# ¿Debemos proteger a nuestros menores de Internet?

Si realizamos esta pregunta a la ciudadanía, seguramente el resultado sería un SI claro y contundente, por lo menos es lo que nosotros apreciamos de nuestras comunicaciones con los padres de dichos menores.

Sin embargo, desde mi punto de vista, no debemos proteger a los menores de Internet; debemos proteger a los menores de las personas que hacen mal uso de la red, incluso de ellos mismos. Es decir, Internet no es el enemigo, es únicamente una herramienta y por lo tanto, conceptos tales como la bondad o la maldad le son ajenos. La tecnología es neutra. Es el uso que se haga de la misma lo que determina su catalogación moral. Internet no es más que una lupa en la que se magnifican las características de quienes participan en ella. Así, podemos encontrar brillantes creaciones artísticas, científicas o literarias, cohabitando con pornografía infantil, fraudes y diversas apologías del odio.

Nuestros menores conforman la generación de los llamados “nativos digitales” (terminología utilizada por primera vez por Marc Prensky en su libro “Enseñanza de los nativos digitales”), es decir, niños que han nacido cuando Internet y las tecnologías asociadas ya estaban desplegadas y su uso era común.

Eso les ha llevado a que asuman, desde su más tierna infancia, como algo normal, el uso de estas tecnologías, a las cuales se han ido acercando con naturalidad según iban creciendo. Para ellos, su vida digital es parte integrante de su vida real y en ocasiones no son conscientes del doble plano en el que tienen que moverse, ya que las fronteras entre los mundos virtual y real están muy difuminadas y desleídas.

La principal consecuencia de esta temprana inmersión tecnológica es el establecimiento de una brecha digital entre su generación y la de sus progenitores, quienes a la postre somos “inmigrantes digitales” (según la misma terminología utilizada por Marc Prensky).

Para la generación de sus padres, el acercamiento a Internet y las tecnologías relacionadas, se ha llevado a cabo unas veces de forma voluntaria, y otras de forma forzada, debido sobre todo a la necesidad de utilizar estas herramientas, y casi “por obligación” en muchos casos, lo que implica que su comprensión del “mundo virtual” es muy limitada.

Si a cualquiera de nuestros menores se le entrega un móvil de última generación, en tres minutos lo han desembalado, puesto la tarjeta sim, la batería, lo han conectado a Internet, se han descargado el Whatsapp, han configurado los tonos, los fondos y lo han personalizado. En ese tiempo, sus padres, estarían aún buscando en el manual la sección que viene en su idioma materno.

Esta brecha digital también existe, aunque es cierto que en menor medida, con sus profesores, ya que aunque el Departamento de Educación les forma y les obliga a utilizar en la docencia las nuevas tecnologías (p.e. plan Eskola 2.0), únicamente comprenden aquellas herramientas que utilizan habitualmente y solo en contadas ocasiones realizan una inmersión más profunda en el campo tecnológico. El descubrimiento de nuevas tecnologías no asociadas a la educación es algo que dependerá únicamente del interés personal del docente. (Y estas tecnologías pueden ser tan importantes como el Whatsapp, distintas redes sociales, etc.)

Debido a este desfase, unos y otros, padres y profesores, se sienten, y así nos lo han manifestado en innumerables ocasiones, completamente impotentes a la hora de educar a los menores en el uso responsable de Internet.

Esta pretendida discapacidad formativa, en realidad no es tal, es únicamente una apariencia, y se basa en la demonización de la tecnología, en hacer hincapié en las conductas perniciosas de la Red, frente a las cosas positivas de las mismas. Se ve Internet como un ente del que hay que proteger a los menores. Este enfoque, como se ha apuntado anteriormente, desde nuestro punto de vista es erróneo: no hay que defender a nuestros menores de la tecnología. Hay que defender a nuestros menores de las personas que hacen mal uso de la misma.

Así las cosas, aquellas normas de educación y protección que nuestros padres y abuelos nos inculcaban cuando nosotros éramos pequeños sirven todavía en nuestros días, incluso si se aplican a Internet y sus riesgos. Por ello aconsejamos a los padres que si para la educación de sus hijos la tecnología supone un problema, que la eliminen de la ecuación, no que le prohíban usarla, sino que apliquen los mismos sistemas de protección y educación que utilizan con sus hijos en la vida real. Que conviertan a la tecnología en algo transparente, que se pueda fluir a su través sin que sea un impedimento.

