LA VANGUARDIA (ES-ESTILOS DE VIDA)
BARCELONA
21/07/12
Prensa: Semanal (Sabado)
Tirada: 238.004 Ejemplares
Difusión: 201.859 Ejemplares
Cód: 60163194
Página: 30
Sección: OTROS Valor: 12.285,00 € Área (cm2): 868,6 Ocupación: 100 % Documento: 1/4 Autor: Texto Cristina Sáez Núm. Lectores: 132000

Texto Cristina Sáez

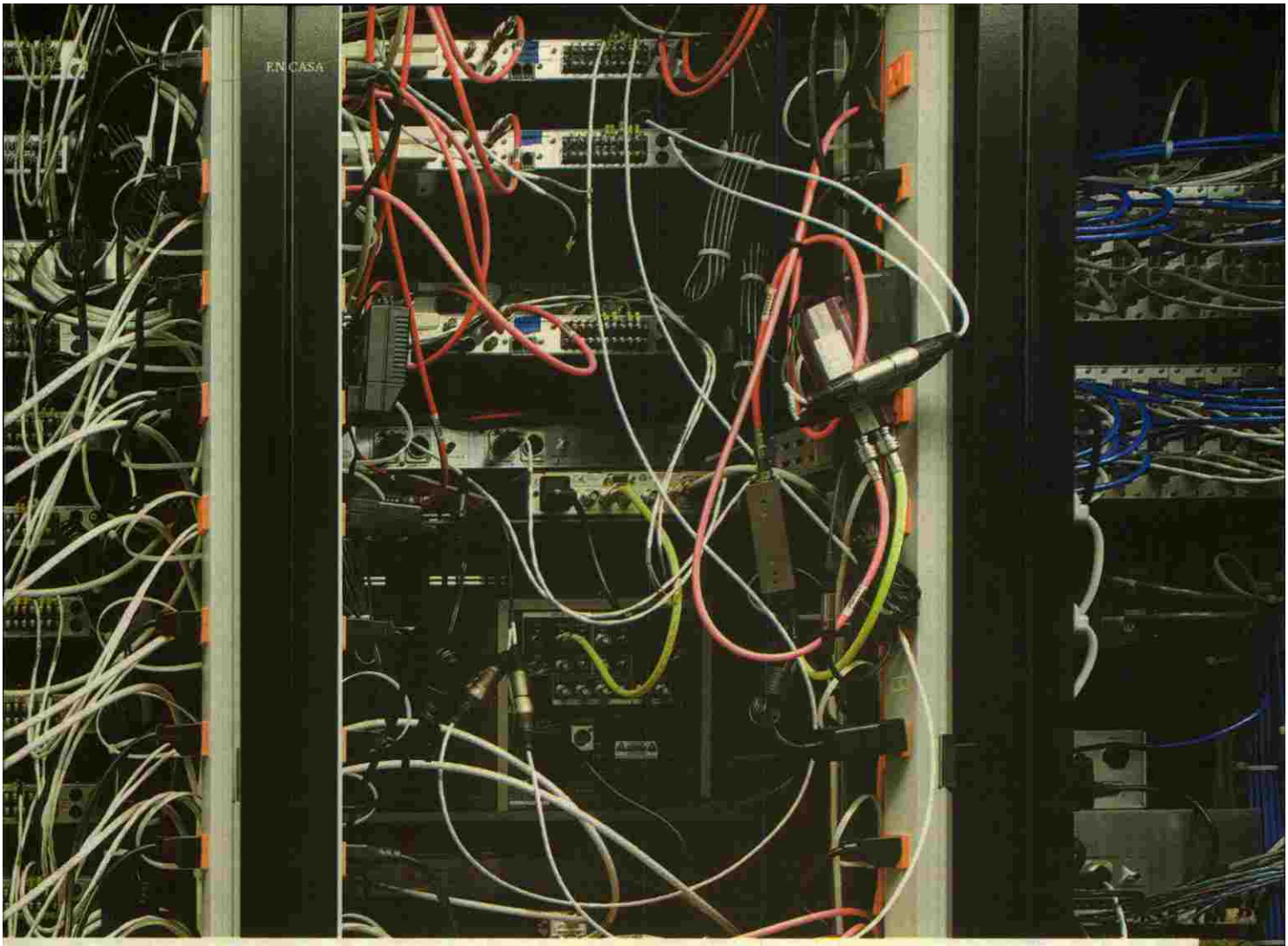
¿Dónde han metido mi información?

