auna
Fundación

CUADERNOS / SOCIEDAD DE LA INFORMACIÓN 6

Los menores en la Red: comportamiento y navegación segura

Rocío Miranda de Larra
Fundación AUNA

BIBLIOTECA
Fundación AUNA

'CUADERNOS / SOCIEDAD
DE LA INFORMACIÓN'

Edita: Fundación AUNA
Obenque, 4 - 4ª planta - 28042 MADRID
Tel.: (+34) 912 137 000
Fax: (+34) 912 137 099
e-mail: fundacion@auna.es
www.fundacionauna.org

Edición y Diseño
Fundación AUNA

Impresión
OMÁN Impresores

Los menores en la Red: comportamiento y navegación segura

Rocío Miranda de Larra

Rocío Miranda de Larra es licenciada en Derecho por la Universidad Autónoma de Madrid y Master en Dirección de Empresas por la Escuela de Organización Industrial de Madrid. Ha desarrollado su carrera profesional en España y en el extranjero, ocupando puestos de responsabilidad en diversas instituciones públicas en las que se ha dedicado principalmente a la realización de actividades de prospección e investigación de mercados internacionales.

En la actualidad es gerente de proyectos de la Fundación AUNA donde coordina proyectos relacionados con las TIC principalmente en el campo de la e-Inclusión, en colaboración con Universidades e instituciones públicas y privadas.

INTRODUCCIÓN

Las Tecnologías de la Información y las Comunicaciones (TIC), y en especial Internet, se han convertido en el "territorio natural" de los más jóvenes. En el año 2005 ya hay más niños navegando que adultos. Como decía Nicholas Negroponte[1] hace ya diez años "...emerge en el paisaje digital una generación liberada de muchos viejos prejuicios. Estos niños "digitales" están libres de limitaciones tales como la situación geográfica como condición para la amistad, la colaboración, el juego o la comunidad. La tecnología digital puede ser una fuerza natural que propicie un mundo más armónico".

En efecto, Internet ofrece una oportunidad sin precedentes en la historia de la humanidad. Para niños y adolescentes en particular, Internet se ha convertido en un espacio para comunicarse, buscar información, estudiar, jugar, descubrir y crear. Pero como sucede con otras tantas cuestiones, la utilización de la Red por los menores también presenta una cara menos favorable: Internet se ha convertido en el vehículo ideal para transmitir informaciones perjudiciales para los más pequeños y para la comisión de diversos abusos.

Cualquier debate público sobre la educación de niños y jóvenes, girará en algún momento alrededor de la presencia y el papel de Internet en sus vidas y una parte importante del mismo estará centrado en las posibles ventajas y riesgos derivados de su uso. La Sociedad, y en especial padres y educadores, están preocupados por la posibilidad de que los menores y otros colectivos merecedores de especial protección, accedan a informaciones inadecuadas en la Red.

Sin embargo, aunque esas preocupaciones sean lícitas, no se debe culpar a la Red de los vicios de la Sociedad ni, menos aún, prohibir o tener una actitud excesivamente reticente hacia su uso por parte de los menores, sino, más bien, fomentar una utilización responsable de la misma. Prescindir de los logros de Internet sería hoy una pretensión imposible, porque se trata de un avance irrenunciable y un signo del progreso de nuestro tiempo.

Para impulsar un uso seguro de la Red, dos son las vías principales de actuación. Por una parte, la lucha frente a los contenidos ilícitos por medio de la Ley y las líneas de denuncia y, por otra, la protección de los menores frente a aquellos contenidos y comportamientos nocivos que, inevitablemente, van a encontrar en el ciberespacio. Para enfrentarse al primer objetivo, los gobiernos se encuentran con inquietantes obstáculos. No es fácil localizar al autor de los contenidos perniciosos puesto que se ampara en el anonimato que le brinda la Red. Además, el carácter transnacional de Internet y la ausencia de una autoridad que regule y controle los contenidos que circulan por ella, favorece la impunidad de los infractores.

Para lograr el segundo de los objetivos, los padres y educadores tienen a su disposición una serie de herramientas tecnológicas que filtran y bloquean el acceso a este tipo de contenidos. Pero estas herramientas, aunque útiles, no son suficientes; es necesario también el establecimiento de una serie de estrategias -principalmente de tipo educativo y social- que persuadan a los menores de acceder a los materiales inapropiados y les enseñen a tomar decisiones sobre su uso.

Las reflexiones que siguen a continuación tienen la intención de mostrar cuál es el comportamiento *"on-line"* de los menores –dónde van, qué ven, qué hacen o con quién hablan-, cuáles son los riesgos a los que se pueden enfrentar y qué mecanismos existen para el fomento de una "navegación" segura □

1. LOS MENORES, ¿UNA GENERACIÓN DIGITAL?

El uso de Internet y las Nuevas Tecnologías está creciendo. Según la encuesta de las TIC en los hogares elaborada por el Instituto Nacional de Estadística (INE), casi uno de cada dos hogares (48,11%) está equipado con al menos un ordenador personal y uno de cada tres (30,85%) dispone de una conexión a Internet. Además, el 13,8% tiene conexión de banda ancha, lo que supone un incremento de un 54,14% con respecto al año anterior.

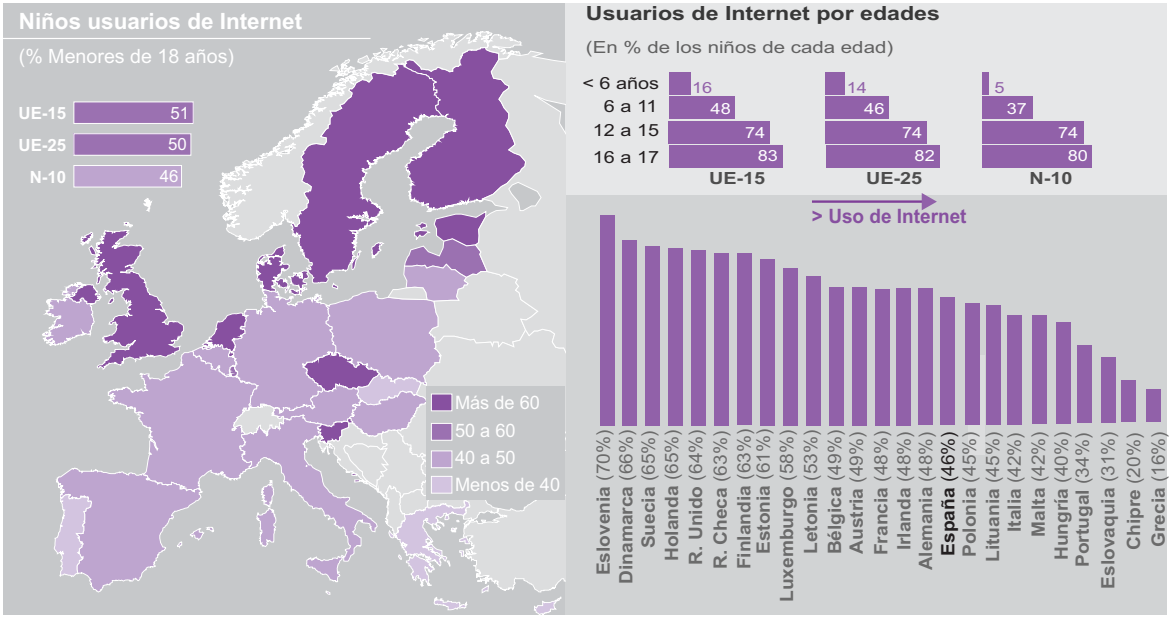
1.1. Los menores en la Red

Ahora bien, si atendemos a las edades de los usuarios, ¿cómo está distribuido ese uso entre la población? y, más concretamente, ¿qué aceptación tienen los principales recursos tecnológicos entre los menores? Se considera menor, desde el nacimiento hasta la mayoría de edad, que en España está cifrada en los 18 años. Aunque, en muchas ocasiones se utilizan indistintamente los términos "menor", "chico", "niño", "joven" o "adolescente", estos conceptos hacen referencia a distintas etapas del proceso de desarrollo. Según los últimos estudios publicados[2], en nuestro país el 66,7% de los niños de 10 a 15 años utiliza la Red, mientras que entre los jóvenes de 16 y 17 años, el porcentaje de internautas aumenta hasta un 83,9%. Estos datos ponen de manifiesto que los jóvenes son quienes hacen un mayor uso de la Red, con porcentajes muy superiores al 38,3% de media de la población española.

Otra de las fuentes que ofrecen información relativa a los niveles de acceso a Internet entre los menores es el Eurobarómetro, según el cual el porcentaje de niños españoles que accede a Internet es del 46%. A pesar de que esta cifra es sensiblemente inferior a la referida con anterioridad (incluye el intervalo de 0 a 10 años), la utilización de este indicador resulta interesante, al permitir su comparativa con los principales países de nuestro entorno. España se encuentra en la decimoquinta posición de la Europa de los 25, por debajo del promedio, situado en un 50%. En el gráfico siguiente se observa que el país con mayor porcentaje de internautas menores de edad es Eslovenia, con un 70%; seguido de Dinamarca con un 66%, siendo el último Grecia con un 16%. En Estados Unidos, las cifras de menores internautas se sitúan en torno al 85%.

Internet es ya una realidad al alcance de casi todos y el acceso a la Red es prácticamente ubicuo. Cada vez más, los niños tienen la habilidad de navegar por la Red, conducidos por la progresiva presencia de las TIC en los hogares y el creciente número de centros educativos conectados a Internet (en la actualidad el porcentaje de escuelas con conexión a Internet en España, es de un 94%[3]). Es

El uso de Internet por los menores en la Unión Europea



Fuente: Fundación AUNA a partir de Comisión Europea, Eurobarómetro

más, la existencia de niños y jóvenes en el hogar, incide directamente en la compra de equipamiento y en la contratación de servicios de Internet y de banda ancha. Este hecho tiene su explicación: el principal motivo de compra de un PC y de suscripción a Internet en las familias es la educación de los hijos.

Por otra parte, los jóvenes juegan un papel clave al iniciar a sus padres en el uso de Internet, hecho que ha sido a menudo destacado como uno de los cambios más importantes dentro de la tradicional estructura familiar: los menores son, por primera vez, quienes enseñan a los adultos, en lugar de quienes aprenden de ellos.

Penetración de los servicios TIC en hogares

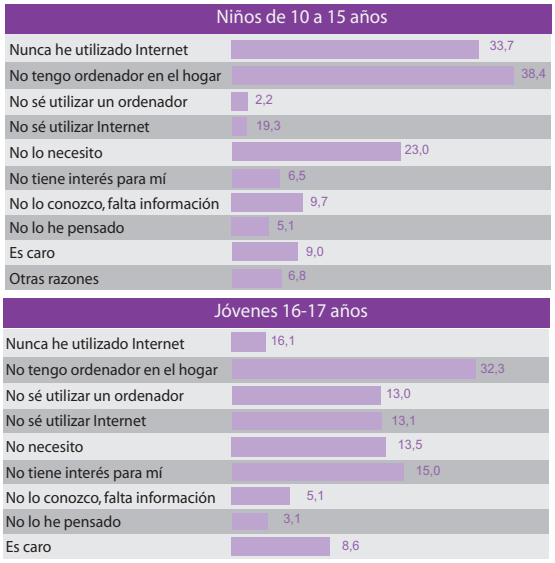
	Hogares con niños	Hogares sin niños
Ordenador sobremesa	58,5	35,6
Telefonía móvil	92,8	71,9
Internet	31,9	24,6
ADSL	**7,6**	**6,4**
Cable	**5,5**	**4,7**
TV de pago	**22,0**	**19,5**

Fuente: Fundación AUNA a partir de Red.es

Sin embargo, y a pesar de la elevada aceptación de Internet entre niños y jóvenes, todavía existe un alto porcentaje de ellos que no ha navegado por el ciberespacio, ¿Por qué?

La primera razón esgrimida es la falta de acceso desde el hogar, lo que tiene gran importancia ya que, como se verá más adelante, el domicilio particular es la primera opción elegida para navegar. Así lo han manifestado el 38,4% de los niños de entre 10 y 15 años y el 32,3% de aquellos entre 16 y 17. El segundo de los motivos es la falta de interés o de necesidad, lo que refleja una actitud de rechazo a la incorporación de Internet a los hábitos individuales y la consecuente necesidad de políticas de inclusión digital centradas en la sensibilización y la motivación.

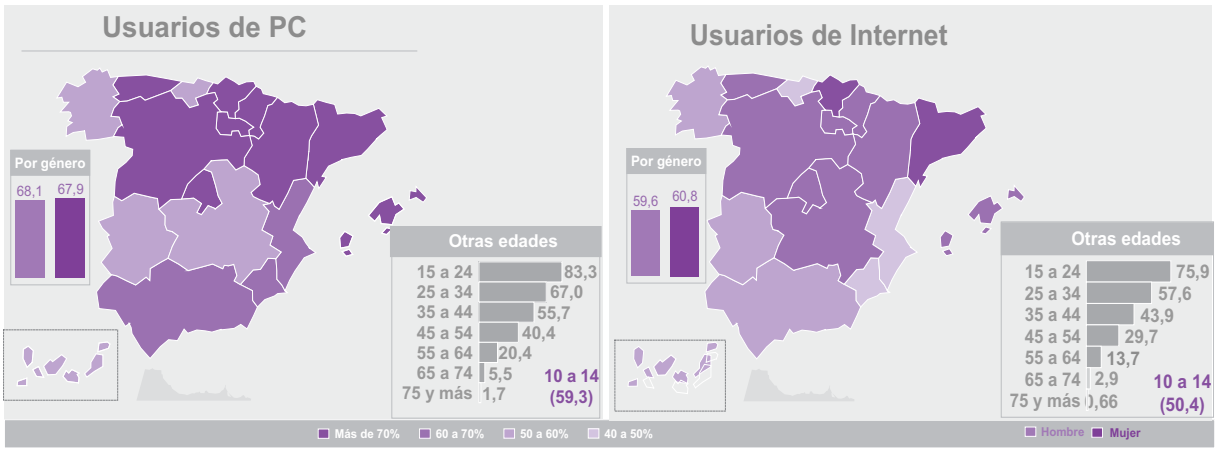
Razones por las que no se usa Internet, en %



Fuente: Fundación AUNA a partir de Red.es

Ya en nuestro país, es en Cataluña, las Islas Baleares, Madrid, Asturias y País Vasco donde se hace un uso más intensivo de Internet en términos relativos, aunque las Comunidades con mayor número de internautas en términos absolutos son Cataluña, Andalucía y Madrid. A diferencia de lo que ocurre en el resto de la población española, en la que Internet se manifiesta como un fenómeno fundamentalmente urbano, entre los menores las diferencias de acceso según el tamaño del hábitat, apenas son significativas.