Es cierto que un mejor conocimiento por parte de todos los actores implicados, de las distintas tecnologías, facilitaría enormemente su comprensión y por lo tanto serían mucho más capaces de educar a sus hijos, y por ello no debe aislarse de todo lo que suponen las nuevas tecnologías.

Por otro lado, nuestros menores, aunque muy capaces técnicamente, carecen de la madurez necesaria para comprender las implicaciones y consecuencias que sus acciones tienen, tanto en los demás como en si mismos. Muchas de sus acciones son tomadas por ellos mismos como juegos o bromas carentes de importancia cuando en la realidad es que se trata de delitos, y en ocasiones graves. Todo el mundo sabe que robar es un delito, pero sin embargo el sustraer una cuenta de correo de otra persona no estaría tan claro, por lo menos para cierta parte de la Sociedad, porque al fin y al cabo, las cuentas de correo son gratuitas, al menos la inmensa mayoría de ellas.

# RIESGOS O CONDUCTAS ERRÓNEAS

Pero, ¿cuales son los peligros más frecuentes a los que se pueden enfrentar los menores al acceder a Internet?

1. **Conexión constante a la Red**. Hace solo unos años, para poder conectarnos a Internet teníamos que utilizar unos ruidosos módems. Estos módems solo se podían utilizar en los hogares desde las 8 de la noche hasta las 8 de la mañana, pues era cuando teníamos la llamada "Tarifa plana", hacerlo fuera de esas horas suponía en muchos casos un "suicidio económico" por los costes asociados que tenían otros horarios. Además al realizar la conexión hacían un ruido espantoso, y han generado más de una discusión porque los cohabitantes se despertaban y eso además ocurría varias veces por errores en las conexiones.

   En esa época, si alguien quería atacarnos, tenía que utilizar ese horario porque fuera de él no estábamos "online". Los menores de edad, disponían de un horario más reducido porque eran enviados a la cama e internet se acababa. Ya no podían hacer uso de ella sin que sus padres lo supieran por el ruido que generaba el módem. Además, como otro hándicap, durante la conexión a la Red no se podía utilizar el teléfono. En algunos casos cuando estabas descargando un fichero grande y estabas próximo a acabar alguien te llamaba y en ocasiones reseteaba la conexión y vuelta a empezar. Por último las conexiones eran extremadamente lentas.

   Sin embargo ahora, todos los hogares con conexión a Internet lo hacen mediante la alta velocidad, bien sea ADSL o cable, con tarifa plana real, y sin interferir en el teléfono. Esto supone que muchos equipos están permanente conectados a la Red porque puesto que… "ya que pago la conexión la aprovecho al máximo". Aunque no haya nadie en el ordenador, el mismo suele estar conectado a internet.

   Además la mayoría de los routers modernos tienen conectividad wifi, la cual en la inmensa mayoría de los casos se encuentra abierta pese a no tener ningún dispositivo conectado.

   Estos avances en la comunicación tienen también su contrapartida y es que aumentamos exponencialmente la ventana temporal de exposición. Ahora nuestros equipos pueden ser localizados y por lo tanto atacados las 24 horas del día. Nuestros wifis pueden ser utilizados por nuestros vecinos a cualquier hora del día, bien sea para navegar por internet gratis (el menor de los males), para hacerlo de forma anónima o bien para atacar a nuestros sistemas.

   Si a eso le unimos que en breve se producirá el abandono del protocolo IPV4 y su cambio por el IPV6, que va a permitir que cualquier dispositivo que se alimente de electricidad pueda estar permanentemente conectado a Internet

veremos como el riesgo potencial de ser víctimas aumenta de manera considerable.

Por último a nuestros menores a partir casi de los 10 años ya les estamos dando teléfonos móviles con la excusa de "tenerlos localizados y que nos llamen cuando pase algo". Creo que se nos está yendo de las manos... Un menor de 10 años va de casa a la escuela, y al salir sus padres o la persona designada lo recogen y lo llevan al parque (si tiene suerte) o a actividades extraescolares (si no la tiene). ¿Necesitan realmente un móvil?.

Además, para no gastar, les instalamos el Whatsapp o el Line o programas similares para que puedan chatear gratis. Aumentamos doblemente los riesgos: por un lado, porque estos móviles son nuevas vías de contacto que pueden ser aprovechadas por delincuentes para acceder a nuestros menores y en segundo lugar porque no son pocos los menores, que en la soledad de su cuarto, de madrugada, permanecen chateando con sus contactos mientras deberían estar durmiendo. Esto se traduce en la bajada del rendimiento escolar.

