtual víctima propiciatoria para las variopintas modalidades de acoso.

Primero, porque son los internautas más numerosos en las redes. Aunque en El Estudio(*) no hay cifras exactas relativas a la circulación en red de los llamados «menores maduros» (en España aquellos comprendidos entre los 15 y los 18 años, creo, por coherencia con el sistema de protección de menores prohibiendo el uso de redes sociales a los menores de 14 años), sí hay datos de nuestro país del año 2008 que muestran que los internautas situados en una horquilla de edad comprendida entre los 15 y los 34 años son los más numerosos y son los que han configurado su perfil en una red social. Si tenemos en cuenta que el 36,5% del 70% de usuarios españoles de redes en Internet son usuarios cuya edad se mueve de los 15 a los 24, se comprenderá fácilmente la necesidad de fijar la atención en ellos[2]. Del último Informe abreviado relativo al Eurobarómetro (Flash Eurobarometer n.º 428 –Safe Internet for children[3]) de la Unión Europea, de diciembre de 2008, proviene el resultado de que el 75% de los menores comprendidos entre los 6 y 17 años utilizan habitualmente Internet y que el 50% con

---

[1] El examen científico-jurídico de la seguridad de las redes sociales pasa por encontrar buenas estadísticas. A día de hoy son fiables los numerosos datos manejados en diversos documentos (Informes, y Estudios), realizados por diversos organismos europeos y españoles. Merecen atención, los que han sido creados a iniciativa europea como la Agencia Europea de Seguridad de las Redes y de la Información (ENISA, Reglamento (EC) No 460/2004 del Parlamento europeo y del Consejo de 10 de marzo de 2004, DOCE L 077, 13/03/2004 P. 0001-0011), que elaboró en octubre 2007 el documento *Problemas de seguridad y recomendaciones para las Redes sociales en línea*, dirigido a los reguladores y proveedores de Redes sociales, (www.enisa.europa.es) y los distintos Eurobarómetros o informes cuantitativos y cualitativos que han ido apareciendo desde el año 2003 a impulso del Programa europeo «Safer Internet» (Internet más segura), éstos más atentos a la concienciación de los padres respecto de los potenciales peligros de sus hijos en el manejo de Internet y de la telefonía móvil. Entre los españoles, destacaría dos estudios: (*) *El Estudio sobre la privacidad de los datos personales y la seguridad de la información en las Redes sociales online y El Estudio sobre hábitos seguros en el uso de las TIC por niños y adolescentes y e-confianza de sus padres* (en adelante, El Estudio 1 y El Estudio 2), elaborado en bilateral tanto por el Instituto Nacional de Tecnologías de la Comunicación (INTECO; www.inteco.es), como por la Agencia Española de Protección de datos (AEPD; www.agpd), en febrero y marzo 2009, la cual a su vez nos va dando año a año otros datos en las Memorias que realiza sobre sus actividades. Con todo, cada documento hace mención de sus propias fuentes estadísticas; así, el Estudio 1 menciona, a nivel mundial, la «*3ª Oleada del Estudio Power to the people social media*», Wave 3 de Universal MacCann, marzo de 2008 y a nivel nacional, la Zed Digital (autora de *El fenómeno de las redes sociales. Percepción, usos y publicidad*, noviembre 2008), Cocktail Analysis (con su documento intitulado «*Herramientas de comunicación on-line: Las redes sociales*», noviembre 2008), el Instituto Nacional de Estadística (que elaboró en octubre de 2008 el llamado «*Encuesta sobre Equipamiento y Uso de tecnologías de la Información y Comunicación en los hogares*»), Office of Communications (Ofcom) (con su «Estudio sobre redes sociales: Análisis cuantitativo y cualitativo sobre los hábitos, usos y actuaciones», de 2 de abril de 2008). Sus datos los desarrolla en las págs. 27 a 30. A su vez, la Memoria de la AEPD 2009 utiliza en gran parte los datos estadísticos del Centro de Investigaciones Sociológicas (CIS).

[2] Piénsese que según estos documentos, el número estimativo de usuarios de redes sociales en el mundo alcanza ya más de la mitad de los usuarios de Internet, concretamente el 58%.

