28 de enero, Día de la Protección de Datos en Europa

Soy padre ¿cómo puedo proteger la privacidad de mis hijos en Internet?

- **El próximo mes de mayo comenzará a aplicarse el nuevo Reglamento General de Protección de Datos europeo (RGPD).**
- **The Valley crea un protocolo con 7 consejos dirigido a padres para salvaguardar la privacidad en Internet de los menores de edad.**

Madrid, 23 de enero de 2018. El próximo mes de mayo de 2018 comenzará a aplicarse el nuevo Reglamento General de Protección de Datos europeo (RGPD), norma que sustituirá a la actual Ley Orgánica de Protección de Datos (LOPD). La expectación respecto al tema es máxima, tanto en el sector empresarial como en el de los consumidores en general.

La cuestión de la protección de la privacidad de los menores es, de nuevo, uno de los aspectos en los que más se hace hincapié. Entre las novedades, el RGPD obliga a que, en caso de cesión de algún tipo de información relativa a este grupo poblacional, los responsables del sitio pongan en marcha los medios y procedimientos necesarios, teniendo en cuenta la tecnología disponible, para verificar que, efectivamente, son los padres o tutores los que dan el consentimiento.

Aunque ya están contempladas en la agenda de las autoridades competentes actividades de formación y sensibilización dirigidas a niños y adolescentes, los padres son la pieza clave en el proceso. ¿Qué nociones deben tener para preservar los intereses de sus hijos? Los expertos de **The Valley** desgranan siete consejos:

- **La protección siempre empieza por el usuario:** En un mundo en el que los niños empiezan a utilizar dispositivos con acceso a Internet desde muy pequeños, son precisamente ellos lo que tienen que ser conscientes de que han de ser muy cautelosos con los contenidos que visitan y con los posibles datos que puedan ceder sin consentimiento. Tienen que entender que el móvil, la tablet o el ordenador no son juguetes. Para ello, conviene enseñarles a usarlos con moderación, potenciando su vertiente más funcional y pedagógica.

- **Facilitar información a extraños, peligro Nº1.** No solo hay que mostrarles cómo hacer un uso debido de las funcionalidades de Internet, también, como en la vida real, se debe inculcar que nunca deben contactar o facilitar datos a extraños. Las redes sociales y las aplicaciones son un peligro potencial. Algunos expertos en psicología pediátrica recomiendan educar sobre cuestiones como el *sexting*, el *grooming*, el ciberacoso o sobre la revelación indebida de información.

- **Con las redes sociales: información, límites y vigilancia.** Actualmente, los menores de 14 años no pueden acceder a las redes sociales si no cuentan con consentimiento paterno. Sin embargo, las utilizan, con o sin éste. Según las estadísticas, los niños comienzan a crearse perfiles sociales incluso antes de los diez años. En este contexto, la solución no será prohibirles su acceso a Internet, sino comenzar a informarles y advertirles lo antes posible sobre la importancia de usarlas con sentido común, protegiendo su identidad y con la condición de una supervisión periódica para asegurar de que la configuración de la privacidad es la adecuada y de que no están expuestos a otros peligros.

- **¿Solo hay que preocuparse del tratamiento de datos en redes sociales y webs?** En caso de que llegue el momento de dar un consentimiento, tanto con la entrada de la nueva normativa como con la actualmente vigente, es preciso conocer al dedillo cuál será el uso los datos y las condiciones de este tratamiento (políticas de privacidad), así como si son de uso exclusivo del sitio o si está incluida la cesión a terceros. Tanto en webs o redes sociales, como en Apps, navegadores o sistemas operativos móviles.

- **Las Apps también son peligrosas.** Precisamente las Apps son, dentro de las posibilidades que ofrece internet, lo que más utilizan los niños: juegos, vídeos e, incluso si se trata de los más pequeños, redes sociales. Por este motivo, conviene comprobar su fiabilidad. Algunas de ellas, descargadas desde una página web peligrosa, pueden abrir la puerta a ciberdelincuentes, suponer la suscripción a un servicio *premium* o devenir en un control de ubicación, documentos o información personal. Es recomendable, en este sentido, instalar los antivirus correspondientes.

- **¿Hasta qué edad es necesario mi consentimento directo?** Aunque la norma europea habla de que el consentimiento personal solo será válido a partir de los 16 años, otorga total libertad a los estados miembros para establecer una edad inferior que supere, eso sí, los 13 años. Actualmente, nuestro sistema normativo fija los 14 años, aunque el anteproyecto de la nueva ley nacional, impulsada para adaptarse al reglamento comunitario, recoge los 13 años.

- **No olvidarse de que los adolescentes también son menores.** Aunque la normativa hable en cuanto a consentimiento de menores de 13 o 14 años, no hay que olvidarse de este grupo que, aunque tiene más autonomía, tampoco cuenta con la mayoría de edad. Son, precisamente, los adolescentes los más expuestos en este ámbito, sobre todo en lo que respecta a las redes sociales. Aquí también habrá que concienciarles de que hay que privatizar la información personal, que solo añadan a gente conocida a sus listas de amigos, que no divulguen sus contraseñas, que publiquen fotos adecuadas y, sobre todo, que sean conscientes de que Internet NO es privado.

Acerca de *The Valley*

THE VALLEY es un ecosistema digital donde se une formación, talento y emprendimiento a través de la actividad de la escuela, THE VALLEY DIGITAL BUSINESS SCHOOL, el coworking para startups digitales y THE VALLEY TALENT, un headhunter especializado en perfiles digitales. Con sede en Madrid, Barcelona y Canarias, el objetivo es fomentar las sinergias y el networking entre profesores, alumnos y emprendedores con el fin de generar proyectos innovadores de éxito para el sector digital.
www.thevalley.es

Para más información: **Trescom Comunicación:**
Sara Gonzalo / Alba Tortosa 91 411 58 68 / 615 18 41 66
sara.gonzalo@trescom.es, florita.vallcaneras@trescom.es