Vivimos todo el tiempo en la nube... y no estamos hablando de despistes. La nube es ese espacio etéreo, que no tenemos muy claro qué es, en el que parece caber todo, donde cada día subimos vídeos, fotos, documentos, música, pero también donde dejamos nuestra huella digital. Es decir, de manera directa o indirecta, confesamos quienes somos, qué hacemos, qué nos gusta... Dicen los expertos que todo son ventajas, pero también hay voces que alertan que de eso nada

Cada segundo, se sube una hora de vídeo a YouTube; es decir que en un día se cuelgan 86.400 horas, lo que supone, anualmente, unos 3.600 años de vídeo. Las cifras de Facebook no son menos impresionantes: se publican más de mil fotos personales por segundo, 3.000 millones al mes. Ya el año pasado los expertos afirmaban que la humanidad había alcanzado un Zettabyte (ZB) de almacenamiento digital, el equivalente a más de mil billones (1.125.899.906.842.624) de los disquetes de hace unos años. ¿Se han preguntado alguna vez dónde está toda esa información? ¿En qué lugar se guardan las fotos que posteamos en Instagram, los e-mails con adjuntos que enviamos a través de Gmail o de Yahoo, o los documentos, las películas o la música que depositamos en Dropbox? ¿A dónde va a parar nuestro calendario, la agenda, los contactos de móvil que sincronizamos con el correo?

A la nube, dirán. Hace ya algunos años que oímos hablar del *cloud computing*, o de la computación en nube: nuestros datos, están almacenados en servidores físicos y virtuales repartidos por todo el mundo. Y moviéndose por todos los continentes. Enrique Dans (enriquedans.com), profesor de sistemas de información de IE Business School y autor

LA VANGUARDIA (ES-ESTILOS DE VIDA) 21/07/12
BARCELONA
Prensa: Semanal (Sabado)
Tirada: 238.004 Ejemplares
Difusión: 201.859 Ejemplares
Cod: 60163194
Página: 31
Sección: OTROS Valor: 12.285,00 € Área (cm2): 860,2 Ocupación: 100 % Documento: 2/4 Autor: Texto Cristina Sáez Núm. Lectores: 132000



del libro *Todo va a cambiar* (Deusto), lo explica: "Tus datos están en algún centro de datos, en los que hay muchos servidores con discos duros. De hecho, no están en uno solo, sino en varios, replicados, para que no se pierdan. Nuestra información se mueve continuamente de un centro a otro; se copia desde la distancia y con copias de seguridad, para que ante algún problema, como un atentado o un terremoto, se evite la destrucción de datos".

De hecho, Google, por ejemplo, tiene copia de toda la web. Han leído bien. De toda. Cada vez que hacemos una petición de información, el buscador no va a explorar la inmensidad de internet, sino que se dirige a una de las muchas bases de datos que replican todo el contenido de la red: eso es, todas las webs que Google ha podido indexar, así como las versiones anteriores de esas páginas (caché). Así es que... ¡imagínense la cantidad ingente de servidores y centros de datos de que dispone esta empresa!

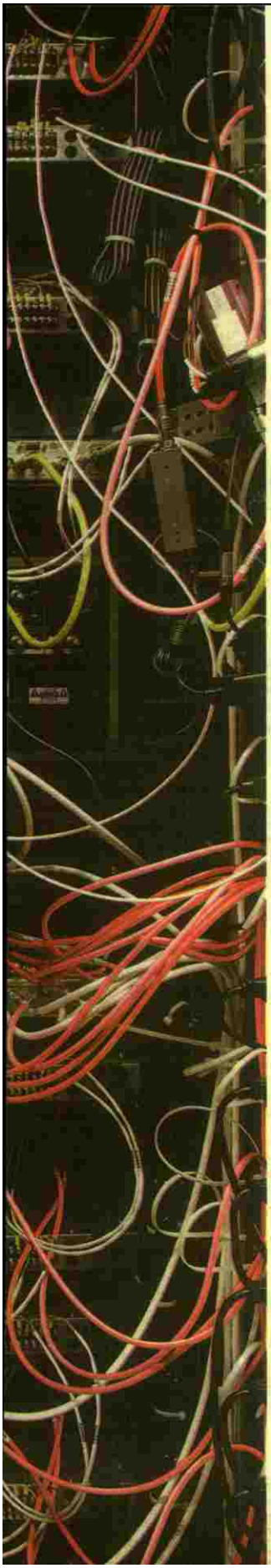
Local o virtual La nube, ese espacio virtual inacabable, nos libera de las ataduras físicas. Nos permite disponer de toda nuestra información desde cualquier lugar del mundo y desde cualquier dispositivo. El concepto es sencillo: en lugar de guardar nuestros archivos en el disco duro de nuestro ordenador, en casa, lo hacemos en uno virtual. Y eso hace posible que podamos consultar el material siempre. Así, podemos, pongamos por caso, prepararnos una clase o una presentación en casa, y luego acceder a ella desde la tableta en el aula o en la oficina. O tener todos nuestros contactos y agenda sincronizados y accesibles desde el móvil, el portátil o cualquier otro gadget.