[3] Vid. *Towards a safer use of internet for children in EU- a parents' perspective*, pág. 5.

tan solo 10 años tienen un teléfono móvil, por lo que el futuro será que este colectivo aumente y no disminuya su uso[4].

Segundo, porque dichos menores son los usuarios más numerosos de las redes sociales llamadas «de ocio o generalistas»[5], en las que se ha comprobado existe el mayor nivel de riesgo de códigos maliciosos[6]. Se dirá, no sin razón, «niños, adolescentes y jóvenes son la generación del ocio digital[7]».

Tercero, porque el uso más habitual que dichos menores realizan en las redes, como subir y compartir fotos personales, comentar fotos de otros y en general, cotillear[8], son actos que pueden conducirles a verdaderas situaciones de riesgo en su privacidad, pese a que ellos se creen, según el Estudio *pan-European qualitative* «*Safer Internet for children- a children's perspectives* (2007[9])», que son capaces de controlarlas.

A las acciones que pueden entrañar riesgo para el menor en el manejo de sus redes sociales hay que añadir aquellas que son comunes a cualquier usuario que circula en la red y que han sido analizadas por el *Estudio sobre la Privacidad de los datos personales y la seguridad de la información en las redes sociales online* de 2009 (en adelante, El Estudio), realizado por el Instituto Nacional de Tecnologías de la Comunicación (INTECO), y la Agencia Española de Protección de datos (AEPD), el cual expone los peligros comunes a cualquier usuario considerando tres momentos críticos en la circulación: el del registro del usuario, el del uso habitual de la plataforma y el momento de causar baja en el servicio. En coherencia, el Observatorio de la Seguridad de la Información de INTECO, como parte de un proyecto conjunto con la Universidad Politécnica de Madrid (UPM), lleva publicadas 12 guías[10] para servir de ayuda a los usuarios a la hora de configurar la privacidad y mantener la seguridad de sus perfiles en las principales redes sociales, en las que entra en el análisis de la identificación de los riesgos para la seguridad y privacidad en dichas plataformas abiertas, estructurándolas conforme a los tres momentos clave mencionados.

En cada uno de esos momentos los peligros pueden tener su origen en la propia diligencia del usuario, o en la propia plataforma que utiliza, o en ambos factores a la vez.

Es común a cualquier usuario (menor o mayor), en el momento de su registro en la red en la que desea circular, el peligro que supone una configuración desmesurada de su perfil. Ello es debido fundamentalmente a que normalmente las plataformas se configuran

---

[4] Dato que prácticamente coincide con el último arrojado por la reciente Comunicación de la Comisión Europea denominada *European Estrategy for a Better Internet for Children*, de 2 de mayo de 2012 [COM (2012) 196 final, punto 1.1].

[5] Según el Estudio, el número de usuarios españoles con perfil en alguna Red alcanza el 44,6%; es decir, el 7/10 son internautas menores de 35 años y en estas proporciones: de 15-24 años el 36,5%; de 25-34 años el 32,5%. De entre los usuarios menores comprendidos entre los 14 a 20 años, el 33% tiene perfil en Facebook; el 31% prefiere Tuenti y el 21% Myspace y Hi5.

[6] En comparación, parece que el mayor riesgo en redes profesionales son los coleccionistas de datos.

[7] Luengo, *Glosario*, *En busca del éxito educativo: realidades y soluciones*, Fundación Antena 3, Madrid, 2010, pág. 124.

[8] La proporción a día de hoy en el uso de las redes por los menores es esta: 70,9% de los menores ocupan su tiempo en compartir o subir fotos; comentarlas con los amigos se hace en un tanto por ciento menor: el 55,0%; cotillear es otra de las actividades que no se queda atrás pues se aprecia en un 46,2%.

[9] Cubre dicho Estudio 29 países y se encuestaron a menores de entre 9-10 y 12-14 años sobre el manejo de Internet y de teléfonos móviles.