2. **Las webcams y los teléfonos con cámara**. Existen infinidad de malware que pueden controlar remotamente las cámaras instaladas en equipos informáticos. Esto no sería preocupante si nuestros menores no tuvieran el ordenador instalado en su dormitorio con la webcam apuntando hacia dónde duermen o se cambian de ropa. O si tienen portátil, que cuando están chateando y tienen que hacer alguna necesidad fisiológica no se lo llevan al baño, o incluso a la ducha para evitar perderse esos "interesantísimos chats" con sus amistades.

   Hace un tiempo aconsejábamos a los padres que los ordenadores estuvieran situados en un lugar común, pero ahora con la proliferación de los móviles y tablets este consejo se nos ha quedado completamente corto.

3. **No hay cultura de seguridad informática** ya no solo en los menores, sino en la Sociedad en general. Venimos de un ordenamiento jurídico destinado a proteger el mundo físico y ahora ante el mundo digital, intangible pero real, se torna un poco vago y esa cultura tiene su reflejo en muchos ámbitos de la vida.

   Si en un barrio cualquiera una persona abre una tienda de golosinas, lo primero que hace antes de llenarla de género y abrirla al público es poner una persiana y en ocasiones una alarma. Sin embargo si lo que abro es una tienda por internet, ni se preocupan en cumplir las mínimas medidas de seguridad para evitar que alguien ataque a su aplicación. Esta discordancia también se aplica a otros ámbitos de la vida. Como para navegar por la Red únicamente necesitamos un ordenador y una conexión creemos que esa facilidad es sinónimo de seguridad. ¿Para que me van a atacar a mi si no tengo nada importante?

4. **Contenidos inapropiados.** Dentro de esta catalogación podríamos incluir todas aquellas páginas que alojan contenidos que de ser vistos por mentes en formación pueden tener consecuencias lesivas para el correcto desarrollo cognitivo y emocional. Ejemplos serían las páginas de pornografía en general, las de ensalzamiento de la anorexia y bulimia, las "gore" que muestran escenas escalofriantes en cuanto a su brutalidad, las que hacen apología de los distintos tipos de odio, bien sean xenófobos, políticos, de clases o de sexo.

5. **Depredadores sexuales.** Sujetos que navegan por las redes a la caza y captura de menores a los que embaucar para que les envíen fotogramas eróticos y llegado el caso a obtener contactos sexuales con los mismos. Estos sujetos utilizan sofisticados métodos psicológicos para hacerse con el control de las mentes de nuestros adolescentes, los cuales por sus características de maduración son muy vulnerables a estas técnicas. No debemos olvidar que el paso de la infancia a la adolescencia es un periodo vital caracterizado por incontables problemas psicológicos, desde la falta de autoestima, conductas agresivas, necesidad de reconocimiento, despertar a las conductas sexuales, que si bien en la inmensa mayoría de los casos son superados con el paso del tiempo, no es menos cierto que este periodo hace a los adolescentes especialmente vulnerables.

   Uno de los modus operandi de estos depredadores consiste en que se apropian de la cuenta de correo electrónico de un menor. Teniendo en su poder la cuenta de correo electrónico tienen acceso a toda su vida digital, fotografías almacenadas, perfiles de redes sociales, mensajes, contactos, etc. Haciendo uso de la ingeniería social, mantienen conversaciones con sus contactos para obtener el control de más cuentas.

   Una vez obtenido el control suelen contactar nuevamente con las víctimas para extorsionarles diciendo que si no acceden a activar la webcam, o al envío de fotogramas sexuales, sus secretos, (en algunas ocasiones, bastante sensibles) serán distribuidos entre sus amigos, padres y profesores. Debido a la inmadurez propia de la edad, esta situación de estrés se magnifica y en muchas ocasiones estos menores sucumben a las amenazas y entran en un círculo vicioso de difícil ruptura, puesto que las imágenes exigidas son cada vez más comprometidas.

   Pero no siempre es necesaria la captura de un perfil para la extorsión. En otras ocasiones el delincuente adopta la identidad de un adolescente y se produce un "enamoramiento". Para poder obtener la información necesaria para llevar a cabo su plan, hace años el acosador tenía que estar mucho tiempo sonsacando y conociendo a su víctima hasta que tenía los datos precisos para conocer bien sus gustos y aficiones. Ahora, este paso ya no es necesario. Basta con "echar un ojo" a los perfiles de las redes sociales y allí tenemos toda la información, edad, altura, peso, gustos, deportes que practico, libros que leo, incluso una detallada colección de fotografías, que permite además elegir a la víctima según los gustos de los pederastas.