El uso de las TIC por los niños en España, 2004, 10 a 14 años, en %



Fuente: Fundación AUNA a partir de INE

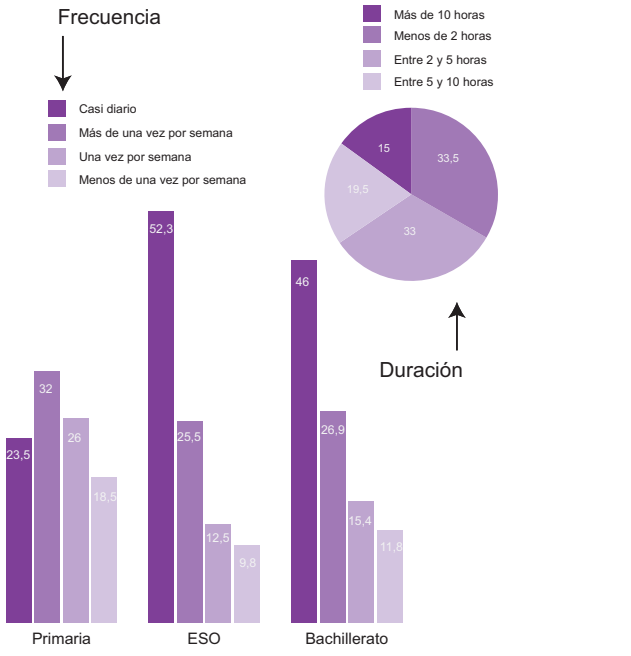
1.2. El perfil del menor internauta

Nos encontramos, por tanto, ante la primera generación que está creciendo y educándose con Internet y las cifras reflejadas hasta ahora así lo indican: se trata de una generación que realiza un uso intensivo de las Nuevas Tecnologías. Pero, ¿qué hacen los niños y adolescentes en Internet?, ¿cuánto tiempo dedican y con qué propósitos?, ¿son en efecto pioneros de la Era digital?

Un primer dato que refleja información relevante en este sentido es el lugar de acceso a Internet. Si bien las cifras difieren según la fuente que se utilice, todas coinciden en señalar que el hogar es el lugar principal de acceso, seguido muy de lejos del centro de estudios y de los lugares públicos de acceso (cibercafé, biblioteca,...). Aunque estas pautas son comunes a todos los jóvenes, existen diferencias en función de la edad y el género. Por ejemplo, las niñas acceden más desde sus hogares y apenas acuden a cibercafés y, por edades, son los jóvenes mayores de 14 años quienes hacen un mayor uso de los lugares públicos de acceso.

Una segunda cuestión de gran importancia es la frecuencia de conexión[4]. En este aspecto, se observa que casi la mitad de los menores internautas se conecta a diario (48%); otro 26,5% lo hace varias veces por semana; un 14,5% navega una vez por semana y el 10,5% restante, con menor frecuencia.

Frecuencia y duración de las conexiones en, %



Fuente: Elaboración propia a partir del Defensor del Menor

Sin embargo, a pesar de la elevada frecuencia de conexión, se trata de períodos de conexión cortos. Prácticamente las tres cuartas partes de los usuarios jóvenes, se conecta menos de 5 horas semanales (un 33,3 % se conecta menos de dos horas semanales y otro 32% entre 2 y 5 horas). Un 19,5% navega entre 5 y 10 horas, y un 15% lo hace más de 10 horas a la semana.

Las horas de conexión aumentan con la edad. En una primera etapa, los más pequeños tienen un contacto esporádico, siendo los preadolescentes quienes realizan un uso más intensivo de la Red. Así, mientras el 64% de los alumnos de Educación Primaria se conectan menos de 2 horas semanales, el 50% de los alumnos de Bachillerato lo hace más de 5 horas a la semana.

Si se analizan los datos en función del género, prácticamente no existen diferencias en cuanto a la frecuencia de las conexiones. Sin embargo, es significativa la diferencia en la duración de la mismas, ya que el porcentaje de varones que navega más de 10 horas semanales, duplica al de las mujeres (un 20% y un 10% respectivamente).

Pero la cuestión que va a ofrecer una información más relevante a la hora de analizar los patrones de navegación de los menores es el uso que éstos hacen de la Red y los servicios *on-line* que más utilizan.

Según un estudio publicado por el Defensor del Menor[5], si se pregunta a los jóvenes cuál es el objetivo principal de sus conexiones, el 36% contestará que es la comunicación, seguido del ocio y la búsqueda de información.

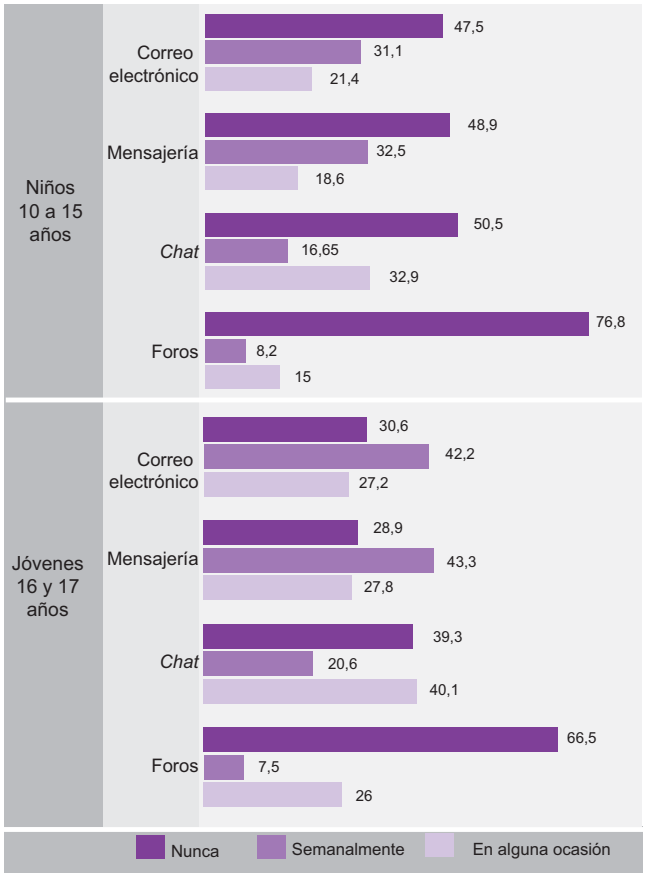
Si lo que analizamos son los servicios de Internet que más utilizan, los gráficos siguientes muestran la frecuencia de uso de los 12 servicios de Internet que cuentan con mayor aceptación entre los menores[6]. Así, se han agrupado estos servicios en tres categorías: comunicación (correo electrónico, mensajería instantánea, *chat* y foros), búsqueda de información (buscador, ayuda para el estudio y consulta de noticias) y, en tercer lugar, ocio y descargas en red (juegos, redes P2P –*peer to peer* o entre particulares-, descarga de música, de vídeo y de otro tipo de archivos).

Con carácter general, el correo electrónico, la mensajería instantánea y el buscador son los servicios más utilizados por los menores, mientras que los foros, la descarga de vídeos y la consulta de noticias son los menos utilizados. En este punto hay que destacar la elevada aceptación que ha tenido entre los jóvenes la mensajería instantánea ya

que se ha convertido, no sólo en el servicio más popular, sino en el que usan con mayor frecuencia.

En la actualidad, el 51,1% de los menores de 10 a 15 años utiliza servicios de mensajería instantánea, llegando hasta el 71,1% para los jóvenes de 16 y 17 años, superando incluso al correo electrónico y con elevadas tasas de crecimiento.

Uso de Servicios de Internet: comunicación, en %

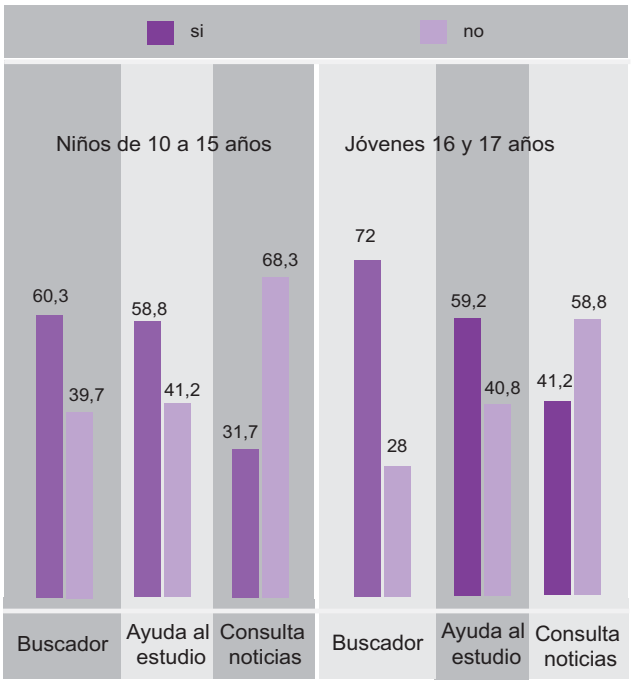


Fuente: Fundación AUNA a partir de Red.es

Llama la atención el poco uso que se hace de la Red como ayuda al estudio. Aproximadamente un 41% de los menores nunca ha utilizado Internet con esa finalidad, lo que contrasta con las opiniones de los padres.

Según éstos, las actividades principales por las que sus hijos acceden a Internet son: la búsqueda de información para estudios o trabajos con un 62,75%, seguida de la comunicación con sus amigos (33,6%) y del ocio con un 14%[7].

Uso de Servicios de Internet: búsqueda de información, en %

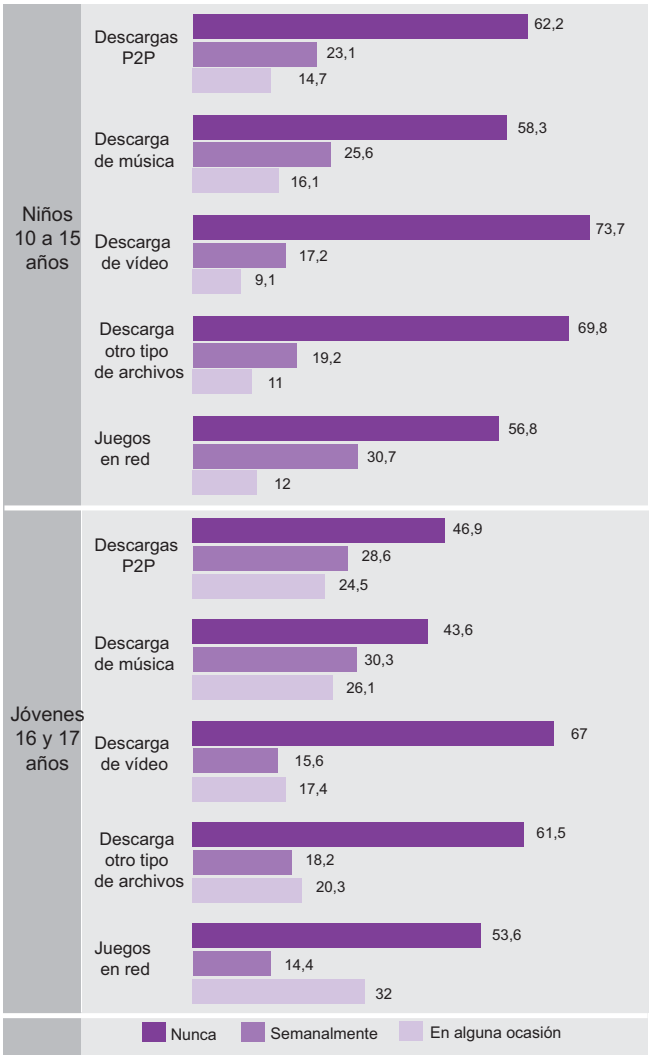


Fuente: Fundación AUNA a partir de Red.es

En cuanto a los servicios de entretenimiento y descargas de archivos, destaca, por un lado, la alta frecuencia de uso de los juegos en red – un 14,4% de los jóvenes de 16 y 17 años juega semanalmente- y, por otro, que las descargas de archivos son una actividad característica de los adolescentes (por encima de la media), ya que más de la mitad de los jóvenes ha realizado en alguna ocasión descargas de música y de archivos *P2P*.

Vemos que el uso de los juegos en los chicos duplica al uso que hacen las mujeres, mientras que ellas valoran mucho más la Red como fuente de información: un 42% de las chicas afirma que es muy importante, mientras que sólo lo hace un 28% de los chicos[8] □

Ocio y descargas en Red, en %



Fuente: Fundación AUNA a partir de Red.es

NOTAS

[1] Negroponte, N. (1995) *El mundo digital*. Barcelona: Ediciones B.

[2] Observatorio de las Telecomunicaciones y de la Sociedad de la Información. Red.es. (2005) *Infancia y Adolescencia en la SI.*

[3] EOS Gallup Europe. Flash Eurobarometre 118 (2002) *Les Responsable d´Ecole et la Societé de l´Information*.

[4] ACPI-PROTEGELES para el Defensor del Menor (2002) *Seguridad Infantil y Costumbres de los Menores en Internet.*

[5] Ver nota 4.

[6] Ver nota 2.

[7] CEACCU, Instituto Nacional de Consumo (2004?.

[8] E-business Center PricewaterhouseCoopers & IESE (2004) *Uso y actitud de los jóvenes hacia internet y la telefonía móvil.*

2. INTERNET ¿MOTIVO DE ESPERANZA O FUENTE DE PREOCUPACION?

2.1. Las claves del debate

La manera en que Internet se está convirtiendo de forma vertiginosa en una parte de nuestra vida cotidiana está planteando nuevas cuestiones acerca del acceso y las desigualdades; la naturaleza y calidad del uso, sus implicaciones en el desarrollo social y educativo de los niños y, últimamente, sobre el equilibrio entre los riesgos y las oportunidades que plantea para éstos y sus familias.

