



## Quiénes son los “menores”

Para los fines de este artículo nos puede ser útil distinguir entre mayores y menores de catorce años en la medida en que sólo los primeros están sujetos a responsabilidad penal según Ley Orgánica 5/2000, de 12 de enero. Hablar de “menores”, generalizando, resulta difícil puesto que no todos los menores carecen de capacidad de discernimiento. El criterio de la edad, utilizado por el legislador, puede ser ciertamente arbitrario, como muestran algunas “voces” que abogan por ampliar este límite a 12 años, dada la cada vez más temprana edad en que los niños empiezan a utilizar Internet.

## La prevención como instrumento para detener el mal uso

La principal herramienta de prevención del mal uso de las nuevas tecnologías es la educación del menor. Sin embargo la brecha generacional que existe respecto a los educadores dificulta su aplicación.

Un primer paso para superar esta dificultad es acotar el problema. Así, se plantean tres ámbitos en los que el menor puede abusar de las nuevas tecnologías.

El primero es la casa, donde la familia debería educar al menor en lo que se refiere a los peligros de Internet y a un uso razonable del ordenador, sobre todo en lo que se refiere a la duración y a los horarios del uso, ya que hoy en día muchos expertos avisan del creciente problema de adicción que crea la red.

Otro posible ámbito de riesgo es la escuela/instituto o, en general, lugares de acceso público que proporcionan conexión a Internet. Aquí la prevención debe adoptar un carácter más tecnológico. Medidas de seguridad preventivas son el uso de usuario/contraseña individual, el establecimiento de un log de las páginas web visitadas, filtros de contenidos, etc.

Por último, el uso del móvil merece un tratamiento específico y diferenciado que no abordaremos en el presente artículo.



## **La prueba electrónica como herramienta procesal decisoria para probar el mal uso que pueden hacer los menores de las nuevas tecnologías**

La prueba electrónica es el instrumento más adecuado para acreditar la realidad de un acto realizado a través de medios electrónicos.

Antes de entrar en el análisis del uso de dicha prueba, como herramienta procesal decisoria en los tres ámbitos mencionados, resulta útil una pequeña introducción.

### **La prueba electrónica**

Un estudio de la sociedad española de investigación de fraudes en entornos virtuales Cybex<sup>1</sup>, ha puesto en evidencia que en Europa, ninguno de los países miembros dispone en sus ordenamientos jurídicos de una definición de prueba electrónica.

En términos generales, y lejos de dar una definición exhaustiva, la prueba electrónica puede ser definida como cualquier información obtenida a partir de un dispositivo electrónico o medio digital que sirve para adquirir convencimiento de la certeza de un hecho.

Las pruebas electrónicas correctamente obtenidas y presentadas serán exactas, veraces y objetivas.

No obstante, para su plena aceptación es necesario resolver importantes problemas.

Las pruebas electrónicas se caracterizan por su naturaleza inmaterial y por su volatilidad que permiten el fácil traslado, alteración y manipulación de las mismas. Por lo tanto, el primer problema es garantizar su autenticidad e integridad.

El estudio de Cybex sobre pruebas electrónicas revela que en el sistema normativo procesal vigente en Europa no existen procedimientos específicos que regulen la obtención, preservación y presentación de la prueba electrónica ante los tribunales y durante la investigación. Sin embargo, en algunos países ya existen unas “*best practices*” que todavía no tienen fuerza vinculante<sup>2</sup>. Aun cuando existan dichas normas procesales, será necesario analizar cómo las modalidades técnicas de su adquisición puedan encajar en el cuadro de las garantías procesales, evitando así la violación de derechos fundamentales (en la mayoría relativos a la protección de datos y al secretos de comunicaciones).

<sup>1</sup> La admisibilidad de la prueba electrónica ante los tribunales. AGIS 2005

<sup>2</sup> En EEUU, *Federal Guidelines for Searching and Seizing Computer*, del US Department of Justice. En el Reino Unido las *Good Practice Guide for Computer based Electronic Evidence*, de la *Association of Chief Police Officer (ACPO)*



También hay que cuidar el lenguaje técnico de los dictámenes periciales para que sean comprendidos por los juzgadores y puedan cumplir con su función auxiliar de refuerzo a la eficacia probatoria de la prueba electrónica.

### La prueba electrónica en el ordenador familiar

Los padres habitualmente desconocen la actividad realizada por sus hijos en Internet, encontrándose el problema cuando ya es demasiado tarde.

Una muestra de este desconocimiento es el dato de un estudio, elaborado por dos organizaciones de protección de la infancia, en el que se indica que el 80% de los niños encuestados accede a la red a través de ordenadores sin sistema de filtrado alguno<sup>3</sup>.

Por otro lado, el éxito de las recientes acciones de sensibilización sobre los peligros de Internet, ha llevado a los padres a controlar más los hábitos de sus hijos en la red, por ejemplo accediendo a sus cuentas de correo electrónico. En estos casos se plantean cuestiones sobre el derecho a la intimidad del menor, sobre todo a medida que éste se va acercando a los 18 años.

