



A poboación galega é das máis preocupadas por protexer a súa privacidade e por reclamar en caso de abusos, segundo a experta de R Susana Rey

R celebra o Día Europeo da Protección de Datos: “Para unha vida boa é esencial salvagardar a nosa información sensible”

- ***Susana Rey, especialista en ciberseguridade e privacidade e membro da Oficina de Protección de Datos de R explica que se trata de “formar un espírito crítico compartido que nos permita tomar decisións adecuadas en cada caso” (...)***
Primeira lección: Menos é máis; menos datos, máis seguridade”.
- ***Para Rey é imprescindible “contar con información rigorosa do que realmente aceptamos cando damos o ok ás condicións de privacidade dunha páxina, servizo ou aplicación, para evitar usos inadecuados ou fraudulentos dos nosos datos”.***
- ***Cada vez dámoslle máis importancia á protección dos nosos datos persoais: só en 2020, a Axencia Española de Protección de Datos (AEPD) xestionou máis de 10.000 reclamacións e multas por un total de 8 millóns de euros.***

Xoves, 27 de xaneiro de 2022.- Dende o ano 2006, tal día como mañá, 28 de febreiro, celébrase o *Día Europeo da Protección de Datos* para destacar a importancia da privacidade e a protección dos datos persoais e sensibles. O fin desta conmemoración é formar e concienciar as persoas sobre os seus dereitos e deberes, especialmente na contratación de servizos e/ou na realización de xestións a través de internet e das novas tecnoloxías.

A especialista en ciberseguridade e privacidade da Oficina de Protección de Datos de R, Susana Rey, reflexionou sobre as consecuencias que pode ocasionar nas nosas vidas o non protexer a información máis sensible que posuímos: os nosos datos persoais; porque *“son susceptibles de utilizarse para fins que poden ter impactos verdadeiramente desagradables nas nosas vidas: perdas económicas, suplantacións de personalidade, publicación de información íntima, recepción de múltiples comunicacións comerciais... etc. É esencial, por todo iso, que salvagardemos con celo a nosa información sensible”.*

Algúns consellos para protexernos na rede

Para avanzar na formación dun “espírito crítico compartido que lles permita ás persoas tomaren decisións axeitadas en cada caso”, a experta de **R** en PD ofrece unha serie de consellos:

“Ante o vicio de pedir, a virtude de non dar”: en contornas dixitais adoitamos dar os nosos datos sen pensar que seguramente non sexa necesario facelo. Aínda que non haxa mala intención en quen os pide, ante algún problema de ciberseguridade eses datos poden rematar en malas mans e implicar problemas serios para nós. Por iso, como punto de partida neste terreo hai que assimilar que “Menos é máis: menos datos, máis seguridade”, sempre.

“Seguinte-seguinte... e despois?”: se nos habituamos a aceptar todas as condicións de privacidade dunha web, servizo, *app*... de xeito automático, podemos estar a dar permiso para que utilicen os nosos datos con fins que non compartimos e/ou impliquen riscos que descoñecemos. Hai que ler a información de privacidade, obrigatoria en todos os casos, e pensar se nos interesa ou non aceptala. Se non existe esa información ou é incompleta, estraña ou inintelixible... desconfiemos.

“Nada é de balde”: cando un servizo, web, *app*... non nos cobra polo seu uso, probablemente esteamos ao pagar cos nosos datos. Trátase de valorar se nos compensa que unha empresa poida saber, por exemplo, onde estamos en todo momento a través do noso móbil, a cambio dunha aplicación que nos mostra a dirección exacta a Cuenca.