Con todos esos datos en su poder, lograr el enamoramiento es relativamente sencillo. Una vez obtenido, el acosador va a enviar una fotografía de quien se supone que es él. La victima le va a mandar otra. El pederasta le va a contestar con una foto con el torso desnudo, la victima una en bikini….. y así se va subiendo la intensidad sexual de las imágenes hasta que logra fotografías verdaderamente comprometidas.

Llegado a este punto el delincuente se descubre y empieza la verdadera extorsión, exigiéndole a su víctima nuevos fotogramas o vídeos con la amenaza de que si no los obtiene publicará las que ya tiene en su poder y se las reenviará a sus amigos, padres y profesores.

Debido a la falta de maduración y a la carencia de herramientas psicológicas adecuadas, es muy fácil que estos menores, presas del miedo y la vergüenza, caigan en esta espiral de la que es muy difícil salir.

6. **Acoso entre iguales**, el tristemente famoso ciberbullying. Como su vida transcurre entre los mundos virtuales y reales, este acoso también se libra en ese campo de batalla. Los insultos, vejaciones y demás actos impropios tienen lugar en ambos frentes. Crean perfiles, cuentas, identidades ficticias para suplantar la identidad de la víctima o bien para catalizar el odio hacia ella.

   Frecuentemente observamos como los menores son capaces de hacerse con el control de una cuenta de correo electrónico de uno de sus compañeros, suplantar su identidad ante el grupo y leer sus mensajes de correo, en un símil actualizado de lo que en nuestra época era el leer los diarios de los hermanos mayores.

   Bien, esta conducta, para la que se encuentran capacitados técnicamente, puede conllevar penas, que de ser mayores de edad, se convertirían en penas de prisión, y por lo tanto al trasladarse al ámbito de la protección del menor también deberían llevar aparejadas sanciones altas.

   Además el uso de Internet y del resto de tecnologías para comunicarse entre ellos proporciona un halo de impunidad, de relajo del control social de sus acciones y un pretendido anonimato, lo que deriva en que se atrevan a decir a un compañero cosas a través de la tecnología, que en directo no serían capaces, ya no solo por la posible represalia, sino por la dificultad de afrontar la comunicación “cara a cara”.

   No tenemos que engañarnos, el acoso como tal, ha existido siempre. Lo que pasa es que antes, la vida escolar y la extraescolar, frecuentemente estaban separadas, es decir, los niños se relacionaban con sus compañeros en el colegio pero al salir de él establecían otras relaciones con otros niños que frecuentemente no tenían nada que ver con la institución escolar. Es decir, existían dos grupos sociales distintos que pocas veces se mezclaban. Por lo tanto, lo que ocurría en uno de estos círculos no solía tener trascendencia en el otro grupo. Sin embargo en la actualidad, estos grupos se hallan generalmente interconectados a través de las

redes sociales y es prácticamente imposible mantener privado un suceso ocurrido en cualquiera de nuestros ámbitos de relación: enseguida se extiende hacia otros grupos a los que pertenezcamos.

Además la trascendencia de las acciones realizadas en la vida real y en Internet tienen una muy distinta repercusión. No es lo mismo que dos chavales se insulten en el baño y nadie escuche esa bronca, que mantengan esta discusión a través de las redes sociales. El daño ocasionado en el segundo de los casos es enormemente mayor toda vez que la publicidad de los insultos llega al entorno social de ambos y por lo tanto la sensación de agravio es mucho más grave.

Internet ha posibilitado además una "democratización" del acoso. Antes el acosador generalmente solía ser el típico alumno "polirepetidor" con tendencias delincuenciales que basada en su mayor maduración física imponía su dominio a sus compañeros de clase. Pero ahora, cualquiera de los compañeros puede poner en un "brete" a otro sin más que sacarle una fotografía comprometida y publicarla en internet.