Los niños y jóvenes son vistos con ambivalencia: por un lado son percibidos como "la generación digital", pioneros en el desarrollo de las habilidades *on-line* y con unos conocimientos tecnológicos superiores a los de los adultos que les rodean y, por otro, como un colectivo vulnerable, inmersos en un crucial pero frágil proceso de desarrollo social y cognitivo, en el que los medios de comunicación, y concretamente Internet, suponen un riesgo potencial.

No cabe duda de que Internet es una herramienta potente y beneficiosa para los niños que elimina muchas de las limitaciones de tiempo y espacio que encuentran en el mundo "real". La Red amplía su acceso a la información para fines educacionales, permite el estudio en equipo, ofrece la oportunidad de contactar con otras personas sobre una variedad casi infinita de asuntos e intereses, y amplía sus círculos con conocidos y amigos *on-line.*

A pesar de ello, influidos por los medios de comunicación cuya atención se centra a menudo en los peligros y riesgos potenciales de la Red, unido a algunas experiencias personales, los padres y la sociedad en general están mostrando gran preocupación sobre los aspectos menos útiles y de seguridad que pueden resultar del uso de Internet. Mientras sólo una parte mínima del material que se puede encontrar en Internet puede ser calificado como nocivo, esa pequeñísima fracción es enormemente visible y controvertida. En efecto, la mayor parte de los contenidos no sólo no plantea problemas, sino que resultan productivos.

Aunque la definición de riesgo y los límites que de ello se deriven, incluya siempre un componente subjetivo, es cierto que el riesgo existe. Teniendo en cuenta la naturaleza de Internet y la forma en que los niños y adultos lo utilizan, es probable que algunos se hayan expuesto alguna vez a contenidos inapropiados o hayan sufrido malas experiencias. Ahora bien, también cabe preguntarse: ¿acaso no existen contenidos violentos, pornográficos o xenófobos en los medios de comunicación tradicionales? y, ¿no es posible encontrar personas poco convenientes en un parque u otro lugar público?

Por otra parte, existe una asociación fuerte y en sentido positivo entre las oportunidades y los riesgos: aumentar las oportunidades, aumenta los riesgos y por tanto, limitar el uso de Internet, disminuye, no sólo los riesgos, sino también las oportunidades. Por ello, es necesario poner los riesgos del uso de Internet en perspectiva y ofrecer una valoración equilibrada de los diferentes enfoques que pueden ayudar a los padres y otros adultos a afrontar esta cuestión de forma constructiva, en lugar de tomar medidas de tipo restrictivo o limitativo.

Internet es por lo tanto, un reto. En términos de interés nacional, la sociedad –en especial padres y educadores-, debe establecer un equilibrio entre dos prioridades: proteger a los niños y permitir su desarrollo pleno; es decir, entre oportunidades y riesgos. Sin embargo, estas prioridades a veces pueden parecer contradictorias. ¿Se puede proteger a los menores de los contenidos inapropiados sin denegarles el acceso a los contenidos educativos, válidos y atractivos?, ¿se pueden minimizar los peligros sin reducir las oportunidades? Estas cuestiones son el punto capital del dilema al que nos enfrentamos.

2.2. Riesgos y oportunidades

Como punto de partida, se debe tomar en consideración la siguiente premisa: Internet en sí mismo no es bueno ni malo, depende del uso que se haga de él.

La segunda de las ideas básicas a destacar es que Internet, además de un posible riesgo es también, y sobre todo, una oportunidad. Las oportunidades que brinda el ciberespacio son casi ilimitadas: Internet es en la actualidad un elemento clave en la educación, iguala a las clases sociales al permitir el acceso a las mismas informaciones, posibilita la interrelación con personas de otros países y culturas, sirve como herramienta integradora para los discapacitados y aumenta las posibilidades de ocio, entre otras muchas ventajas.

En tercer lugar, Internet es ya una realidad. Las cifras comentadas reflejan que se trata de una herramienta utilizada de manera habitual por los menores. Esa situación

pone de relieve que niños y mayores, y especialmente los primeros, no pueden quedarse al margen de su uso o, de lo contrario, quedarán excluidos del futuro mercado laboral, rezagados en sus estudios y aislados de una Sociedad de la Información que es ya un hecho palpable.

A continuación, y sin ánimo de establecer un listado de los riesgos y oportunidades que brinda la Red, se van mostrar las principales preocupaciones mostradas por la sociedad, que en algunos casos tienen una base sólida y, en otros, se trata de estereotipos o falsos mitos que deben ser puestos, al menos, en tela de juicio.

■ Los riesgos

Una vez analizados los motivos de acceso, la frecuencia de las conexiones y las utilidades principales de su uso, la siguiente cuestión por desvelar es ¿de dónde procede el riesgo?

Naturaleza del riesgo potencial

Origen del peligro	Fuente del daño	Naturaleza del daño	Grado de "proactividad"
Navegación por páginas *web* (www)	Contenido	Emocional o psicológico	Bajo / Alto
Servicios interactivos (*chat*, *e-mail*, mensajería instantánea, foros...)	Persona	Emocional + físico	Alto
Tiempo de navegación	Exceso tiempo de navegación	Emocional + físico (en menor escala)	Alto

Fuente: Elaboración propia

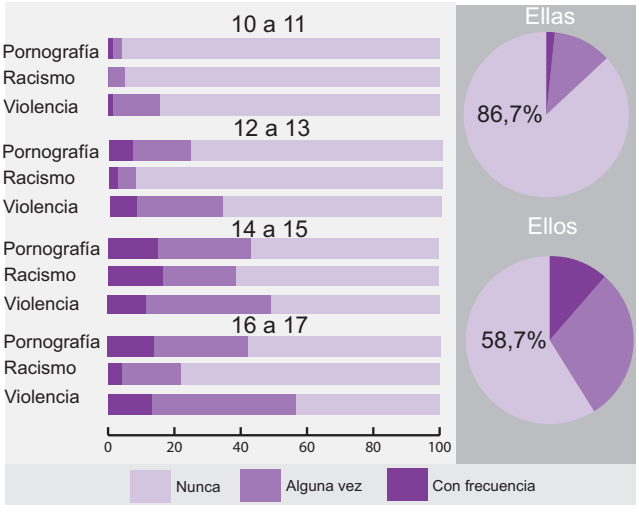
Con carácter general, los riesgos que generan mayor preocupación son los que tienen una naturaleza social, es decir, los que pueden tener un fuerte impacto en la vida social, emocional y física de los menores. Atendiendo a este factor, y a la existencia de situaciones que pueden ser constitutivas de un riesgo para el menor, se ha optado por dividir el peligro potencial en tres categorías: el riesgo procedente de la navegación por páginas *web* (el daño procede del material o contenido de la *web*); el riesgo procedente de la participación en servicios interactivos (el daño potencial reside en las personas y en el comportamiento) y los riesgos derivados del exceso de tiempo de exposición.

a.- Riesgos derivados de la navegación por la *www*

Uno de los temas más recurrentes en la literatura que relaciona a los menores con Internet es su posible exposición, de forma consciente o inconsciente, a material perjudicial y, en ocasiones peligroso, procedente de la Red. Pongamos un ejemplo: un estudiante tiene que realizar un trabajo para el colegio y al buscar determinada información, pincha en un enlace y le aparece de forma involuntaria una página con contenido inapropiado para su edad. Esta situación, o cualquiera de similares características, es una de las que más preocupan a los padres en lo que respecta al uso de Internet.

A este respecto, el estudio "Seguridad Infantil y Costumbres de los Menores en Internet", divulgado en España por el Defensor del Menor ha preguntado a menores de entre 10 y 18 años si acceden a contenidos inconvenientes y su frecuencia. Los contenidos se han dividido en tres categorías: pornográficos, violentos y racistas o xenófobos. Un 28% de los menores reconoce haber entrado en páginas de pornografía, un 38% en páginas de violencia y un 16% en páginas con contenidos racistas o xenófobos. De ellos, un 9%, un 8% y un 3% accede con frecuencia a páginas con los tres tipos de contenidos, aunque el estudio no aclara si esos accesos son intencionados.

Accesos a contenidos inconvenientes por edades y género, en %



Fuente: Fundación AUNA a partir del Defensor del Menor

Como es lógico, el acceso a este tipo de páginas aumenta con la edad. Esto se debe a dos factores fundamentales;

por un lado, a que su tiempo de navegación es mayor y, por otro, a una menor presencia de los padres u otros adultos durante sus conexiones.

Si realizamos una comparativa por género, se observa que las mujeres tienen menor curiosidad por acceder a contenidos inapropiados: sólo el 14% de las menores declara acceder a contenidos perjudiciales, mientras que en el caso de ellos, este porcentaje alcanza el 42%.

b.- Riesgos derivados de la utilización de servicios interactivos

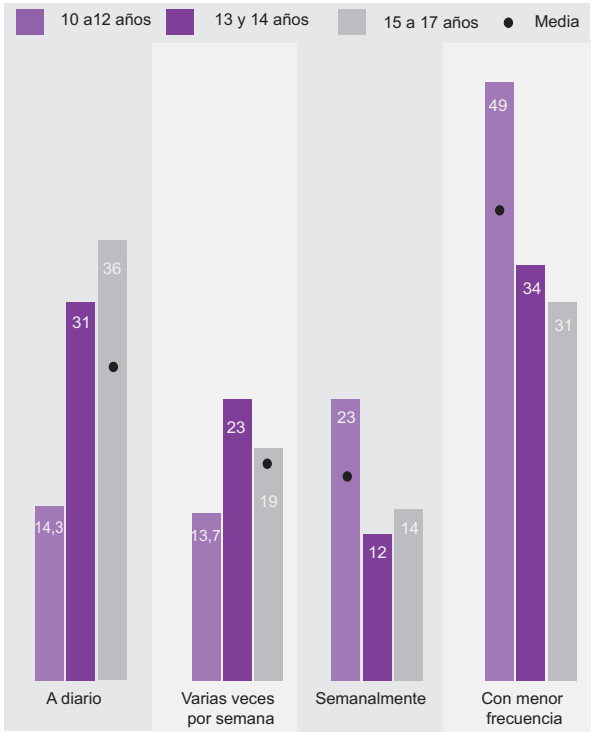
Otro de los peligros más significativos y que más expectación y ríos de tinta está haciendo correr es el potencial contacto con desconocidos: posibles pederastas o que pretendan inducir a la comisión de delitos. Existe la posibilidad de que el menor se encuentre, por ejemplo mientras "chatea", con invitaciones de personas que desean citarse con ellos, que reciban correos desagradables o sean víctimas de acoso. El peligro potencial que tiene Internet para propiciar contactos cara a cara es muy superior al que supone la mera recepción o visualización pasiva de un material, incluso aunque éste sea altamente inapropiado. Sin embargo, y aunque evidentemente estos peligros existen, como ya se ha comentado con anterioridad no son exclusivos de Internet y es posible también encontrar situaciones similares en entornos físicos.

Concretamente, una de las principales preocupaciones es el uso que los menores hacen del *chat* y los riesgos derivados de esa herramienta.

Casi la mitad de los menores (un 45%) "chatea" varias veces por semana[1], -de ellos un 27% lo hace a diario-, un 17% lo hace una vez por semana y el 38% restante con menor frecuencia. Normalmente, a medida que aumenta la edad, aumenta la frecuencia de acceso, llegando hasta un 40% el porcentaje de chicos de 15 y 16 años que "chatea" a diario.

Al entrar en un *chat* el 12% utiliza su nombre para identificarse, el 21% usa su apodo y el 67% utilizar un nombre inventado o *nick*. Este dato tiene importancia por dos razones: en primer lugar, porque facilita una primera información sobre su identidad y en segundo, porque la postura de los niños cuando alguien se dirige a ellos por su nombre es mucho más receptiva.

Frecuencia de acceso a los *chats,* en %



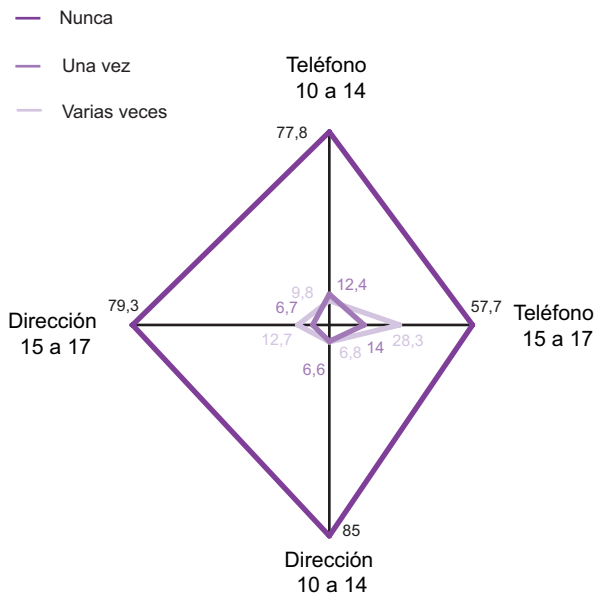
Funte. Fundación AUNA a partir del Defensor del Menor

Pero además del nombre, ¿facilitan los niños y jóvenes más datos de tipo personal? Sorprendentemente sí. Aproximadamente el 30% de los menores que utiliza Internet de manera habitual, ha facilitado su teléfono en alguna ocasión y un 16% ha dado la dirección de su domicilio. A mayor edad, mayor es el porcentaje de jóvenes que facilita sus datos personales.

Un alto porcentaje considera que ha sido víctima de acoso, si bien la definición de lo que se puede considerar "acoso" es subjetiva y varía entre las diferentes edades. Un 43,6% de los menores que navega con regularidad, se ha sentido ofendido sexualmente en Internet en alguna ocasión, aunque en niños de Primaria este nivel es sensiblemente inferior, descendiendo hasta un 15,5%.

En otros casos, las ofensas pueden tomar la forma de insultos por parte de otros internautas (11%) o de correos no solicitados con contenidos desagradables (4%). Sin embargo, a diferencia del caso anterior, el porcentaje de personas que han recibido insultos de otros internautas disminuye con la edad: un 13,5% en el caso de los alumnos de Primaria, un 11% en la ESO y un 8,5% para los alumnos de bachillerato.