O caso das **redes sociais e os menores** é especialmente delicado. Susana Rey incide en que sempre resulta arriscado expor a nosa información sensible en redes sociais e en internet, *“e moito máis se é de terceiras persoas e sobre todo de menores. Na actualidade, a súa sobreexposición pública e os temas de ‘sexting’ ou ‘bullying’ en redes sociais constitúen un problema serio para moitos/as nenos/as e adolescentes, con consecuencias gravísimas nalgúns casos. É preciso educar xa os/as máis pequenos/as na necesidade de ser responsables cos seus datos e cos dos/as demais, tomando ao tempo unha actitude belixerante fronte a este tipo de actuacións doutros/as cando as atopemos”*.

Para as empresas, un *plus* de credibilidade

Para autónomos e empresas tamén resulta imprescindible cumprir coa lexislación actual en materia de privacidade e protección de datos. Non facelo ou manter ante un tema tan transcendente unha actitude de desleixo ou negligencia supón expor a un risco innecesario a propia organización, que pode provocar a imposición de multas por parte das autoridades competentes e a perda de confianza e credibilidade dos/as seus/súas clientes/as.

A filtración ou roubo de información almacenada no negocio igualmente pode usarse para a comisión doutras fraudes por parte de ciberdelinquentes. De aí a importancia de aplicar medidas e políticas de seguridade para a súa protección, que van necesariamente vinculadas ao concepto de ciberseguridade na empresa.

Susana Rey aconsella, como primeiro paso, *“cambiar a percepción sobre a ciberseguridade, pasando de vela como un gasto prescindible cando as tensións financeiras do negocio o esixan a un investimento realmente importante e básico”*. En palabras da especialista, a dixitalización é *“un alicerce básico para o desenvolvemento actual das empresas, mais esa dixitalización sen o axeitado investimento en ciberseguridade, co respaldo imprescindible de profesionais e expertos, implica crear un xigante de pés de barro que en calquera momento pode vir abaixo”*.

Reclamacións e multas en aumento

Na Unión Europea, a protección de datos é un dereito fundamental, e o **Regulamento Xeral de Protección de Datos (RGPD)** é o marco regulatorio que lles permite aos/ás europeos/as recuperar o control sobre a súa información persoal.

Parece que cada vez somos máis conscientes desa necesidade, como reflicten os números que manexa a Axencia Española de Protección de Datos (AEPD), organismo que en 2020 xestionou **máis de 10.000 reclamacións** que se traduciron en **172 sancións ou multas** cun montante total de máis de **8 millóns de euros**.

A poboación de Galicia é das máis preocupadas por protexer a súa privacidade e por reclamar en caso de abusos, segundo explica Susana Rey: *“As/os galegas somos dos/as máis combativas/os e preocupadas/os polos temas de protección de datos e ciberseguridade en España, e non pasamos nin unha; ademais, hai unha tendencia xeral a cumprir coa lexislación vixente e a denunciar en caso de incidentes detectados (...) Non podemos ofrecer datos actualizados agora porque a AEPD xa non desagrega os informes por comunidades autónomas como antes; mais a tendencia sempre foi esa ao longo dos anos”*, asegura a especialista de **R**.

Canle oficial aberta para denunciar

Neste sentido, a AEPD puxo a disposición de todos/as a chamada **Canle Prioritaria** en <https://www.aepd.es/canalprioritario/>. A través desta vía, a Axencia lle permite a calquera español/a informar da publicación de contidos que impliquen grandes riscos potenciais para a(s) persoa(s) afectada(s): contidos sexuais, de violencia ou de incitación á violencia, especialmente se hai menores polo medio... e outros. A propia Axencia **xestiona a retirada deses contidos** cando considera que ese risco existe, que é real.

As actuacións derivadas de denuncias presentadas nesta canle triplicáronse nos últimos anos, e a AEPD xestionou a clausura de contidos en **49 casos**, a maioría relacionados con **menores en situacións de acoso e/ou contido sexual**. Calquera persoa pode denunciar, aínda que non sexa unha das afectadas, e evitar, talvez, consecuencias tremendas e irreparables para a saúde e a vida dos/as menores expostos/as nas redes e/ou en internet.

comunicación R
prensa@mun-do-r.net
R.gal