Este acoso se lleva a cabo de muchas formas distintas pero muchas de ellas pasan por la creación de perfiles en las redes sociales, suplantando la identidad de las víctimas, en las que se muestran conductas que buscan minorar su relevancia social y hacer que el grupo "la tome" con la víctima. Esta conducta tiene difícil encaje en nuestro ordenamiento jurídico, puesto que los jueces para considerar este delito como suplantación de personalidad estiman que es necesario que tal usurpación se lleve de manera íntegra en todos los aspectos de la vida de la víctima y que además tenga una permanencia muy amplia en el tiempo. Por lo tanto estas conductas pueden resultar impunes, aunque causen un grave daño psicológico a las víctimas que ven como sus amigos se apartan de él en base a unos comentarios que le son atribuidos pero que no ha generado.

En bastantes ocasiones las víctimas del bullying suelen cambiar de colegio buscando dejar atrás las agresiones, pero estas las persiguen. Este abandono del centro escolar es una victimización secundaria, que lejos de arreglar el problema lo magnifica, porque en el nuevo centro educativo, sus nuevos compañeros van a tener constancia de lo que ha ocurrido en el centro de origen y el acoso, con mucha probabilidad, se va a reproducir. El problema tiene que resolverse en el mismo lugar en el que se genera, bien sea mediante una charla entre los padres implicados, o con la intervención del centro o en último caso con nuestra participación. En cualquier caso, si alguien debe abandonar el centro escolar para restaurar la convivencia, deberían ser siempre los agresores, nunca las víctimas. No es de recibo que a la víctima de una agresión se le imponga además una medida de alejamiento de su agresor, por mucho que consideremos que lo hacemos para su protección. Es una forma fácil de eludir el problema, no de solucionarlo.

7. **Fraudes.** Estos, en principio son muy restringidos, por la escasa importancia de los mismos debido a la limitada disponibilidad monetaria de los adolescentes. La gran mayoría de ellos suelen consistir en compraventas a través de internet, y los mensajes Premium. Sin embargo, en ocasiones se tornan graves cuando se hacen con la tarjeta de crédito de sus progenitores para utilizarlas en sitios de juego online, siendo de ellos los más peligrosos los juegos de apuestas.

8. **Autoexhibición.** Los menores vierten en Internet cantidades ingentes de información sobre su vida e intimidad que puede ser utilizada en su contra. Ya no solo esas fotos "atrevidas" que cuelgan en sus perfiles de las redes sociales, sino el resto de información sobre sus estudios, domicilios, viajes que realizan, etc.

   Hay perfiles que son verdaderos diarios vitales minuto a minuto, la proliferación de los teléfonos móviles con conexión a Internet ha posibilitado una conexión 24/7 y todo lo que le pasa a un menor suele volcarse en su red social. Es triste observar como cuadrillas de adolescentes se reúnen en algún lugar y entre ellos no hablan solo se comunican a través de los móviles, aunque estén a un escaso metro de distancia.

   Además, la inmensa mayoría de los smartphones tienen el servicio gps activado lo que posibilita que las fotografías que se obtienen con estos dispositivos estén geoetiquetadas y pueda realizarse un seguimiento de los lugares exactos dónde han sido obtenidas.

   Otro de los problemas añadidos de la publicación de fotos en las redes sociales es la inmediatez de su publicación, es decir, desde que se obtiene la fotografía hasta que se manda a la red, pasan escasos segundos. Hace relativamente poco tiempo, para subir una foto a la red teníamos que sacarla con una cámara digital, pasarla al ordenador, verla en nuestro monitor, y después enviarla. En cualquiera de estos estadios podríamos arrepentirnos del contenido que íbamos a enviar y abortar su distribución. Además la visualización de la foto en un monitor aporta un mayor control de detalle de lo que realmente se ha captado, cosa que no pasa en la pequeña pantalla de nuestro móvil, donde los detalles del fondo suelen pasar desapercibidos.

   En las charlas que impartimos, llegado este punto, solemos hablarles de lo que nosotros denominamos "la prueba del tablón". Para centrar el ejemplo hacemos varias preguntas:
   - ¿Quienes de los asistentes han acudido el verano pasado a la playa o a la piscina?. Suelen ser la práctica mayoría los que asienten.
   - ¿Os habéis sacado fotografías en bikini o bañador?. Suelen contestar la práctica totalidad de forma afirmativa.
   - Ahora nos solemos centrar en las chicas porque su pudor suele ser mayor: les preguntamos si alguna de ellas pondría esas fotografías en un tablón de anuncios que íbamos a instalar en la entrada del centro escolar. Aquí, sin excepción todas contestan negativamente.