No faltarán voces que estimen que entre las facultades de “*corrección razonable y moderada*” que otorga el art. 154 del Código Civil a los titulares de la patria potestad se incluye la legitimidad del acto de injerencia de intimidad. Sin embargo, aún reconociendo las dificultades para fijar reglas generales, no parece que el Código Civil conciba el ejercicio de la patria potestad como una fuente de legitimación de cualquier clase de injerencia. El juicio que los titulares de la patria potestad tengan acerca de las repercusiones que en la formación integral del menor pueda acarrear la incontrolada utilización del correo electrónico, puede condicionar, desde luego, la decisión acerca de si el hijo ha de ser o no titular de una cuenta, pero no debería, una vez concedida la autorización, invocarse para defender injerencias injustificadas<sup>4</sup>.

<sup>3</sup> *Seguridad infantil y costumbres de los menores en Internet*. Estudio realizado para el DEFENSOR DEL MENOR por ACPI (ACCIÓN CONTRA LA PORNOGRAFÍA INFANTIL) y PROTÉGELES, 2002.

<sup>4</sup> Dimensión jurídico-penal del correo electrónico, MARCHENA GÓMEZ, Manuel, *Diario La Ley*, Nº 6475, Sección Doctrina, 4 May. 2006, Ref. D-114, Editorial LA LEY.

Otra cuestión es el registro domiciliario y la intervención del ordenador familiar por parte de la policía una vez que el delito se haya cometido. En este caso, ¿en qué medida se puede consentir la violación de la esfera de intimidad del menor?

No hemos sido capaces de localizar una sentencia que ilustre adecuadamente este supuesto. No obstante no debemos dejar de señalar los principales problemas ligados a la intervención de ordenadores privados en las investigaciones de delitos informáticos.

### *1. Identificación del equipo informático*

Toda investigación informática exitosa acaba conduciendo a un equipo informático que se conecta a Internet a través de un determinado proveedor de acceso.

El éxito de esta fase de la investigación depende de la conservación de los datos de tráfico. En este sentido, además del derogado artículo 12 de la Ley de Servicios de la Sociedad de la Información, debe tenerse muy en cuenta la Ley 25/2007, de 18 de octubre, relativa a la conservación de datos relativos a las comunicaciones electrónicas y que es la transposición de la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo.

Todas coinciden en la necesidad y obligación de conservar estos datos de tráfico en cuanto se trata de un elemento fundamental de partida de toda investigación de delitos informáticos.

### *2. Entrada y registro en lugares cerrados*

Una vez localizado el ordenador, para acceder a éste habrá que superar el obstáculo de la protección del derecho a la inviolabilidad del domicilio y a la intimidad, por lo que la intervención del ordenador deberá estar amparada por las exigencias constitucionales y legales que rodean la entrada y registro en domicilio y otros lugares cerrados (art 545 LeCrim).

### *3. Identificación del usuario del equipo informático*

Después de la identificación del equipo, debe procederse con la identificación del usuario a través de investigación policial clásica.

En efecto, la dirección IP identifica a un equipo, pero no necesariamente a la persona que lo está utilizando (usuario). Esto puede llevar a que el padre o la madre de un menor sean acusados de un delito, por ejemplo, de amenazas, que ha cometido su hijo menor de 18 años.



#### *4. Conservación de las pruebas electrónicas*

La sentencia de la sección 7 de la Audiencia Provincial de Barcelona de 29 de enero<sup>5</sup> ha destacado la necesidad de almacenar de forma adecuada el material informático incautado para que pueda ser consultado y considerado como prueba de convicción.

Esto resulta especialmente importante dada la fragilidad de la información en formato digital. Por tanto, la adecuada conservación y almacenamiento de las pruebas electrónicas hasta el día del juicio es fundamental para la acreditación de su autenticidad, como ya ha tenido ocasión de resaltar el Tribunal Constitucional en su sentencia 170/2003 de 29 de septiembre.

#### **Conclusiones**

La brecha generacional existente entre padres e hijos y el bajo grado de conocimiento del funcionamiento de los medios informáticos entre los usuarios obstaculizan la prevención para detener el mal uso que los menores pueden hacer de las nuevas tecnologías. El conocimiento de los padres relativo al peligro que supone un uso incorrecto de los medios informáticos, no está suficientemente generalizado.

Esto provoca que los menores se encuentren solos frente a un nuevo medio que puede prestarse a malos usos. Además se trata de malos usos que no quedan impunes puesto que existe la herramienta procesal para probarlos: la prueba electrónica. Por último, es importante destacar que, en el caso de que el delito se hubiera cometido por un menor de catorce años y, por lo tanto, no sujeto a responsabilidad penal, las consecuencias penales de su acto inconsciente podrían caer sobre los padres.

Quedan muchas cosas por analizar, que serán objeto de posteriores artículos. Por ahora es suficiente destacar la necesidad de sensibilizar a la sociedad sobre esta temática para proteger a hijos y padres.

<sup>5</sup> Audiencia Provincial de Barcelona (Sección 7) Sentencia núm. 95/2008 de 29 de enero ARP/2008/317