Además, apunta Niels Christian Krüger, director general de Google Enterprise España y Portugal, esa información siempre está actualizada. Si estamos escribiendo un libro o un informe, podemos trabajar en la última versión. Si lo tenemos en nuestro disco duro, seguramente nos tocará andar lidiando con el control de cambios del procesador de textos. Estar en la nube permite, también, trabajar en equipo con un mismo documento. "Puedes ver online qué cambios hace tu compañero en el texto, incluso chatear con él e ir comentando las variaciones", apunta Dans, de IE Business School.

Luego está la seguridad. Asunto estrella. A pesar de la creencia popular de que tener los documentos colgados no sabemos dónde nos hace estar expuestos a ataques de *hackers*, a pirateos, a control por parte de empresas y gobiernos, a espías, a perderlos, lo cierto es que los expertos coinciden en señalar que no hay sitio más seguro que la nube. Y aunque el ejemplo a día de hoy puede levantar suspicacias, apunta Dans que "es como tener el dinero en casa, debajo del colchón, o meterlo en un banco. ¿Dónde va a estar más seguro? Estas empresas son especialistas en proveer un servicio de manera segura. Su reputación depende de ello. Un problema de seguridad les supone un grave problema de imagen, por lo que se esmeran al máximo para que todo esté bien y los contenidos están blindados", asegura Enrique Dans.

Para este experto, asimismo, estar en la nube comporta otros muchos beneficios en materia de seguridad: "Si estás escribiendo un libro y le pasa algo al ordenador, y no has hecho copias o *backups*, podemos perder todo nuestro trabajo, quizá de años. O si nos roban el ordenador, o se nos cae un vaso de agua encima. También pueden *hackearnos* la conexión y hacernos barbaridades en el disco duro. El nivel se seguridad que tenemos como particulares es muy bajo". ►

LA VANGUARDIA (ES-ESTILOS DE VIDA) 21/07/12
BARCELONA
Prensa: Semanal (Sabado)
Tirada: 238.004 Ejemplares
Difusión: 201.859 Ejemplares
Cod: 60163194
Página: 32
Sección: OTROS Valor: 12.285,00 € Área (cm2): 865,3 Ocupación: 100 % Documento: 3/4 Autor: Texto Cristina Sáez Núm. Lectores: 132000



TOP

► "Si un día cae un *data center* –añade Krüger, de Google–, tenemos copias de todos los datos en otros *data center*. Y es casi imposible que caigan todos los *data center* de golpe, en cuatro continentes y en diferentes países". La seguridad física también es muy grande. "En Yahoo –cuenta Flavio Junqueira, investigador sénior y mánager del equipo de computaciones escalables– tenemos muchas medidas de seguridad para evitar ataques, por ejemplo. La seguridad física en los centros de datos es enorme; hay numerosos controles para evitar que cualquiera pueda entrar y tener acceso a las máquinas".

No todo es oro... Como en muchas cosas de la vida, no es oro todo lo que reluce. Si bien la nube aporta muchas ventajas para usuarios y empresas, también presenta algunos *peros*, algunos de ellos de peso. Para empezar, si nuestros datos están en la nube de una empresa, ¿continúan siendo nuestros? Pues sí. "Siempre son del usuario", asegura Niels Christian Krüger, de Google. "Nosotros –añade– ofrecemos una plataforma para usar, pero las empresas y los individuos siempre son dueños de sus datos y tienen acceso a ellos. Como si tuviéramos un coche y lo aparcáramos en un garaje. El coche seguiría siendo nuestro, ¿no?".

¿Y qué pasa si un día quiebra la propietaria de la nube? ¿Y si caen Apple, Amazon, Google, Yahoo, Microsoft? ¿O si, como en el caso de Megaupload, se cierra de un día para otro? ¿Podemos perder nuestros datos? "Si pones tus datos en la nube de X empresa y esta quiebra, puedes perderlos, pero igual que ocurriría si hay un incendio en tu empresa física y se queman los servidores", señala Junqueira, de Yahoo. "Es muy raro que una empresa de este tipo quiebre –opina Enrique Dans–. Y más aún que no dé rutinas de recuperación de la información y que no contacte con los usuarios y les dé un tiempo de margen para que puedan recuperar sus datos. El caso Megaupload fue un tema de denuncia de ilegalidad y se hizo con mucha prisa; y ahora todo indica que fue un procedimiento incorrecto".