- La última pregunta es si han subido esas fotos a las redes sociales. Muchas suelen contestar positivamente.

Curiosamente son muy pudorosas a la hora de colgar las fotografías en un tablón físico por el miedo o la vergüenza de que sus compañeros de clase pudieran verlas y sin embargo no tienen ningún reparo en colgarla en sus perfiles donde curiosamente tienen agregados, a todos sus compañeros de clase, además de el resto de contactos ajenos al centro escolar.

Además se da la circunstancia, todavía más grave, de que si alguien le gusta la fotografía física del tablón y la coge solo habría una foto circulando, sin embargo puesta en Internet, cualquiera que la vea puede realizar una copia. Si me arrepiento de haberla colgado físicamente, cuando la retire, nadie más la podrá ver, pero en el mundo virtual, aunque la retire, nadie puede saber cuantas copias hay almacenadas en los discos duros de los que la hayan visualizado.

Y no hablemos del conocido como sexting que consiste en el envío de fotografías pretendidamente sexys a las parejas sentimentales. Cuando las parejas se rompen no de forma consensuada, curiosamente a uno de ellos siempre le "entran en el ordenador", le roban las fotos y las distribuyen.

9. **Sacarse fotos con el teléfono móvil**. Aunque no tengan intención de subirlas a la Red. Esas fotografías que empiezan siendo atrevidas y en muchas ocasiones llegan hasta ser pornográficas, se almacenan en el teléfono móvil y estos pueden ser robados o simplemente perdidos. Si a esto unimos que muchos adolescentes no tienen contraseña en el móvil en la creencia de que de este modo si se les pierde el que lo encuentre llamará a sus padres y se lo devolverá…. El acceso a estas fotografías no está restringido. Y aún en el caso de que tengan clave de acceso estas fotos se guardan en la tarjeta sd y por lo tanto puede ser extraída y vista en cualquier ordenador o en otro móvil sin ninguna restricción. Además, para acabar de rematar la faena, las fotografías previamente borradas pueden ser recuperadas muy fácilmente mediante programas gratuitos, con lo que aquellas fotos que eran demasiado escandalosas para enviarlas e incluso para guardarlas en el móvil, siguen estando latentes en la tarjeta sd a la espera de como decía Bequer … " una mano de nieve sepa arrancarlas… " .

10. **Aceptar a desconocidos como contactos en las redes sociales**. Existe una especie de competición entre los menores para ser el que más contactos tenga en su perfil, como símbolo de popularidad y estatus. Es imposible que si tengo 500 contactos pueda conocer físicamente a todos y cada uno de ellos con lo que las posibilidades de que entre estos haya alguien que es quien no dice ser se multiplican de forma exponencial.

11. **Facilitar contraseñas.** En su inocencia, los menores confían en exceso en sus contactos y es muy frecuente que faciliten sus contraseñas a sus conocidos cuando les son requeridas. Esta es una de las formas en las que los acosadores se hacen con el control de cuentas de correo y perfiles.

    Una vez han logrado la primera de las cuentas, contactan con los amigos de la primera víctima y, suplantando su identidad, les pide sus contraseñas pretendiendo que necesita enviar un mensaje, bajar una foto o lo que sea y no le funciona su perfil.

    Hay que señalar que todos nuestros secretos, toda nuestra vida digital únicamente está separada de los delincuentes por una palabra, la contraseña y si la damos alegremente, cualquiera podrá acceder a mis recuerdos y vivencias.

    Estamos sufriendo una transformación en el almacenamiento, no hace demasiados años, las fotografías las guardábamos en los álbumes de fotos, pasamos a las cámaras digitales y los discos duros y los cds y ahora estamos en los smartphones y el almacenamiento en la nube. La información ya no está (solo) en nuestros dispositivos hay copias de la misma en páginas web, perfiles, en sitios de almacenamiento online, etc.

# PRETENDIDAS SOLUCIONES.

Analizados los principales problemas vamos a ver cuales son las soluciones más utilizadas

1. **Control parental tipo filtro.** Los filtros de navegación se basan en que un programa informático determine la idoneidad del contenido al que el usuario está accediendo y que puede ser configurado para que permita o impida ver determinados contenidos. Desde nuestro punto de vista, este tipo de control parental debería ser pactado por padres y menores de forma que estos supieran que no se les va a permitir acceder a determinados lugares porque son peligrosos para su desarrollo psicológico. Sin embargo esta medida tiene una limitada eficacia, toda vez, que estos menores estarán protegidos, únicamente cuando accedan a la Red a través del ordenador en el que se haya instalado el software. En cuanto vaya a casa de un amigo, un cibercafé, o haga uso de tablets, móviles, etc. será completamente ineficaz.