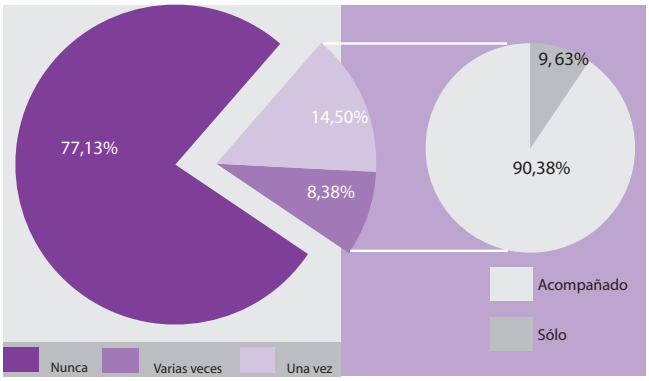
¿Has facilitado datos personales?, en %



Fuente: Fundación AUNA a partir del Defensor del Menor

Pero el dato que suscita una mayor alarma social es el porcentaje de menores que se ha citado con alguien que han conocido en Internet. En el ámbito español existen dos estudios al respecto. Según el primero de ellos[2], un 22,5% de los menores de entre 10 y 18 años ha concertado una cita con alguien a quien ha conocido a través de Internet (un 18% de las chicas y un 25% los chicos) y de ellos, un 8% lo ha hecho en más de una ocasión; el segundo de los estudios[3], sitúa esta cifra en un 17%. A pesar de esta disparidad, en cualquiera de los casos, el dato resulta preocupante si se tienen en cuenta las posibles consecuencias.

Cita con desconocidos y con quién acudió



Fuente: Fundación AUNA a partir del Defensor del Menor

Y profundizando en este tema, no menos alarmante es el siguiente hecho: un 10% de los menores, además de acudir a la cita, se presentó sólo y el 7% ni siquiera avisó a otras personas sobre su intención de acudir a la misma. Pero, una vez más, no se debe tomar este hecho como una actividad propia del uso de Internet, sino como una posible consecuencia de ello.

c.- Riesgos derivados del excesivo tiempo de uso

El sector más crítico hacia Internet denuncia la paulatina "subordinación" de los menores a la pantalla. Para éstos, la constante exposición de los menores a los medios, destruye la capacidad del niño para realizar análisis críticos de la realidad, anulando la creatividad y el pensamiento abstracto -normalmente unidos a los textos escritos-. Los sectores más pesimistas normalmente argumentan que los contenidos de estos medios son excesivamente violentos, sexistas, racistas,... y en el caso específico del ciberespacio, estiman que causa adicción y aislamiento social.

Sin embargo, frente a estos, están quienes afirman que, por el contrario, un buen uso de la Red puede potenciar las relaciones con los compañeros e incluso mejorar la comunicación entre la familia y los educadores[4]. Del mismo modo, frente a aquellos que piensan que Internet interfiere en las actividades diarias de los menores, otros opinan que una vez que los jóvenes se interesan por el uso de Internet, pasan menos tiempo viendo la TV, aumentan el tiempo de lectura de periódicos, revistas y libros y amplían el tiempo de juego fuera del hogar, debido fundamentalmente a la capacidad "multitarea" que están desarrollando.

Lo que sí es cierto es que, en general, el alto nivel de equipamiento audiovisual individualizado del que disfrutan los menores (posesión de televisión, videoconsola e incluso Internet en el dormitorio) implica una accesibilidad casi sin límites a contenidos de todo tipo sin la supervisión de un adulto. En el caso de Internet, la oferta es aún mayor, lo que unido a la falta de conocimientos sobre su uso por parte de los adultos, hace que el riesgo aumente.

Otros riesgos percibidos como riesgos potenciales de Internet y del uso de las TIC son aspectos relacionados con la salud como pérdidas de visión, problemas de espalda u obesidad que, si bien son ciertos, no son riesgos implí-

citos ni exclusivos de la Red (TV, videoconsola...), sino que dependen del buen uso que se haga de ella y, sobre todo, de la cantidad de tiempo que el menor la utilice.

■ La oportunidad educativa

A pesar de los posibles riesgos mencionados, cabe destacar que el mayor riesgo de Internet no está derivado de su uso, sino de su "no uso", ya que Internet se ha convertido en la herramienta básica de intercambio de información del siglo XXI. Por lo tanto, aquellos que no estén educados para interactuar y comunicarse con la tecnología, quedarán en clara desventaja.

Las ventajas y oportunidades que ofrece la Red de redes son evidentes. Alrededor del mundo, los usuarios jóvenes utilizan cada vez más Internet como una fuente de información, comunicación, socialización y ocio. Internet permite a los jóvenes ensanchar los puntos de vista y ofrece un acceso a la información más igualitario.

El objetivo de este informe no es realizar una enumeración de las ventajas de Internet, puesto que son de sobra conocidas. Sin embargo se ha considerado oportuno destacar una de las principales oportunidades que brinda la Red y que tiene todavía un largo camino por recorrer: la oportunidad educativa.

Una de las preguntas a este respecto es: ¿mejora el acceso a Internet el rendimiento escolar? Aunque no es fácil separar los efectos del acceso en sí mismo de otros factores, hay fuertes indicios de que el acceso a Internet desde el hogar fortalece y acelera el aprendizaje. Numerosos estudios[5] han demostrado que los estudiantes con acceso tanto en casa como en la escuela tienen mejores resultados académicos que sus compañeros con acceso únicamente desde la escuela. Otras investigaciones, como la realizada por la Universidad de Michigan, reveló que después de tener acceso desde el hogar, los estudiantes tuvieron mejores notas y, en muchos de los casos, mejoraron los tests de lectura. Además, aquellos que pasaron más tiempo conectados tuvieron mayores progresos.

Ya en nuestro país, y a pesar de que prácticamente todas las escuelas tienen acceso a Internet, muy pocas están rentabilizando al máximo ese gran potencial ilimitado integrando el ordenador en el aula. Es un hecho probado que los estudiantes con conexión a Internet en su clase, en oposición a aquellos en un lugar común, como la biblioteca o el aula de informática, muestran mayores progresos y obtienen mejores resultados.

Pero Internet puede ir mucho más allá: La Red puede ayudar a involucrar más a los padres en la escuela. Existen también investigaciones[6] en este sentido que demuestran que la implicación de los padres es un elemento esencial para los logros escolares de los alumnos. Internet es un instrumento sin igual para conectar a los padres con las actividades escolares, el aprendizaje en clase y el progreso individual del alumno.

En España una de las iniciativas más significativas es la desarrollada por el Liceo Europeo[7]. En este centro, una vez acabada la jornada escolar, los alumnos pueden resolver las dudas al instante utilizando el *e-mail*, enviar sus deberes a los profesores o solicitar más ejercicios, lo que permite un seguimiento mucho más individualizado, así como realizar trabajos en grupo con alumnos de su centro o de otros institutos. Por otra parte, los padres pueden involucrarse en la labor educativa, al recibir indicaciones sobre la mejor forma de ayudar a los alumnos, mantener un contacto mucho más directo con el profesor a través de tutorías o conversaciones en directo, pertenecer a foros, conocer las notas, las evaluaciones... y, en definitiva, implicarse en el proceso educativo de sus hijos □

NOTAS

[1] ACPI-PROTEGELES para el Defensor del Menor (2002) *Seguridad Infantil y Costumbres de los Menores en Internet.*

[2] Ver nota 1.

[3] Fundaciò Catalana per a la Recerca y Universidad de Cádiz (2004) *II estudio sobre los hábitos de uso de Internet entre jóvenes de 12 a 17 años* .

[4] National School Boards Foundation. *Safe & Smart. Research and guidelines for children´s use of the Internet.*

[5] Henry J. Kaiser Family Foundation. *Parents, Media & Public Policy.*

[6] Ver nota 4.

[7] Liceo Europeo de Madrid.

3. EL IMPACTO DE LA INFORMACIÓN DIGITAL EN LOS MENORES

Está claro que los hábitos de diversión y comportamiento de los niños no tienen nada que ver con las generaciones precedentes. Los escenarios virtuales y, sobre todo Internet, ofrecen recursos ilimitados para socializar, entretener y educar a los niños de todas las edades. En la actualidad los muñecos hablan con los niños; los libros, literalmente se leen a sí mismos; los juegos de tablero han sido reemplazados por los videojuegos y la comunicación tradicional se ha cambiado por los mensajes multimedia. Para los adolescentes, los medios de comunicación les ayudan a llenar sus lagunas de información, ofreciendo datos sobre temas que padres y profesores no están tratando. El anonimato de los medios en general, y de Internet en particular, ofrecen una vía para obtener información sobre temas comprometidos.

3.1. Internet en comparación con los medios tradicionales

Nuestro consumo de medios de comunicación está aumentando de forma constante. En los países occidentales el tiempo de exposición a los diversos medios ronda las diez horas diarias y las generaciones más jóvenes registran tasas de consumo mucho más elevadas que sus mayores. Tras la introducción de las TIC en nuestras vidas, el término medios de comunicación ha variado sustancialmente. Ya no sólo hacen referencia a los periódicos, radio y televisión, ahora incluyen también una serie de dispositivos y aplicaciones cableadas o radiofónicas. En este entorno, los jóvenes se encuentran en su hábitat natural y, desde su más tierna infancia, las TIC forman parte de su vida cotidiana.

Las investigaciones sobre los efectos de los medios de comunicación tradicionales mostraron la dificultad de establecer los efectos cognitivos, emocionales y de comportamiento sobre los niños. Por ejemplo, los contenidos con mensajes académicos y sociales han sido vinculados con una mejor preparación para el desempeño escolar y un aumento de sus comportamientos altruistas, y los programas de tipo educativo han sido asociados con una mejora en numerosas habilidades. Estas mismas cuestiones se plantean ahora sobre Internet. No obstante, a pesar de tener características comunes, Internet también tiene una serie de peculiaridades que hacen que sea diferente de los otros medios de comunicación. Por otra parte, se trata de un medio relativamente nuevo; diez años es un tiempo considerable si tenemos en cuenta la escala de los cambios tecnológicos, pero es un periodo corto si nos atenemos a la escala de los cambios sociales, económicos y legales.

Ahora bien ¿cuáles son esas características distintivas de los contenidos de la Red?

- Internet soporta conexiones de "muchos a muchos". Un usuario puede recibir información de un gran número de fuentes, pudiendo asimismo transmitir sus contenidos a un inmenso número de receptores. En los medios audiovisuales tradicionales, así como en los escritos, la información es enviada desde la estación emisora o la editorial a muchos receptores (uno a muchos). La telefonía suele ser uno a uno, aunque en la actualidad, las "*party lines*" y las llamadas "a tres" están cambiando, en parte, dicha característica.

- Internet permite un alto grado de interactividad, ya que ofrece capacidad bi-direccional entre las partes, que puede ser igualmente rica en ambas direcciones. En los medios tradicionales, el usuario es un espectador pasivo que recibe información. En Internet, el usuario es un actor que participa, se comunica, interactúa, construye y decide la naturaleza de su relación con el medio en función de sus necesidades e intereses.

- Desregulación. No existe una autoridad que regule el funcionamiento de la Red y que controle los contenidos. Por el contrario, la televisión y el teléfono operan bajo una autoridad claramente identificada.

- Carácter transnacional y alcance global. Los contenidos introducidos en la Red trascienden las fronteras de los estados y pueden ser consultados por un usuario en cualquier lugar del mundo. La naturaleza transnacional de Internet hace más complicado para un gobierno obtener el consenso necesario para imponer políticas regulatorias y, además, aunque así fuera, sus efectos dentro de un país no lo serían en los de los operadores de los *websites* extranjeros.

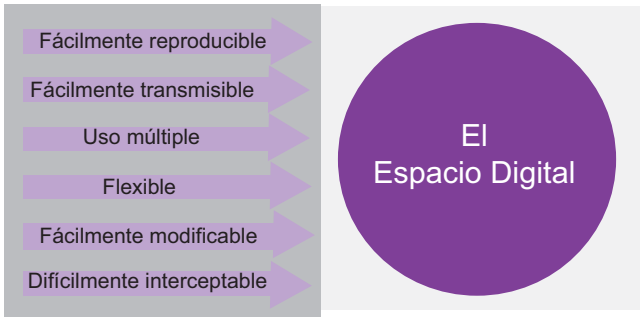
- Internet es un medio fundamentalmente anónimo en el que no es necesaria la identificación de los emisores de la información. Las aproximaciones tecnológicas para diferenciar entre menores y adultos, generalmente entrañan una pérdida de privacidad en

los segundos, quienes son legítimos usuarios de determinados materiales.

- Bajo coste de publicación. Los costes de publicar en Internet son relativamente bajos y por lo tanto cualquiera puede tener presencia en la *web* a bajo coste. Por ello, la propiedad, la utilidad e incluso la veracidad de dicha información son, en muchas ocasiones, dudosas. Por otra parte, su potencialidad en la difusión ilimitada de imágenes e informaciones, implica el riesgo de un efecto multiplicador de los abusos contra derechos, bienes e intereses jurídicos.

Todos estos rasgos distintivos hacen que la información digital sea:

Características de la Información Digital



Fuente: Elaboración propia

3.2. El impacto de los contenidos inapropiados en los menores

Una vez tratados los peligros de la Red y las características de la información que transita por ella, es necesario conocer cuál es el impacto de la misma en los menores, así como la naturaleza y alcance de las conductas o materiales inapropiados, ya que no todas van a ser merecedoras del mismo tratamiento. Es necesario definir qué conductas no se pueden tolerar, instrumentar nuevos medios para perseguir a los infractores y delimitar la responsabilidad de los actores, y para ello no sirven los criterios tradicionales. Es preciso, por tanto, elaborar nuevas respuestas que salvaguarden al mismo tiempo las libertades fundamentales - libertad de expresión, derecho a la información, derecho al secreto de las comunicaciones y a la intimidad de los ciudadanos-, y la protección de los colectivos más vulnerables, en este caso los niños.

Cuando nos preguntamos cuál es el impacto de los contenidos inapropiados en los menores, hay que tener en cuenta que los términos "impacto", "menor", y "contenidos inapropiados" son relativos y tienen diferentes implicaciones y niveles.