[10] Son estas las guías: Guía inteco-facebook, Guía inteco-flickr, Guía inteco-hi5, Guía inteco-last.fm, Guía inteco-linkedin, Guía inteco-myspace, Guía inteco-orkut, Guía inteco-tuenti, Guía inteco-twitter, Guía inteco-windows live spaces, guía inteco-xing, Guía inteco-youtube.

por defecto para dar un máximo de publicidad. Así, si el usuario no puede construir adecuadamente su perfil, bien por desconocimiento, bien porque la propia red no le permite hacerlo, al no ofrecerle la configuración de sus datos personales con acceso «restringido» o «público», correrá el riesgo de que dicha información propia y la compartida con otros usuarios pueda ser accesible para cualquiera en la red, por lo que la vulneración de la privacidad aumenta considerablemente. Parece que en este momento todo depende de que la plataforma dote al usuario de lo imprescindible para poder controlar la información que cuelga, y de que el usuario esté concienciado de los peligros que suponen construir un perfil con excesivos datos personales. Desde luego, si la plataforma no le incitara a ello, ya sería maravilloso y constituiría un paso de honestidad en favor de la privacidad del usuario.

Además, a partir del registro hay que contar con otros peligros que son, diríamos, inherentes a las propias plataformas y que no puede controlar su usuario. Así, también por defecto, existen los llamados «Códigos maliciosos» o «software malignos» y los «coleccionistas de contactos» o «*social spammers*». Los primeros se dan normalmente en las redes sociales de ocio o generalistas, y sirven, entre otras acciones, para redireccionar el navegador de usuarios no experimentados. Se localizan en su mayor parte en programas espías o en publicidad emergente contenida en aplicaciones internas ejecutadas desde los navegadores de los usuarios. De ello se aprovechan los delincuentes informáticos, porque recordemos, que esa clase de redes son las más pobladas. Los «*social spammers*» hicieron que alguna red social profesional, como Linkedin, reaccionara e introdujera la llamada «relación de confianza mutua»[11].

Lo dicho nada tiene que ver con el control de la información publicada en una red social, perteneciente al segundo momento a considerar llamado «uso habitual de la plataforma», el cual es en sí mismo limitado, ya que depende en su mayor parte de la decisión del propio usuario (luego se matizará con el comentario de la mayor o menor permisibilidad en el acceso de las aplicaciones y publicidad), y es de suyo imposible controlar que otro usuario no pueda, con el nombre de otro, colgar cualquier dato de éste. Aquí el potencial riesgo a la intromisión ilegítima en la privacidad del usuario depende casi en su totalidad del control de la privacidad que ejerza el propio usuario y del azar; dicho usuario debe valorar qué publicar de sí mismo, y ser consciente de que inclusive sus propios datos pueden implicar ser utilizados por terceros. Pero subrayo que «casi» exclusivamente, porque lo que no puede el usuario es controlar la manipulación que desde la plataforma puede darse; como explica el Estudio «en la gran mayoría de ocasiones, las redes sociales permiten a los motores de búsqueda de Internet indexar en sus búsquedas los perfiles de los usuarios, junto con información de contactos y de perfiles amigos, lo que puede suponer otro riesgo para la protección de la privacidad, además de dificultar el proceso de eliminación de su información en Internet. Además,

> «la posibilidad que tienen estas plataformas de ubicar geográficamente al usuario a través de la dirección IP y conocer el dispositivo desde el que se conecta, para contextualizar los contenidos y la publicidad mostrada, puede considerarse como una intromisión en las rutinas del usuario que puede suponer un grave menoscabo del derecho a la intimidad»[12].

[11] Significa que la red exigió que para contactar con otro usuario de la red ambos usuarios hubieran aceptado previamente la existencia de la relación entre ambos.

[12] Estudio, pág. 63.

Hay que mencionar también que en el momento de usar la plataforma (esto es común también al momento del registro) el usuario en un consentimiento mal informado puede no ser consciente de que lo que cuelgue pase a ser propiedad de la plataforma. En efecto, la cesión de derechos de explotación de contenidos propios de forma ilimitada y plena hará que pasen a ser propiedad de la plataforma con su consiguiente explotación económica.

En el momento último en que el usuario solicita la baja del servicio, puede haber riesgos no controlables por el usuario, puesto que la cancelación de su cuenta no implica necesariamente la de su información, que una vez colgada puede seguir «indexada y almacenada en la caché de los distintos buscadores existentes en Internet» y accesible para el resto de los usuarios con los que la compartía. Aquí las preguntas más habituales de los usuarios adultos, puesto que los menores, incluso los maduros, no son conscientes de ello hasta que se pasa a mayores, se resumen diciendo: ¿cómo puedo desaparecer del mapa?