2. **Control parental tipo espía**. Existen muchos desacuerdos sobre la legitimidad de instalar este tipo de software, que lo que hace es realizar un exhaustivo informe sobre lo que el menor está viendo. Por un lado los tutores son responsables de la educación y de las acciones que sus hijos realicen y por lo tanto deben tener algún tipo de control sobre sus conductas, pero por otro lado los menores también deben tener derecho a cierta intimidad. Además la maduración de los jóvenes no se realiza de forma cuántica, sino de forma progresiva y secuencial. Sin embargo para la Ley tan menor es alguien de 17 años y 364 días como uno de 13 años, aunque su nivel evolutivo sea completamente distinto. Además, siempre desde nuestro punto de vista, la instalación de este control parental espía, supone un riesgo importantísimo con respecto a la relación entre padres e hijos. El instalar un software de este tipo, a la larga va a suponer que debido a alguna actualización del antivirus sea reportado como instalado en el sistema y el menor se va a dar cuenta de ello.

   Por otro lado está una reflexión sobre la necesidad e idoneidad de estas conductas. Es cierto que muchos padres se sienten tentados a instalar estos programas de control para saber que es lo que sus hijos hacen en internet. Como se ve, son solo chivatos, es decir no impiden que se accedan a los contenidos, sino únicamente avisa de lo que se ha visto. Además estos padres, tan proclives a este sistema de control en Internet, ni se plantearían contratar a un detective privado para controlar a sus hijos cuando salen de fiesta. ¿Es que Internet es más peligroso para los menores que la vida real?.

   Además este sistema adolece de los mismos problemas que el anterior, solo que en el primero de los casos ha sido aceptado por el menor y en el segundo ha sido impuesto, con lo que si lo descubren, además de la pérdida de confianza en sus progenitores, el menor, con toda seguridad va a ser capaz de soslayarlo, pues en

la mayoría de los casos, la competencia técnica de ellos supera con mucho la de sus tutores.

3. **La educación**. Internet es para nuestros menores, una parte indisoluble de su vida y por lo tanto tenemos que orientarles en ella de la misma forma que lo hacemos en la vida real.

   Si en nuestra infancia los padres despreocupados, dejaban a sus hijos viendo durante horas la televisión, ahora los dejarán desprotegidos navegando en Internet.

   Aunque ambas conductas parezcan similares hay que tener en cuenta que por muy mala que sea la programación de la cadena televisiva que estén viendo, detrás de la misma hay una serie de personas que filtran de alguna forma su contenido y sus horas de emisión, en base a una autorregulación, y sin embargo esto no pasa en Internet donde les permitimos un acceso ilimitado para buscar lo que quieran e incluso que puedan ser contactados por extraños.

   Este es el único sistema verdaderamente eficaz para prevenir los delitos en Internet. Es cierto que no podremos impedir que los acosadores nos tomen como víctimas, pero si que podremos detectar estos riesgos con anticipación y poder evitar el agravamiento de la conducta.

   Hemos de enseñarles hábitos saludables de navegación, que herramientas utilizar, que páginas web visitar y cuales no, que protejan su intimidad, su identidad, que no agreguen ni charlen con desconocidos, etc. De esta manera, cuando lo interioricen serán capaces de navegar autónomamente sin la supervisión de un adulto y estarán más seguros en su uso de Internet.

   En esta educación debería participar varios estamentos, por un lado los padres, quienes deberían encauzar las conductas desde la más tierna infancia realizando la navegación conjunta, posteriormente permitirles el acceso a sitios seguros para al final ir dándoles mayor libertad. Es cierto que esto implica una dedicación de los padres para aprender como funciona Internet y en muchas ocasiones estos se muestran reacios a tal formación.

   Además estaría la escuela, que como parte de la preparación de nuestros jóvenes para la vida no pueden dejar de lado las nuevas tecnologías, porque no estamos hablando del mañana en lo tocante a las TIC, estamos ya hablando del ayer.

   Otros estamentos también deben colaborar, las empresas de Internet, las policías, medios de comunicación, asociaciones, los legisladores, en fin toda la Sociedad para llevar a cabo una concienciación sobre el uso responsable de Internet.