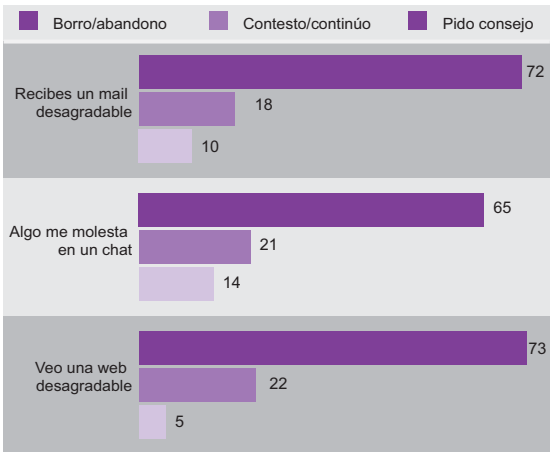
Impacto

En general, las investigaciones muestran que la exposición y uso de Internet pueden tener efectos positivos o negativos en el aprendizaje, la conducta y la salud de las personas, en función de una variedad de factores tales como el contenido del material, el tiempo de exposición, las características y personalidad del menor y el contexto de que se trate. Además, el impacto puede ser medido a corto o a largo plazo, puede ser de mayor o menor magnitud y puede ser o no ser deseable.

Pero, ¿cuál es el impacto y cómo reaccionan los niños ante una situación indeseada en la Red? En general, los jóvenes no se sienten muy angustiados por este tipo de experiencias negativas y son muy pocos los que se mantiene al margen de la Red tras una situación comprometida. Aunque la tendencia general es actuar y tomar decisiones por sí mismos, las respuestas son diferentes en función del tipo de contenido[1].

Cuando ven una página *web* o reciben información que les resulta desagradable, el 70% cambia de *web*, borra el correo o abandona el *chat*; el 20,3% navega por ella o continúa conversando y otro 9,66% lo comenta con un adulto o persona de su confianza.

Reacciones a contenidos desagradables, en %



Fuente: II Estudio sobre hábitos de Internet
Fundaciò Catalana per a la Recerça y Universidad de Cádiz

■ Menor

Se considera menor desde el nacimiento hasta los 18 años, momento en el que se alcanza la a mayoría de edad, abarcando un amplio recorrido de desarrollo. Para el tema que nos ocupa, no se pueden poner los mismos medios de protección para un niño que para un adolescente ya que sus capacidades cognitivas, sociales, emocionales y morales varían enormemente. Por otra parte, la legislación española realiza una distinción entre niño y menor castigando con penas superiores a quienes abusen de menores de 13 años.

■ Material inapropiado

Con carácter general cuando se habla de los materiales inapropiados en la Red, se hace referencia a dos tipos de contenido: por un lado a los ilícitos y, por otro, a los nocivos. Aunque en muchas ocasiones se tratan como sinónimos, es necesario aclarar que nos encontramos ante conceptos diferentes.

Son contenidos ilícitos aquellas informaciones y comportamientos considerados delitos y, como tales, merecedores de una respuesta penal. Estos están prohibidos para el conjunto de los ciudadanos, con independencia de la edad o del medio utilizado para su comisión.

Los contenidos nocivos son, sin embargo, lícitos pero considerados ofensivos o perjudiciales para el normal desarrollo de los menores. El alcance es, por tanto, mayor; mientras que los contenidos nocivos no tienen por qué ser ilícitos, los ilícitos, por definición, están incluidos dentro de los nocivos.

Si bien existe cierto consenso entre los Estados occidentales acerca de los comportamientos o informaciones delictivas (difusión de pornografía infantil, de contenidos racistas o xenófobos, la apología de terrorismo,...), no existe tal aquiescencia para los nocivos. Estos están basados en concepciones difíciles de medir en una "aldea global" ya que dependen de valores culturales, sociales, religiosos y morales. Por ejemplo, la pornografía infantil es un contenido prohibido para el conjunto de la sociedad. Sin embargo la pornografía, lícita para adultos al menos en los países occidentales puede, presumiblemente, producir determinados efectos perjudiciales para el normal desarrollo de algunos menores. En el primer caso nos encontramos ante un contenido ilícito, y que por tanto entra en el ámbito de la ley vigente en cada Estado y, en el segundo, ante uno nocivo y perteneciente al ámbito de la moral □

NOTAS

[1] Fundaciò Catalana per a la Recerca y Universidad de Cádiz (2004) *II estudio sobre los hábitos de uso de Internet entre jóvenes de 12 a 17 años*.

4. LA LUCHA FRENTE A LOS CONTENIDOS ILICITOS

La distinción entre los contenidos ilícitos y los nocivos o indeseados nos va a permitir realizar una clasificación de las medidas que deben ser adoptadas para fomentar un ciberespacio más seguro. Ambos tipos de contenido persiguen objetivos diferentes, plantean problemas distintos y, por lo tanto, exigen soluciones *ad-hoc.*

Medidas para fomentar un uso seguro de la Red

Fuente: Elaboración propia

Para hacer frente a los contenidos ilícitos, se utilizará la legislación vigente y los canales de denuncia tanto policiales como civiles. En este caso, lo que se pretende es eliminar los contenidos de la circulación, detener a los infractores y llevarlos ante la justicia.

En el caso de los contenidos nocivos, el objetivo está limitado a evitar que los menores encuentren materiales indeseados o que puedan afectar a su normal desarrollo. Las estrategias serán, por tanto, de tipo preventivo, refiriéndonos fundamentalmente a soluciones de tipo tecnológico, educativo y social.

4.1. La protección legal de los menores: valores jurídicos implicados

Internet se ha convertido en otra vía para atacar valores jurídicos protegidos: la libertad e indemnidad sexual de los menores, el derecho al honor, a la intimidad personal y familiar, a la propia imagen, a la dignidad humana, a la seguridad nacional o al orden público. Son, todos ellos, valores susceptibles de ser atacados fuera de la Red, pero que se presentan especialmente vulnerables ante las peculiares características de la misma.

La propia Comisión Europea[1] define los contenidos y comportamientos ilícitos como "aquellos susceptibles de entrar bajo el ámbito de aplicación de las normas de los estados miembros". Según esta definición, son ilícitas las conductas tipificadas en la legislación española, si bien ni el Código Civil ni el Código Penal en nuestro país contienen un título específico para lo que conocemos como "delitos informáticos".

Ante esta situación, en algunos casos se dictan leyes específicas (ej. la Ley de Comercio Electrónico), en otros se adapta la legislación para hacer frente al problema concreto (art. 189 del Código Penal sobre pornografía infantil) y, en otros, simplemente se aplican las leyes existentes.

Hemos realizado una clasificación de los delitos más comunes realizados al amparo de la Red, en función del bien jurídico que vulneran. Hay que destacar, en cualquier caso, que se trata de delitos que ya existían en el mundo "analógico", aunque cometidos mediante la utilización de medios informáticos. En la columna de la izquierda se encuentran aquellos que pueden tener una mayor incidencia en los menores, tanto por estar éstos directamente implicados, como por las consecuencias especialmente negativas que les pudieran causar y, a la derecha, los que afectan a la sociedad en general.

Los delitos que más están preocupando a los Gobiernos y a la Sociedad en general, tanto por la frecuencia con la que son cometidos como por las especiales dimensiones que alcanzan en la Red, son aquellos que guardan relación con la pornografía infantil. Según datos de INTERPOL, la pornografía infantil supone el 50% de los delitos que se cometen en Internet a nivel mundial. Por otra parte, más de cuatro millones de sitios en la Red permiten acceder a pornografía infantil y cada día se crean cerca de 500[2]. De ellos, la mitad son de pago, de lo que se deduce que el comercio de material pornográfico infantil mueve al año miles de millones de euros.

Por ello, y a pesar de que el delito de pornografía infantil ya estaba tipificado en la legislación española, el Código Penal español ha sido modificado con el fin de adaptarse a las nuevas necesidades que plantea Internet.

Delitos informáticos según el bien jurídico que vulneran

PROTECCIÓN DE LA JUVENTUD Y LA INFANCIA	**PROTECCIÓN DE LA PRIVACIDAD Y AL SECRETO DE LAS COMUNICACIONES**
- Pornografía infantil. - Captación y tráfico de menores. - Amenazas o acoso y hostigamiento a menores. - El acoso escollar o *bullying.*	- Obtención ilícita de datos personales. - Interceptación de correos electrónicos.
PROTECCIÓN DE LA DIGNIDAD HUMANA	**SEGURIDAD DE LA INFORMACIÓN**
- Propagación de los materiales que inciten al odio, racismo, antisemitismo u otro tipo de discriminación en función del sexo, religión, origen, orientación sexual. - Propagación de materiales y discursos con violencia extrema o sangre desmesurada *(gore)*. - Incitación al suicidio. - Apología de la anorexia.	- Accesos no autorizados o *hacking.* - Envío de virus informáticos.
	SEGURIDAD NACIONAL
	- Actividades terroristas. - Instrucciones sobre preparación de bombas. - Producción y venta de drogas a través de la Red.
DERECHO AL HONOR, A LA INTIMIDAD O A LA IMAGEN PROPIA	**PROTECCIÓN DEL MERCADO, CONSUMIDORES Y SEGURIDAD ECONÓMICA**
- La difamación en Internet. - La transmisión no autorizada de datos. - El envío de correo no autorizado o *spam.*	- Estafas electrónicas. - Fraudes informáticos. - Falsificaciones documentales.
	PROPIEDAD INTELECTUAL
	- Distribución no autorizada de obras registradas. - Copia ilegal.

Fuente: Elaboración propia

La Ley Orgánica 15/2003 modificó el artículo 189 del Código Penal que regula las actividades relacionadas con la pornografía infantil con fines exhibicionistas o para su difusión por medios públicos. La nueva ley, que entró en vigor en octubre de 2004, introduce dos modificaciones importantes. Por primera vez en España se contempla como delito la posesión de material pornográfico en cuya elaboración haya sido utilizado un menor de 18 años. Por otra parte, se incluye entre dichos delitos la "pseudo-pornografía", es decir la producción o difusión de material pornográfico en el que no se haya utilizado directamente a un menor, pero se emplee su imagen o voz alterada o modificada –fotomontajes, superposición y distorsión de imágenes o *morphing*-, a través de las Nuevas Tecnologías.

Así pues, el artículo 189, además del acto punible (agresión o abuso sexual del menor), incluye todos los "momentos informativos" por los que pasa el mensaje desde que es creado hasta que llega al receptor: la creación (utilización de menores para la elaboración de material pornográfico), la difusión (producción, venta, distribución, exhibición y difusión o exhibición por cualquier medio), la recepción y la mera tenencia.

España, además de su legislación nacional, como país miembro de la Unión Europea, debe tomar las medidas pertinentes para incorporar a su legislación la normativa europea que recomienda la inclusión de los crímenes de racismo, xenofobia, apología de la violencia y del terrorismo y la discriminación racial en Internet, en el marco del Convenio sobre Ciberdelincuencia firmado por nuestro país en 2001, pero no ratificado. Este convenio constituye el primer tratado internacional sobre delitos cometidos vía Internet y otras tecnologías de última generación.

El carácter transnacional de la Red, la ausencia de regulación y la existencia de una serie de "prestadores de servicios" con diferentes roles técnicos, hacen que la

aplicación de la ley plantee diversos problemas, que se comentan a continuación de manera sucinta:

- La dificultad de determinar la **responsabilidad de los "actores intermediarios"** con diferentes roles técnicos (proveedor de red, proveedor de acceso, proveedor de servicio...). España no cuenta con legislación específica que determine el alcance de la responsabilidad de los intermediarios por los delitos cometidos por sus clientes, por lo que les resulta de aplicación el Régimen General Civil y Penal.

  En función de la ley española, los operadores de Telecomunicaciones y los proveedores de acceso a Internet quedan exentos de responsabilidad siempre que su actuación se limite a servir de mero transporte de la información, sin modificarla ni elegir el punto de origen o de destino. Por su parte, los proveedores de alojamiento de contenidos (de sitios *web*, operadores de grupos de discusión o grupos de noticias, buscadores o portales), deberán cumplir con una obligación de diligencia y no se les considera responsables por los contenidos ilícitos introducidos por sus usuarios a no ser que tengan conocimiento de la actividad delictiva u ofensiva, en cuyo caso están obligados a retirar dicha información.

- **La necesidad de una cooperación internacional.** La aplicación del derecho nacional a actuaciones realizadas en una red planetaria sin "localización" geográfica, plantea numerosos problemas de jurisdicción. Las respuestas nacionales no bastan para combatir los contenidos ilícitos que proceden de diferentes países. El carácter transnacional de estas conductas hace más difícil su descubrimiento, prevención y castigo, ya que incluso en los casos en que puedan ser detectadas, pueden plantearse conflictos sobre la jurisdicción sancionadora competente. Esta problemática se agudiza cuando los diferentes elementos de la cadena se hallan en países distintos con legislaciones, a su vez, diferentes.

  Por ello, es imprescindible una armonización entre legislaciones y una cooperación entre las autoridades judiciales y policiales de los estados afectados. Numerosos organismos internacionales como el Consejo de Europa, la ONU o la OCDE están publicando diversos textos en los que se dictan las pautas de actuación en este sentido. Igualmente importante es la cooperación entre las policías nacionales. Para ello se han creado, dentro de los organismos policiales internacionales como EUROPOL o INTERPOL, departamentos especializados en la persecución de este tipo de delitos.

- **Colisión de derechos.** Con carácter general, la regulación de los contenidos nocivos reclama una respuesta global que compatibilice la necesidad de proteger a los menores respecto de esos materiales ilícitos y la salvaguarda de las libertades fundamentales (derecho a la libertad de expresión, derecho a la libertad de información y derecho a la protección de la intimidad y a la privacidad de las comunicaciones).

  La Constitución Española establece en su artículo 20.4 una limitación a la libertad de expresión cuando ésta entra en colisión con otros derechos como los relativos al honor, a la intimidad y a la propia imagen o a la protección de la juventud y de la infancia. Eso sí, a la hora de tomar medidas que conculquen esos derechos, es necesario utilizar el "principio de proporcionalidad", aplicando únicamente aquellas medidas que sean imprescindibles, menos restrictivas y adecuadas al fin propuesto.