Cada vez que una de estas grandes empresas proveedoras de servicios de internet sale a bolsa, a menudo se suelen extender toda clase de creencias entre los usuarios que apuntan a que se comercia con nuestros datos. Que Facebook, por ejemplo, se los vende a compañías de publicidad; que Flickr roba tus fotos y se las pasa a agencias de imágenes. Pero lo cierto es que "nadie comercia con tus datos", asegura Dans. Eso sería acabar con la gallina de los huevos de oro. Lo que las empresas almacenadoras hacen es analizar los datos, crear perfiles y facilitar el acceso a esa información a empresas que buscan perfiles como el nuestro. "Pero en ningún caso le da los datos a otros, porque eso vulneraría todas las leyes de privacidad. Se requeriría que diéramos nuestro consentimiento expreso".

Es decir, que estas empresas hacen negocio generando "perfiles anónimos" de usuarios. En función de la información que nosotros les ofrecemos, dibujan segmentos de población. Y cuando una empresa de publicidad, por ejemplo, les pide enviar un anuncio a jóvenes de entre 25 y 35 años, a los que les guste la música, Facebook busca en sus bases de datos y lo envía sólo a los usuarios que entren dentro de esos parámetros. Quizá no comercia con nuestros datos, pero sí que lo hacen, en cierta medida, con nuestra privacidad, que por otra parte, regalamos, a menudo, a las redes sociales..witter, en este sentido, es paradigmático. Se niega a facilitar a nadie información de los usuarios.

¿Gran Hermano? ¿Y qué pasa con el control de la información? ¿Tienen empresas y gobiernos acceso a mis cosas? ¿O es una leyenda urbana? Este es ya un asunto mucho más complicado. Y la respuesta es... que sí. Que nos controlan. Cualquier empresa, por el hecho de tener su sede en un determinado país, debe acatar las normas de ese lugar. Así, por ejemplo, Amazon, Microsoft, Google, Yahoo están ubicados en Estados Unidos, por lo que deben responder ante la justicia de allí. Y al parecer, si bien antes se necesitaba un requerimiento legal para poder pedir a los proveedores de internet datos sobre sus clientes, ahora ya no hace falta.

"Desde que se produjeron los ataques terroristas del 11-S en EE.UU., parece que los gobiernos se dediquen ahora a esgrimir la necesidad de protegernos frente a un ataque terrorista, contra la pederastia y contra la violación de la propiedad intelectual –considera el experto en sistemas de información Enrique Dans–; se dedican a usar estas tres excusas para tener un mayor control sobre el ciudadano".

Todo el mundo recuerda el caso Wikileaks. Proveedores de servicios como Amazon, bancos y pasarelas de pago como Visa, MasterCard y PayPal, cerraron las páginas y las cuentas bancarias de la organización liderada por Julien Assange sin que hubiera una orden judicial para ello. "No es que se prohibiera que alojaran a Wikileaks, sino que hubo presiones por parte del gobierno americano en que se afirmaba que no era nada recomendable que lo hicieran. Y cuando un gobierno presiona, eso deja a las empresas pocos grados de libertad", explica Dans. Y eso también implicaba que, en cierta medida, la libertad de expresión no está garantizada.

Por eso, algunas entidades que trabajan con información delicada desde hace algún tiempo están optando por llevarse sus servidores al extranjero, a países más comprometidos con la libertad de expresión y más garantes de los derechos de los usuarios. Es el caso de Nodo50.org, un proveedor de servicios de internet, sin ánimo de lucro, que está orientado a los movimientos sociales. Nació hace 17 años y desde entonces proporciona información, contenidos y servicios de comunicación a cientos de grupos y organizaciones de izquierdas en España y Latinoamérica.

A comienzos del 2011, la Asamblea de Nodo50, tal como exponen en su página web y en el documental *Error en el sistema* (info.nodo50.org/Documental-Nodo50-Error-en-el.html), comenzó a valorar la posibilidad de llevarse sus servidores a un nuevo centro de datos, en este caso a Bahnhof,