   Conscientes de que la inmersión de los menores en las Tecnologías de la Información y Comunicaciones (TIC) es un proceso completamente automático, irrefrenable e irreversible al que no puede ponerse trabas ni obstáculos, desde

hace ya tres años, en la Ertzaintza, venimos desarrollando un proyecto de colaboración con distintas escuelas, colegios, institutos y universidades del País Vasco consistente en la impartición de charlas formativas sobre los peligros de Internet y las consecuencias que el mal uso de las tecnologías pueden acarrearles a los menores.

Este proyecto está teniendo una magnífica acogida, entre otras cosas, porque no es lo mismo que una cosa te la diga tu "profe", tu padre, o un policía que trabaja en "delitos informáticos". El peso que los menores otorgan a nuestras aportaciones es muy alto y nos es más fácil llegar hasta ellos porque son muy receptivos a nuestros consejos, sobre todo porque nos basamos en casos reales que hemos investigado.

4. **Medidas represivas.** Cuando estas medidas preventivas fallan tienen que existir las medidas represivas. Si bien es cierto que sería deseable no tener que hacer uso de estas, resulta de todo punto imposible evitarlas. Es entonces cuanto hacemos acto de presencia, policías, fiscales y jueces.

   Para poder investigar estos delitos que se comenten a través de Internet se necesitan básicamente tres cosas:
   - Conocimientos. Los ponemos nosotros.
   - Recursos técnicos: Los ponen los desarrolladores.
   - Herramientas legales: Las ponen los legisladores.

   En el caso del conocimiento se trata de que los policías vayamos lo más cerca de los delincuentes que sea posible. Adelantarlos va a resultar imposible porque cuentan con mayores recursos económicos, mayor formación y mejor cooperación internacional y además no están constreñidos por reglas que cumplir.

   Los recursos técnicos, pese a no ser completamente indispensables si que son interesantes puesto que facilitan enormemente la labor de los investigadores. Es una cuestión de números, hay más delincuentes que policías.

   La labor de investigación de un delito informático en muchas ocasiones topa con que es necesaria la visualización de una ingente cantidad de archivos que ha de realizarse por parte de un policía sentado detrás de un ordenador, con las incomodidades y posibilidades de error que ello conlleva. También la búsqueda de evidencias conlleva mucho tiempo. Cuanto mejores sean los protocolos y las herramientas más facilidades tendremos para la investigación.

   Pero son las herramientas legales, las que a mi parecer pueden dar un impulso definitivo a la lucha contra el cibercrimen. Se nos tiene que dotar de instrumentos ágiles que podamos utilizar para emplearlos en esta lucha, porque de otro modo, por mucho conocimiento que tengamos, por mucha tecnología que

hayamos desarrollado, no podremos localizar a ningún delincuente. Tendríamos un Formula I encerrado en una plaza de toros.

Aspectos que podrían modificarse:

- Definir correctamente la usurpación de personalidad. Dotarle de relevancia jurídica a estas suplantaciones consistentes en crear perfiles en redes sociales para hacer creer a la gente que es otra persona.
- Convertir en delictiva la distribución de material "sensible" aunque el mismo haya sido entregado voluntariamente por su titular.
- Aumentar la edad legal de consentimiento sexual. Se están barajando los 16 años, pero debería establecerse de forma adicional un nuevo aspecto a tener en cuenta de cara a no culpabilizar unas relaciones sexuales consentidas y debería ser la diferencia de edad entre la pareja. No es lo mismo que un menor de 15 años mantenga una relación sexual con un adulto de 18, que el mismo menor de 15 años la mantenga con un adulto de 60 años.
- Determinar como delictivo el intento de mantener contacto sexual con un menor de 16 años sin que este tenga que ser consumado.
- Regular definitivamente la figura del agente encubierto.
- Permitir como parte de las condenas que el material informático ocupado con relación a cualquier delito pueda pasar a manos de la policía para utilizarlo en sus investigaciones en un símil de lo ya permitido para los casos de narcotráfico.
- Agilizar las identificaciones de los usuarios de direcciones Ips. No es de recibo que para obtener el titular de una dirección IP haya que pedir un oficio judicial y sin embargo cualquier persona va a Tráfico y abonando unas tasas de 8.10 euros le aportan "vida y milagros" del titular de un vehículo.
- Agilizar los procedimientos de asistencia jurídica internacional.
- Crear la figura del juez especialista en Delitos Informáticos, a semejanza del Fiscal Especialista.