4.2. Las medidas policiales

En España se han creado dos departamentos policiales especializados en la vigilancia de los sistemas informáticos y la investigación y persecución de los delitos informáticos.

- El **Grupo de Delitos Telemáticos** es el encargado de centralizar dentro de la Unidad Central Operativa de Policía Judicial de la Guardia Civil, todos los esfuerzos para la investigación y persecución de los delitos que se sirven de Internet o de las Nuevas Tecnologías para su comisión. Para comunicar la existencia de contenidos ilícitos, han habilitado un formulario en la siguiente dirección: http://www.guardiacivil.es/telematicos/formulario.jsp

- La Policía Nacional tiene así mismo una **Brigada de Investigación Tecnológica (BIT)**, con una unidad específica destinada a la protección del menor, que se encarga de recibir las denuncias sobre delitos informáticos. Éstas se pueden realizar en las siguientes direcciones: Delitos.tecnologicos@policia.es, Denuncias.pornografia.infantil@policia.es.

4.3. Las líneas directas civiles

Las líneas directas permiten a los ciudadanos denunciar los contenidos ilícitos que circulan por Internet. Estas líneas transmiten la información a la instancia pertinente para que tome las medidas oportunas. Son complementarias a las policiales y tienen una función diferente , ya que ni persiguen ni detienen a los delincuentes, sino que aseguran la cobertura y el intercambio de denuncias relativas a los principales tipos de contenidos ilícitos.

En España, la página *web* de la institución PROTEGELES (www.protegeles.com) dispone de una línea de denuncia para que los usuarios comuniquen la existencia de contenidos de pornografía infantil, terrorismo, drogas o racismo.

Una opción aún por implementar en este terreno, y que no ha sido puesta en práctica en ningún país, es la posibilidad de complementar las líneas de denuncia con la provisión de ayuda o asistencia inmediata al menor. A través de esta vía se podría reducir el impacto negativo sobre el menor, a la vez que se educa a los niños sobre la mejor manera de evitar el material o las experiencias inapropiadas en un futuro.

El principal problema de poner en práctica esta medida es su elevado coste, ya que para funcione correctamente, en términos de capacidad y rapidez de respuesta, sería necesario desplegar una importante infraestructura humana □

NOTAS

[1] Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones sobre contenidos ilícitos y nocivos en Internet. COM (96) 487 Final, de 16 de octubre de 1996 (DO C 70, de 6 de marzo de 1997)

[2] ECPAT-UNICEF.

5. LA PROTECCIÓN FRENTE A LOS CONTENIDOS NOCIVOS

Mantener a los menores a salvo de los peligros de la Red no es tarea fácil. Además de luchar frente a las conductas y contenidos ilícitos, es preciso adoptar una serie de medidas que les protejan, a la vez que se respeta su necesidad de libertad y su avidez de conocimientos. Sin embargo, cualquiera de estas medidas (ya sean de tipo tecnológico, educativo o social) tiene costes y beneficios y su aplicación va a depender de aspectos como la edad o las características del menor. Encontrar el equilibrio entre intereses no es sencillo: mayores costes pueden estar justificados si el daño presumible es grande o muy probable, o, si están implicados niños de edades tempranas, más que adolescentes. Por otra parte, los diferentes fines institucionales también deben ser tenidos en cuenta. Por ejemplo, el propósito principal de un colegio es la enseñanza, mientras que el de una biblioteca es ofrecer información a toda la comunidad; ambos tienen diferentes necesidades y por lo tanto deberán adoptar diferentes soluciones.

5.1. Las herramientas basadas en la tecnología

Consisten en dispositivos tecnológicos o *software* que pueden ayudar a reducir la exposición de los menores a los materiales o conductas inapropiados en la Red. Las más importantes son:

Herramientas tecnológicas

TIPO DE HERRAMIENTA	FUNCIÓN	OPCIONES	PRINCIPAL DESVENTAJA
FILTRO DE CONTENIDOS	Bloquea el acceso al material predeterminado. Generalmente son páginas *web* aunque también puede limitar otras funciones: *chat*, *e-mail*, tiempo de navegación.	Basado en el contenido (listas blancas y negras), en el reconocimiento de textos, el análisis de imágenes o en el etiquetado.	Sobrebloqueo e infrabloqueo. Restricciones en el flujo de información. Costes psicológicos.
MONITORIZACIÓN	Registra los comportamientos del menor en la Red, permitiendo realizar un rastreo de las páginas visitadas y del tiempo de navegación.	Individual/colectiva Abierta/encubierta.	No es recomendable para niños de edades tempranas ya que no limita el acceso a contenidos inapropiados. Pérdida de privacidad.
CONTROL DE *SPAM*	Evita que el correo electrónicio no deseado llegue al destinatario.	Basado en el contenido (listas blancas y negras), en la fuente o en el receptor.	Sobrebloqueo e infrabloqueo. Restricciones en el flujo de información.

Fuente: Elaboracion propia

Estas herramientas han ganado mucho en eficacia en los últimos años y gozan de gran aceptación entre los usuarios pero, para que su funcionamiento y rendimiento sean óptimos, es necesario tener en cuenta una serie de consideraciones previas:

- **La tecnología no es infalible**. Las herramientas tecnológicas no son perfectas y, además, son susceptibles de ser "pirateadas". Lo que la tecnología puede hacer es instalar barreras que dificulten el acceso a los materiales no deseados, pero aquellos que realmente quieran acceder a dichos contenidos, pueden encontrar la manera de hacerlo, máxime si tenemos en cuenta la cantidad y variedad de puntos de acceso.

- **No debe recaer en ellas la totalidad de la responsabilidad**. Es necesario compatibilizar su uso con otro tipo de estrategias, fundamentalmente de tipo educativo, ya que en caso de que la tecnología falle, el menor que haya sido "protegido" únicamente por estas herramientas, no tendrá las capacidades necesarias para actuar adecuadamente ante estos contenidos. La ventaja de la tecnología es que avanza y se desarrolla con más facilidad de lo que lo hacen los cambios en las estrategias sociales y educativas.

- **Las herramientas deben ser fáciles de usar.** La facilidad de uso es uno de los factores principales en la implementación de cualquier herramienta tecnológica. Éstas no ofrecerán una protección efectiva si son tan difíciles de manejar, que al final no se usan o no se usan correctamente.

- **Deben permitir la adaptación a las preferencias del usuario**. Para que sean plenamente efectivas, deben permitir un cierto grado de personalización. No todas la herramientas son apropiadas para todos los usuarios; dependerá, en la mayoría de los casos, de la madurez, la edad y las características del menor. En muchas ocasiones flexibilidad y facilidad de uso parecen opciones contrapuestas. La industria debe realizar un esfuerzo para ofrecer productos escalables y compatibles con las necesidades de información de aquellos que no tengan conocimientos informáticos.

■ Los filtros de contenido

Es la más común de las herramientas tecnológicas de protección. Los filtros permiten al usuario decidir cuáles son los contenidos de Internet que considera inapropiados y, en función de ello, disponer a qué páginas *web* se puede acceder y, sobre todo, a cuáles no. Además, la gran mayoría de filtros comerciales ofrece una serie de servicios adicionales, entre los que destacan:

- Denegar el acceso a algunos **servicios de Internet** (ej. servicios interactivos: *chats*, descargas de documentos, conexiones *P2P*, comercio electrónico...).

- Bloquear la **información saliente** (ej. Números de teléfono, datos personales, etc.).

- **Limitar el tiempo** de conexión, incluso determinando el número de horas diario o semanal de navegación.

- Mantener un **registro** de las tentativas de acceso a los materiales inapropiados.

- Bloquear el acceso a Internet en función del número de intentos repetidos a páginas no permitidas.

- Establecer distintos **perfiles de usuario.**

Existen multitud de filtros comerciales: *CyberPatrol*, *CyberSitter, Net Nanny, Smartfilter, Surfcontrol* o el español Optenet, de fácil instalación y a precios asequibles[1]. Estos filtros se instalan en el PC del usuario y no tienen un coste elevado. La única diferencia es que la desinstalación "oficial" solo puede ser realizada por la persona autorizada.

Pero, además del *software* comercial, existen otros mecanismos para realizar esta función. La mayoría de los navegadores de Internet[2] de uso común, como *Internet Explorer o Netscape*, incluyen un "asesor de contenido" que permite el filtrado de contenidos de manera gratuita y sin que sea necesario incorporar tecnología adicional, aunque ofrecen menores prestaciones que las herramientas comerciales.

A pesar de la eficiencia de los sistemas tecnológicos, en nuestro país únicamente el 14% de los menores accede a Internet desde ordenadores que disponen de sistemas de filtrado[3]. Sin embargo, a juzgar por los niveles de uso de EE.UU., esta tecnología tiene grandes perspectivas de crecimiento ya que más de la mitad (el 54%) de las familias norteamericanas con adolescentes conectadas a Internet, utiliza filtros, y su crecimiento en los últimos cuatro años ha sido de un 65%[4].

a.- ¿Cuál es el funcionamiento los filtros?

El filtrado puede hacerse por varias vías:

Filtrado por contenido.- La clasificación de los contenidos se puede realizar estableciendo las denominadas "listas negras" y "listas blancas".

Las **"listas negras**" son listados de recursos que han sido catalogados como inapropiados, impidiendo el filtro el acceso a estas páginas *web*.

Las **"listas blancas",** son listas de páginas *web* que han sido catalogadas como apropiadas, siendo éstas las únicas a las que el usuario tiene acceso.

Filtrado por el análisis semántico.- La manera más rudimentaria y básica de análisis es comparar cada palabra de un determinado texto con un listado de vocablos asociados con contenidos inapropiados. Cuando estas palabras son encontradas, el acceso es bloqueado, y la *web* clasificada para su inserción en una lista negra. El problema de este sistema es la existencia de multitud de palabras polisémicas o con diferentes interpretaciones en función del contexto. Por eso, las tendencias futuras apuntan hacia la interpretación de textos y grupos de palabras.

Filtrado por el análisis de la imagen.- Esta técnica se utiliza sobre todo para el análisis de las páginas relacionadas con la pornografía. Los ordenadores reconocen una imagen (ej. una persona desnuda) analizando la información procedente de los píxeles (contraste, color...). El problema es que no distingue si se trata de un adulto o un menor, ni su contexto. Además, no es inusual que se bloqueen también otras imágenes con características similares.

Filtrado por el etiquetado o la calificación moral de los contenidos.- Este es el sistema más utilizado en la actualidad y el recomendado por la Unión Europea. El más común de estos sistemas es el mecanismo de filtrados PICS (Plataforma para la Selección de Contenidos de Internet) desarrollado por el consorcio 3W[5]. Todas las páginas *web* tienen asociada una información que describe varias características de la misma y que suele estar oculta al usuario. El sistema PICS clasifica esa información en una serie de categorías, subcategorías y niveles dentro de

aquellas, que pueden usarse para clasificar contenidos y funcionaría de forma análoga a la calificación de las películas o videojuegos.

Este sistema también tiene sus inconvenientes. En primer lugar, por la dificultad que entraña etiquetar o clasificar *a priori* un espacio que se actualiza en tiempo real y que, además, como ya se ha comentado, no está regulado. Por otra parte, si el etiquetado es ejercido por los propios proveedores de contenidos (autorregulación), no se puede garantizar su fiabilidad hasta que no exista una legislación de obligado cumplimiento para todos aquellos que participen colgando información en Internet (en páginas *web*, foros de discusión, salas de *chat*, etc.). En el caso de que el etiquetado sea realizado por terceros, volverán a existir los problemas de subjetividad y de posible restricción de derechos fundamentales.

b.- Flexibilidad del producto

Con el fin de adaptarlos a las necesidades del usuario (en función de las distintas edades, contextos...), los filtros suelen ofrecer un cierto grado de personalización, permitiendo flexibilizaciones en diversas dimensiones:

Cambios en los criterios usados para el bloqueo. Si un programa de filtrado bloquea un *site* por error, o el administrador (padre, profesor,...) considera que alguna de las clasificaciones no es adecuada, puede crear una lista de excepciones que prevalece sobre las listas establecidas "por defecto".

Escalabilidad de las categorías de los contenidos. Generalmente los contenidos inapropiados están divididos en diferentes categorías (pornografía, terrorismo, violencia, armas, sectas...), subcategorías y niveles, de manera que ofrecen al administrador del sistema la posibilidad de aceptar o bloquear los contenidos por categoría en función de las características del usuario.

Configuración de perfiles de filtrado individuales. En una casa pueden vivir varios chicos de diferentes edades. A través de la creación de perfiles, el menor se registrará en el sistema y el filtro identificará sus coordenadas.

c.- Principales problemas asociados a los filtros

Fallos de funcionamiento.- Normalmente los filtros adolecen de dos tipos de error, que prácticamente son inherentes a los mismos: por exceso o "sobrebloqueo", que se produce cuando una página que es apropiada es filtrada; o por defecto o "infrabloqueo", que ocurre cuando una página que es inapropiada, aparece en la pantalla del usuario. Las principales fuentes de error son las siguientes:

Tipo de error y fuente

INFRABLOQUEO	SOBREBLOQUEO
Renovación y actualización constante de la *web*.	Renovación y actualización constante de la *web*.
Imperfección de los algoritmos (ej. el nacimiento de nuevas palabras y jergas evitan el filtrado basado en el reconocimiento de textos.	Existencia en una misma *web* de contenidos apropiados o inapropiados. Si el filtro no es capaz de separarlos, bloqueará la página entera.
Utilización de técnicas por los "proveedores de contenidos ilícitos". Ej.: utilización de palabras parecidas (eg. Pedrerastia) para eludir los sistemas basados en el reconocimiento de palabras o utilización de personas semi-vestidas en el caso del filtrado basado en el reconocimiento de imágenes.	Ambigüedad de textos e imágenes. la definición de lo que puede ser bloqueado depende del juicio humano y ante la duda, los proveedores de filtros tienden a bloquear la información ambigua.

Fuente: Elaboración propia

Restricciones en el flujo de información.- Como se ha visto, una parte del material incluido en algunas de las categorías incluidas en las listas de bloqueo, no son ilícitas y en algunos casos no son ni siquiera nocivas. El "*sobrebloqueo"* no supone un problema legal en el entorno doméstico, pero sí puede suponerlo en instituciones públicas por atentar contra principios recogidos en la Constitución: libertad de expresión, no discriminación, etc.