Pero ¿dónde están exactamente los servidores?
Corren muchas leyendas urbanas acerca de dónde están ubicados los *data center*. Una de ellas dice, por ejemplo, que Google se dedica a comprar islas perdidas en el Pacífico para ubicar sus centros de datos allí, en medio de un total secretismo. Pero lo cierto es que, si bien no se pregona su ubicación a los cuatro vientos, tampoco es complicado acabar averiguándola. Basta buscar un poco en el mismo Google para dar con mapas mundi en los que están señalados estas instalaciones.
Según la base de datos Datacentermap.com, en Estados Unidos es donde más de estas instalaciones se concentran: nada menos que 1.046 de las 2.386 que hay repartidas por 86 países de todo el planeta. En España hay 36 (Madrid y Barcelona se llevan la palma con 11 cada una).
Como curiosidades, en Groenlandia hay un *data center*, y también en Hawái.
Para saber más sobre centros de datos, se puede consultar la web: Datacenterknowledge.com

LA VANGUARDIA (ES-ESTILOS DE VIDA)
BARCELONA
21/07/12
Prensa: Semanal (Sabado)
Tirada: 238.004 Ejemplares
Difusión: 201.859 Ejemplares
Cód: 60163194
Página: 33
Sección: OTROS Valor: 7.895,00 € Área (cm2): 399,5 Ocupación: 64,26 % Documento: 4/4 Autor: Texto Cristina Sáez Núm. Lectores: 132000

TENER LOS DATOS EN LA 'NUBE' TIENE MUCHAS VENTAJAS, PERO ¿Y LA PRIVACIDAD?

EXISTEN SERVIDORES, COMO EL SUECO BAHNHOF EXCAVADOS EN BUNKERS

en el corazón de Estocolmo. El objetivo era, claro, la protección de la información que contenían. Y escogieron Bahnhof puesto que, además de ser el operador de internet más antiguo de Suecia, cuenta con una larga trayectoria de defensa de la libertad de expresión. Bahnhof opera cinco centros de datos en Suecia, entre los que se encuentra el famoso búnker Pionen, excavado en las entrañas de la roca.

"Se construyó durante la guerra fría para proteger a Estocolmo. Nosotros lo hemos reconstruido para proporcionar un ambiente seguro para los servicios de información que ofrecemos. La protección es tanto física (puertas blindadas y rocas sólidas) como virtual, puesto que la red de servidores está construida para que haya las máximas redundancias", explica Jon Karlung, al frente de las instalaciones de Bahnhof. Desde aquí dan servicios a organizaciones, medios de comunicación y servicios similares que no pueden verse interrumpidos y que necesitan del máximo secreto. Fue aquí, también, donde estuvo durante un año alojado Wikileaks.

Bahnhof también se beneficia de las leyes de privacidad suecas. Si bien este país tiene que cumplir con la directiva europea de derechos de propiedad intelectual que obliga a los proveedores de servicios a dar a los gobiernos los datos de quienes infrinjan esta ley, la legislación de Suecia en esta materia no obliga a retener la información del usuario, por lo que Bahnhof no lo hace. "Nos consideramos como el cartero, en un sentido moderno. De la misma forma que este no abre las cartas que debe entregar, nosotros no comprometemos el tráfico de internet de nuestros clientes. Somos un proveedor técnico neutral y no monitorizamos el tráfico –afirma Jon Karlung–. Los fundamentos de la democracia se basan en buena medida en la posibilidad de enviar o recibir mensajes sin ser controlados por una tercera parte. Y nosotros protegemos ese derecho".

Como Pionen, el búnker de Bahnhof, existen otros excavados en las rocas, en las entrañas de las montañas, con puertas antibomba, revestidos del mismo acero que llevan los tanques blindados, que son la base de los *hostings* más seguros del planeta. En Holanda, por ejemplo, está en Cyberbunker, construido por la OTAN en el año 1955, con capacidad para soportar una guerra nuclear y con el objetivo de mantener a salvo a quienes estuvieran dentro durante al menos una década.

Para Karlung, no sólo las organizaciones que manejan información delicada deben preocuparse por la seguridad de la misma en la nube, sino que todos deberíamos hacerlo. "Poder comunicarnos y ser anónimos cuando nos dé la gana es un derecho fundamental que tenemos que tener como seres humanos. ¿Por qué el Estado debería leer mis correos? Vivimos en una situación de control continuo. Ahora es hasta posible rastrear dónde hemos estado en cada momento, con quién nos hemos comunicado, cuándo... Es información poderosa que pueden usar para controlar a la gente.

Y este defensor de la libertad de expresión advierte que debemos ser más cautos a la hora de confiar nuestra información personal a empresas proveedoras de servicios en internet, como las redes sociales. "Es preferible optar por servicios que no recojan nuestros datos y que sean completamente transparentes sobre su política. Muchos creen que Google o Facebook son gratis. Pero no lo son, porque pagamos con nuestra identidad". La información, nuestra información, queda allí almacenada para siempre. ■