Costes psicológicos.- Otro de los principales costes de los filtros, es que su uso reduce las oportunidades de los jóvenes de tomar decisiones responsables por su cuenta. De ahí que deba ser un complemento, pero no un sustituto de la supervisión de los adultos.

El segundo de los costes psicológicos, según palabras de los propios menores, es que su instalación puede generar desconfianza en la relación paterno-filial. Finalmente, y precisamente porque los filtros prohíben, pueden hacer de los materiales inapropiados un reto que alcanzar y una norma que transgredir.

d.- ¿Cuál es el futuro de los filtros?

Ya hemos visto que todos los métodos descritos tienen sus inconvenientes. Sin embargo, en cada uno de ellos, la fuente del error es diferente. El método que se está implementando para aminorar ese nivel de error, está basado en una combinación de los diferentes sistemas. Por ejemplo, si el análisis de la imagen indica una alta probabilidad de que aparezca una persona desnuda, pero el análisis semántico no indica la existencia de vocabulario asociado a una página para adultos, el dominio de la *web* es ".gov" y la información de la página indica que se trata de un museo, el filtro no actuará bloqueando dicha dirección.

Otra de las líneas en las que se está trabajando en el terreno del análisis de la imagen es la llamada "degradación selectiva del servicio". Consiste en bajar la resolución visual de las imágenes consideradas nocivas, de manera que se reduce también el impacto negativo en el menor.

Para el análisis por reconocimiento de palabras clave, las tendencias futuras apuntan hacia la interpretación del texto en su conjunto, tomando en cuenta tanto las características como la frecuencia de diversas palabras, el análisis de combinaciones de palabras y otros parámetros estadísticos del texto.

■ La monitorización

La monitorización es otra opción basada en la tecnología que se ha propuesto en muchas ocasiones como alternativa a los filtros. Estas herramientas registran los comportamientos del menor en la Red, permitiendo realizar un rastreo de las páginas visitadas y del tiempo de navegación.

Muchas opciones basadas en la monitorización son accesibles (visualización en tiempo real y en remoto de la pantalla del menor, registro de las pulsaciones o grabación de las páginas *web*) y cada una de estas opciones pueden ser usada a su vez de una manera abierta o encubierta.

Si se considera que el objetivo no es limitar el uso de Internet, sino el fomento de una navegación responsable, la mayor ventaja de la monitorización sobre los filtros es que deja al menor el control de sus experiencias en Internet. Pero, precisamente por ello, el acceso al material inapropiado es posible, siendo, por ello, necesario complementarla con estrategias educativas y resultando menos adecuada para los niños cuya capacidad de decisión aún no ha madurado.

Los métodos tecnológicos para la monitorización son muy variados:

- La forma más simple se puede encontrar en los navegadores de Internet, sin que sea necesario, por tanto, incorporar tecnología adicional. Los principales navegadores tienen un "histórico" o historial de archivos que indica los lugares de Internet visitados recientemente[6] y que puede ser revistado por un adulto. También los navegadores tienen una "caché" temporal, con las imágenes que se hayan desplegado. Otra tercera fórmula son las *"cookies"* que indican las páginas con las que el usuario ha interactuado, así como quién ha recibido información del menor. El problema de estas técnicas es que algunos menores pueden tener suficientes conocimientos para borrar los historiales.

- Los sistemas de monitorización a la venta, ofrecen además otras funciones:

  La grabación de cada uno de los movimientos del menor, permitiendo registrar y revisar el *e-mail* entrante y saliente, los diálogos de los *chats* y la mensajería instantánea, accesos a páginas *web*, etc.

  La configuración del puesto de trabajo del supervisor, de forma que en su pantalla aparezcan, en tiempo real, los contenidos visualizados por el menor.

a.- ¿Cómo funciona la monitorización y cuál es su nivel de flexibilidad?

Los mecanismos para identificar el material apropiado son los mismos que ya se han analizado para los filtros: análisis semántico, de texto, por contenidos, etc., y al igual que en ese caso, la mayoría ofrece cierto grado de personalización. Las más comunes son:

* Guardar únicamente el registro del material inapropiado al que se ha tenido acceso.

* Monitorización aleatoria o intermitente (ej. Registrar cada 15 minutos o 10 minutos cada hora).

* En los casos de visualización remota de la pantalla del menor, se puede adaptar tanto el nivel de resolución como el número de pantallas.

* Avisar al menor de un posible acceso a material inapropiado. El menor decide entonces si continúa o no con la navegación y, en caso positivo, la herramienta registrará este acceso y lo notificará al responsable.

* Monitorización colectiva. En lugar de analizar comportamientos individuales, se examina si el comportamiento del grupo es acorde a determinados parámetros. De esta forma no se compromete la privacidad individual, pero se obtiene información sobre los patrones de conducta más habituales de los menores permitiendo conocer las *webs* a las que acceden y las actividades que realizan.

b.- Problemas asociados a la monitorización

Costes psicológicos y emocionales. El principal coste de la monitorización es la pérdida de privacidad. La necesidad de privacidad es un componente esencial de los jóvenes, especialmente a medida que los adolescentes empiezan a crear su propia identidad. La monitorización puede ser vista por parte de los menores como una violación de la privacidad y una intrusión no autorizada que demuestra una ausencia de confianza.

Otros costes. Aunque el coste de adquisición de estas herramientas es bajo, el mayor coste habría que medirlo en términos de esfuerzo humano. El examen de los registros puede ser extenso, tedioso y lento.

c.- ¿Cuál es el futuro de la monitorización?

Existe un campo de actuación para las herramientas que revisan y analizan de forma colectiva los patrones de comportamiento de los menores y que pueden ser útiles para una investigación posterior.

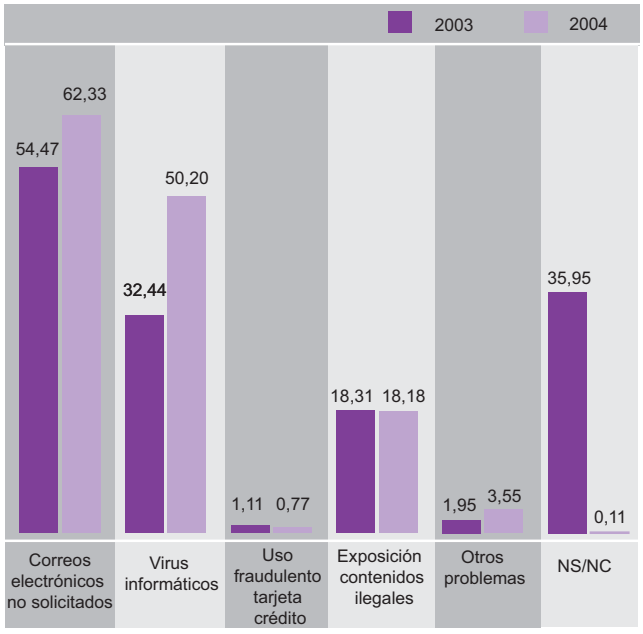
Las tendencias actuales de este tipo de herramientas pasan por registrar únicamente los accesos a páginas problemáticas, determinando la secuencia de acceso y el tiempo de navegación en esa página *web* y en la notificación en tiempo real de dicha circunstancia o del uso de determinados servicios (*chat*, descarga de archivos...). De esta forma se reduce el tiempo de supervisión posterior por parte del adulto.

■ Las herramientas para controlar el *spam*

En ocasiones, los contenidos ilícitos no proceden de páginas *web*, sino de los servicios interactivos y, sobre todo, del correo electrónico no deseado. El *spam* o "correo basura" hace referencia a cualquier tipo de correo no solicitado, enviado normalmente con fines publicitarios y, en ocasiones, por proveedores de contenidos para adultos o con fines ilícitos. En el caso de los contenidos para adultos, normalmente invita a acceder a una página *web* o incluye un enlace a la misma, aunque no suele incluir imágenes explícitas.

En estos momentos, se calcula que aproximadamente el 60% de todos los correos que circulan por Internet, son correos no deseados por sus receptores[7]. Según el Instituto Nacional de Estadística, el principal problema de seguridad manifestado por los internautas españoles, es la recepción de correo no deseado, por encima de los virus informáticos y la existencia de mensajes o ficheros ilegales u ofensivos.

Problemas de seguridad en el acceso a Internet, en %



Fuente: Instituto Nacional de Estadística

Existen dos categorías de herramientas tecnológicas para controlar el *spam*: las que evitan que el correo electrónico llegue al destinatario y las que gestionan el correo una vez que ha sido recibido. Para el caso que nos ocupa, las que más se utilizan son las primeras, y más concretamente, las que permiten al usuario recibir únicamente aquellos co-

rreos que provienen de una lista específica de direcciones o nombres de dominio, previamente autorizados.

a.- Cómo funciona el control de *spam*

El *e-mail* puede ser identificado y bloqueado sobre la base de:

Contenido. El sistema utilizado es el mismo que el usado para el filtrado, analizando el texto y las imágenes para determinar el carácter del *mail*.

Fuente. El correo recibido de una determinada dirección de Internet o nombre de dominio puede ser detectado y bloqueado.

Receptor. En la mayoría de los casos, el correo *spam* no está explícitamente dirigido a un individuo, sino a una gran cantidad de personas con el sistema de "copia oculta". La mayoría de los filtros pueden seleccionar o borrar un correo si proviene de una copia oculta.

b.- Problemas asociados a las herramientas de control de *spam*

Problemas de funcionamiento. Las tecnologías de control de *spam* sufren de los mismos problemas de "infra" y "supra" bloqueo que los filtros. Pero el principal problema surge cuando el material nocivo es enviado a través de enlaces, ya que las técnicas actuales no permiten analizar el contenido de los mismos.

Problemas en el flujo de información. Muchas de las herramientas para controlar *spam* son de gran efectividad y, para los menores, son especialmente útiles aquellas que no aceptan más que los correos procedentes de una determinada lista de direcciones o dominios preestablecida. El problema es que esta técnica restringe el universo de contactos potenciales.

Aunque estas herramientas son enormemente útiles, no existe la herramienta perfecta. La tecnología puede ayudar a crear un entorno que los padres y educadores pueden moderar y modelar en función de sus valores y la madurez de sus hijos. Por ejemplo, para los más pequeños, puede ser adecuado un acceso explícitamente limitado a los contenidos infantiles (acceso basado en las listas blancas), mientras que para los niños de edad intermedia sería más conveniente un acceso a Internet filtrado de forma cerrada (listas negras), reduciendo paulatinamente el número o las categorías de los accesos limitados a medida que avanza la edad, llegando hasta la monitorización para los adolescentes.

Existen otras herramientas tecnológicas para evitar el acceso de los menores a los contenidos nocivos, como pueden ser las técnicas de control de edad, la encriptación, etc., pero no se han detallado en el presente informe, en primer lugar por ser menos comunes que las anteriores y, en segundo, porque su aplicación e implementación no le compete al usuario final.

5.2. Las estrategias educativas

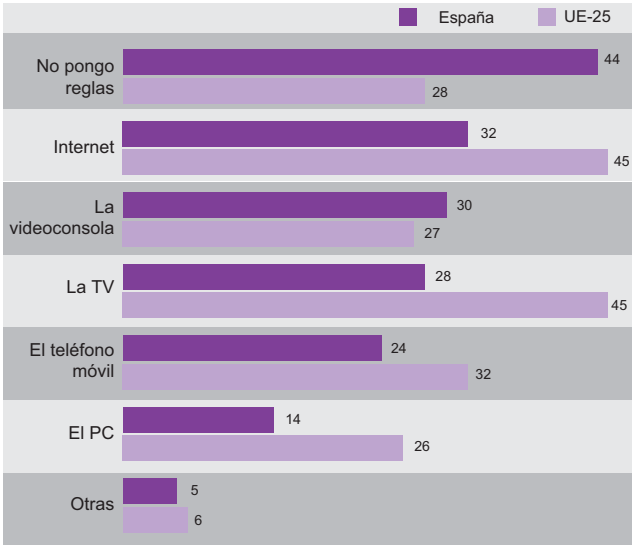
Las medidas analizadas hasta ahora (legislación, líneas de denuncia y herramientas tecnológicas) no protegen por sí solas a los menores de los contenidos ilícitos y nocivos de la Red. Es más, incluso aunque así fuera, seguiría siendo necesario que padres y educadores acompañaran a los menores en la navegación y les enseñaran a tomar decisiones sobre su uso. La tecnología es un medio, pero nunca podrá sustituir totalmente la tarea de padres y educadores. La educación, la supervisión y la implicación directa de los padres siguen siendo la mejor manera de proteger a los menores. Es necesario compartir el tiempo de navegación, enseñarles a controlar y manejar Internet de forma responsable: dónde van, qué ven, qué hacen o con quién hablan. Pero estas estrategias no son, ni mucho menos, características de Internet. Otros medios de comunicación implican la posibilidad de encontrar materiales inapropiados (por ejemplo, revistas con material pornográfico o contenidos violentos en televisión), e incluso fuera de los medios existen peligros similares como es el riesgo de encontrase con personas inconvenientes. Si buscamos una analogía fuera del entorno virtual, podríamos encontrarla en las piscinas. Las piscinas pueden constituir un riesgo para los más pequeños. Para protegerles, se puede instalar una valla, colocar una alarma o comprar un flotador pero, sin lugar a dudas, la mejor opción es enseñarles a nadar. En el ciberespacio, igual que en el mundo "real", la mejor estrategia de protección es la supervisión y la educación.

Existe un amplio consenso en que la mejor forma de proteger a los menores del material y las conductas inapropiados en Internet es a través de la educación. Pero no existe un modelo único, depende de los valores familiares, culturales o del entorno y de la edad del menor. Cada padre tiene la difícil tarea de determinar el límite entre la libertad y la confianza o entre la independencia y la privacidad, y esta línea divisoria nunca está clara.

Pero, ¿cuáles son las normas principales que establecen los padres para limitar la exposición a los contenidos y comportamientos inadecuados?

Si preguntamos a los padres españoles si imponen alguna norma para el uso de los dispositivos electrónicos por parte de sus hijos, más de la mitad (56%) contestará que sí lo hace. El 32% impone reglas para la navegación por Internet, el 30% lo hace para el uso de las videoconsolas y el 28% para ver la televisión[8].

¿Regula el uso de dispositivos electrónicos?, en %



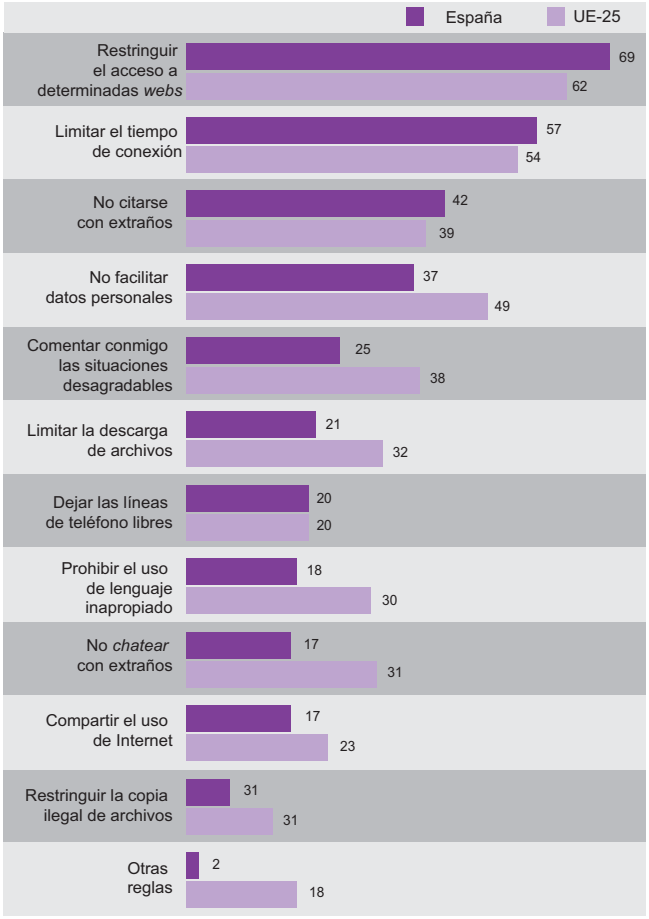
Fuente: Fundación AUNA a partir de Comisión Europea, Eurobarómetro

La comparativa con otros países de la Unión Europea es interesante. España es el segundo país europeo más permisivo, sólo superado por Portugal. Así, mientras un 44% de los padres españoles no impone reglas al uso de dispositivos electrónicos, la media europea se sitúa en un 28%.

Si nos centramos en la navegación, en Europa un 45% de los padres regula esta práctica, llegando esta cifra al 61% en países como Finlandia y Suecia, muy por encima de nuestro país que, con un 32%, es el quinto más flexible.

Las normas más usuales son las que limitan el acceso a las páginas *web* (69%), seguidas de las que limitan el tiempo de conexión (57%), las que restringen el acceso a salas de *chat*, el establecimiento de contactos con desconocidos o la transmisión de datos personales (37%).

Tipo de regla para el uso de Internet, en %



Fuente: Fundación AUNA a partir de Comisión Europea, Eurobarómetro

Existen numerosas páginas *web* que ofrecen recomendaciones sobre un uso seguro de Internet. Entre estas páginas destacan la elaborada por la entidad pública empresarial Red.es "http://navegacion-segura.red.es", por la Asociación contra la Pornografía Infantil "www.asociacion-acpi.org" o por la Asociación PROTEGELES "www.protegeles.com". Las principales son:

Principales recomendaciones

Colocar el ordenador en un lugar "público" de la casa (así se cumple la función de la monitorización en las herramientas tecnológicas).

Comentar las reglas impuestas con relación al uso de Internet. Estas deben incluir: cuándo y bajo qué circunstancias se puede utilizar la Red, tipos de actividades y páginas *web* admisibles o inaceptables, información que no se puede dar y qué hacer en caso de encontrar material ilícito.

Poner límites al tiempo de navegación.

Conocer las herramientas tecnológicas y los programas de navegación segura que están a su alcance.

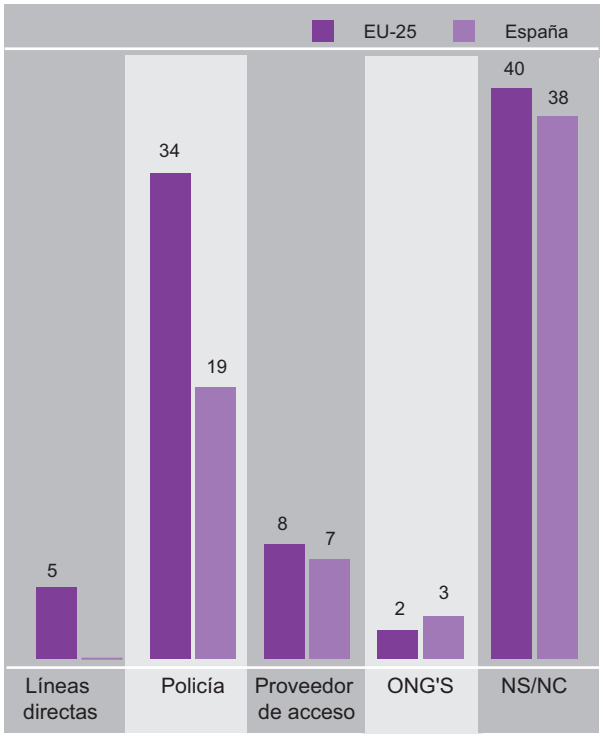
Fuente: Elaboración propia

5.3. Las estrategias sociales

Nos referimos a estrategias sociales para definir aquellos planes de acción coordinados, dirigidos a usuarios finales, padres, educadores, industria, intermediarios..., destinados al fomento de un espacio digital más seguro. Estas estrategias incluyen medidas de sensibilización, información y formación a padres y educadores, la promoción de la elaboración de códigos deontológicos por parte del sector y la coordinación de los diferentes actores implicados.

Las medidas de información y sensibilización pueden ayudar a educar a los adultos acerca de las necesidades de seguridad en Internet y sobre la naturaleza y extensión de los peligros de la Red. Estas deben ir encaminadas a que los usuarios comprendan tanto las ventajas como los inconvenientes de Internet, con el fin de incrementar la utilización de los servicios utilizados. Además deben facilitar a padres y educadores información suficiente para poder aprovechar plenamente los programas informáticos de vigilancia y los mecanismos de clasificación.

¿A quién comunicaría la existencia de contenidos ilícitos o nocivos?, en %



Fuente: Fundación AUNA a partir de Comisión Europea, Eurobarómetro

Estas estrategias son de vital importancia en nuestro país y deben ser prioritarias para los poderes públicos. Las estadísticas al respecto así lo evidencian[9]. Un 62% de los padres españoles afirma que necesitaría más información sobre cómo proteger a los menores y sólo un 34% está suficientemente informado. Las cifras, una vez más, nos sitúan lejos de la media de la Unión Europea en la que prácticamente la mitad (48%) considera que no necesita más información.

Otro dato elocuente es el referente al porcentaje de padres que no sabría dónde acudir en caso de encontrar contenidos ilícitos en la Red y que ninguno de los encuestados mencionó las líneas directas como lugar de denuncia de estos contenidos.

Finalmente, otra de las estrategias sociales para fomentar un uso seguro de la Red es la promoción de las iniciativas de autorregulación y el establecimiento, por parte de los proveedores de contenidos, de códigos de conducta o conjuntos de normas elaboradas por ellos mismos, en los que se establezcan las obligaciones respecto de su actividad en Internet. La Unión Europea es la instancia, a nivel internacional, que ha mostrado la voluntad más firme en el fomento del uso de los códigos de conducta con el fin de luchar eficazmente contra los contenidos ilícitos y nocivos en Internet, incluyendo este aspecto entre todas sus medidas a favor de la protección de los menores. Entre estas medidas, el Parlamento Europeo ha recomendado la creación de un nuevo dominio en Internet, el ".kid", con contenidos para menores y que estaría sometido a un control regular por una autoridad independiente □

NOTAS

[1] Existen comparativas de sistemas de filtrado en la *web* de la Asociación de Usuarios de Internet (www.aui.es) y en la Asociación estadounidense GetNetWise (www.getnetwise.org)

[2] Por ejemplo, se puede encontrar esta opción en Internet Explorer realizando la secuencia: Inicio - Configuración - Panel de Control - Opciones de Internet - Contenido - Asesor de Contenido. En Netscape, esta opción se encuentra en el menú "Editar", eligiendo "Preferencias" y seleccionando los valores "Seguridad" o "Privacidad".

[3] ACPI-PROTEGELES para el Defensor del Menor (2002) *Seguridad Infantil y Costumbres de los Menores en Internet.*

[4] *Pew Internet & American Life Project (*2005). *Protecting teens online.*

[5] www es el organismo encargado de establecer los estándares de Internet.

[6] Por defecto registra los accesos de los últimos 20 días, aunque permite ajustar el tiempo.

[7] OECD (2004) *Background Paper for the OECD Workshop on Spam.*

[8] Comisión Europea - Eurobarómetro (2004) *Illegal and harmful content on the Internet.*

[9] Ver nota 8.

A MODO DE CONCLUSIÓN

La atención a los menores y la protección de los mismos son indicadores claros del nivel de desarrollo cívico alcanzado por una sociedad. En el marco de la preocupación por los niños, las relaciones que se establecen entre los menores y los medios de comunicación, especialmente Internet, han adquirido últimamente un gran protagonismo. De ese debate han surgido dos posiciones: una favorable a Internet como herramienta para la educación y otra contraria, por la necesidad de protegerles ante los riesgos que implica.

Gran parte de este debate se centra en las ventajas y desventajas tanto de las soluciones tecnológicas como de las iniciativas que se impulsan desde los poderes públicos. Las soluciones tecnológicas parecen ofrecer respuestas rápidas y baratas y resulta tentador pensar que el uso de la tecnología puede reducir drásticamente la necesidad de supervisión. Las soluciones de tipo judicial y policial ofrecen eliminar las fuentes del problema. Sin embargo, esta perspectiva podría estar desenfocada: ni la tecnología ni los poderes públicos por sí solos pueden ofrecer una solución completa al problema. Además de las anteriores, es necesario implementar una serie de estrategias de tipo social y educativo encaminadas a desarrollar en los menores habilidades que les permitan controlar y manejar el ciberespacio de forma responsable, para su protección, tanto en Internet, como en el mundo "analógico".

Internet no es un hecho aislado, forma parte de la realidad y, como ocurre con otras muchas actividades, tiene sus ventajas, aunque también entraña riesgos. ¿Acaso no puede ser peligroso cruzar una calle, montar en bicicleta o bañarse en el mar? Sin embargo, no por ello se deben utilizar exclusivamente medidas de tipo restrictivo. El objetivo, por lo tanto, debería ir orientado a ayudar a los menores a utilizar la Red correctamente para fomentar su uso creativo y beneficioso. De esta forma, se podrán rentabilizar plenamente las innumerables posibilidades que ofrece Internet, a la vez que se favorece que padres e hijos utilicen juntos la tecnología, discutan su uso y aprendan a utilizarla como elemento de cohesión y mejora de las relaciones paterno-filiales □

La Fundación AUNA es una institución sin ánimo de lucro que tiene omo objetivo general el contribuir al desarrollo de la Sociedad de la Información en España en beneficio de todos los ciudadanos, empresas e instituciones. Para ello, la Fundación AUNA lleva a cabo una serie de actividades que se centran en las áreas de Formación, I+D y Análisis y Prospectiva, entre las que ocupa un lugar preferente la publicación de estudios e informes sobre los aspectos más importantes relacionados con las Tecnologías de la Información y las Comunicaciones, y su impacto económico y social.

Fundación AUNA

Publicaciones editadas hasta el momento:

Serie **Notas de Análisis y Prospectiva**

- El futuro del acceso a Internet: ¿3G o WiFi?
- El *software* de código abierto ¿mito o realidad?
- Evolución del sector de Telecomunicaciones en EE UU
- Las alternativas en el futuro de la telefonía móvil
- Los retos de la banda ancha
- Los nuevos miembros de la UE en la Sociedad de la Información
- El futuro del pago por contenidos
- China: un nuevo coloso de la Sociedad de la Información
- La Voz IP: hacia la convergencia
- Generación *"e"*
- El marketing *on-line*: presente y futuro

Serie **Cuadernos de Sociedad de la Información**

- Los países árabes y la Sociedad de la Información
- Las tensiones en el desarrollo de la Sociedad de la Información
- El impacto de Internet en la Prensa
- Los Mayores en la Sociedad de la Información: situación actual y retos de futuro
- Las nuevas tecnologías en la educación
- Los menores en la Red: comportamiento y navegación segura

Serie **Referencias**

- Informe al Presidente de los EE UU sobre Internet
  Internet Policy Institute
- La Banda Ancha: situación actual y perspectivas
  National Research Council
- La eDemocracia: una perspectiva de EE UU y Europa
  Program on Information Resources Policy
  Institute de Hautes Etudes en Administration Publique
- La eAdministracaión: Aspectos estratégicos y operativos
  Danish Technological Institute &
  Institut für Informationsmanagement Bremen
  RAND Europe

Informe Anual **eEspaña / eSpain**

- eEspaña 2001
- eEspaña 2002
- eEspaña 2003
- eEspaña 2004
- eEspaña 2005
- eSpain 2002
- eSpain 2003
- eSpain 2004

Colección **Biblioteca Fundación AUNA**

- Seguridad y certificación en el comercio electrónico
- Los contenidos ilícitos y nocivos en Internet
- El comercio electrónico: situación actual y perspectivas
- Estrategias empresariales en Telecomunicaciones e Internet
- La telemedicina: situación actual y perspectivas
- Internet y el español
- La Brecha Digital: el riesgo de exclusión en la Sociedad de la Información
- Educación virtual y *eLearning*

Observatorio de la SI (Encuentro Fundación AUNA - Universia)

- Serie 'La nueva geografía y las cifras de la SI'
- Serie 'Pensamiento y ensayo sobre la SI'
- Serie 'La Sociedad de la Información a pie de calle'

auna
Fundación

c/ Obenque, 4 - 4ª planta
28042 Madrid (España)
Tel.: (+34) 912 137 000
Fax: (+34) 912 137 099
www.fundacionauna.org