

Tirada: 9.425	Channel PARTNER LA WEB DEL RESELLER DE TECNOLOGÍAS DE LA INFORMACIÓN	Superficie 1.102,00 cm ²	
Difusión: 8.837		Ocupación: 100%	
(O.J.D)	Nacional Mensual	Valor: 3.500,00	
Audiencia: 30.929	Tecnología/Informática	Página: 58	1 / 4
Ref: 5059409	1ª Edición 01/10/2013		

www.channelpartner.es octubre 2013

a fondo *espionaje*

El espionaje masivo de Estados Unidos en Internet

Las implicaciones del caso Snowden

Las revelaciones del informático de la CIA delatan prácticas de espionaje masivo en Estados Unidos y vuelven a demostrar que el equilibrio entre seguridad y privacidad es muy difícil.

Juan Ignacio Cabrera



Snowden en una pantalla gigante de una calle de Hong Kong.

Edward Snowden, el joven informático que trabajó para la CIA y que a finales de mayo decidió tirar la de manta para denunciar cómo la inteligencia estadounidense pincha teléfonos y controla la navegación y el correo electrónico de millones de ciudadanos, probablemente pasará a la historia. Y lo hará porque sus revelaciones han demostrado que el espionaje masivo no es exclusivo de dictaduras, como Cuba, Irán o China, sino que cam-

pa a sus anchas en democracias modélicas como la estadounidense o la británica, donde cientos de personas se dedican a analizar la información personal que antes es cribada por potentísimos sistemas informáticos. Es decir, que el Gran Hermano que todo lo escruta está aquí, entre nosotros. Muchos, con resignación, defienden que era cuestión de tiempo que saliera a la luz un escándalo así y que era un secreto a voces que los países con sistemas políticos más irreprochables incurrieran en es-

te tipo de prácticas. Otros no lo ven mal, pues consideran que muchas empresas (las telefónicas y los proveedores de servicios de Internet sin ir más lejos) ya tienen acceso a información privada con la que podrían dar cuenta de cada aspecto de la vida de sus usuarios. Además, argumentan que estas herramientas proporcionan a policía o a los equipos que combaten el terrorismo una herramienta muy eficaz de trabajo. Los hay que, como el abogado experto en nuevas tecnologías **Alejandro**

Tirada: 9.425	Channel PARTNER LA WEB DEL RESELLER DE TECNOLOGÍAS DE LA INFORMACIÓN		
Difusión: 8.837			
(O.J.D)			
Audiencia: 30.929	Nacional	Mensual	
	Tecnología/Informática		
Ref: 5059409	1ª Edición	01/10/2013	
		Superficie 1.102,00 cm²	
		Ocupación: 100%	
		Valor: 3.400,00	
		Página: 59	
			2 / 4

a fondoespionaje

www.channelpartner.esoctubre2013

Touriño, del despacho Écija, no tienen claro la legalidad o no de este tipo de espionaje por la escasa información hecha pública hasta el momento. "El oscurantismo con el que se ha manejado el asunto hace pensar que no se hayan guardado las cautelas legales debidas, pero es muy poca la información que ha salido a la luz". En cualquier caso, el experto legal recuerda que en nuestro sistema normativo, el acceso a comunicaciones por parte de autoridades es "absolutamente restringido" y casi siempre requiere una autorización judicial previa.

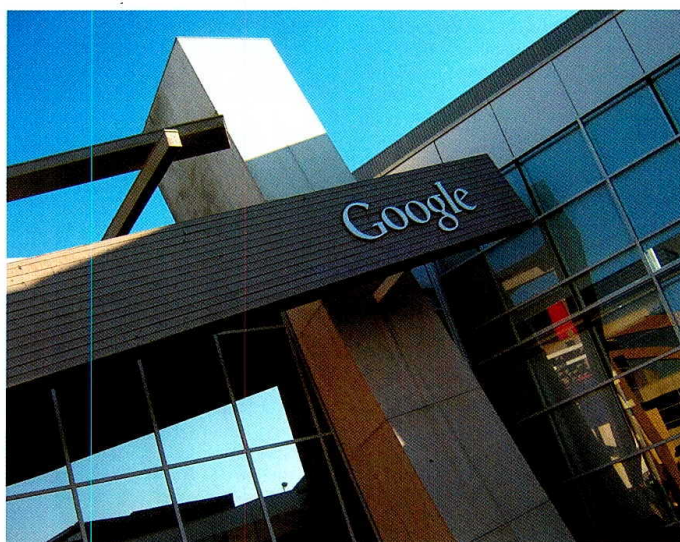
Un "absoluto atropello"

Sin embargo, hay otros que, como el propio Edward Snowden, lo ven como un absoluto atropello y avisan de los peligros de unas prácticas que nos ponen, dicen, en un escenario similar al del Gran Hermano que describiera George Orwell en su novela 1984, publicada hace más de sesenta años. "El caso Snowden supone una evidente ruptura del contrato social", dice el bloguero y profesor del Instituto de Empresa, Enrique Dans. "Lo que tenemos encima de la mesa es la evidencia de un abuso, de la construcción de una desmesurada maquinaria de control por parte de un Gobierno enloquecido. Si el caso Watergate fue un escándalo, el caso Snowden es un escándalo elevado a la enésima potencia", añade Dans. También pone el grito en el cielo Román Martín, responsable del mayorista de programas de seguridad y correo electrónico Interbel. "Habrá un antes y un después en la relación entre usuarios y proveedores de

cuerda Martín, por la Patriot Act, una ley aprobada por el Congreso de los Estados Unidos después del 11-S y que muchos han visto como una clara cortapisa a la libertad de expresión y al derecho a la intimidad, puesto que obliga a los proveedores de Internet a facilitar la información del correo electrónico de sus clientes sin ni siquiera avisarles. El experto de seguridad Chema Alonso es menos apasionado y recuerda que este caso confirma lo que ya los especialistas sabían desde hace tiempo, y es que los gobiernos, de cualquier latitud, están utilizando los sis-

La peripecia de Snowden

Snowden ahora mismo está en Rusia, con un asilo temporal de un año. Sin embargo, hasta que llegar ahí, pasó por una curiosa peripecia que le llevó de Hawai, donde vivía con su novia, a Hong Kong, donde finalmente no pudo quedarse por la presión del Gobierno chino, y posteriormente a Moscú, donde pasó semanas en las dependencias de un aeropuerto, en tierra de nadie, mientras que sus abogados le pedían asilo en multitud de países, entre ellos España. Pero volvamos al principio. A finales de mayo el analista infor-



El alcance de PRISM

Realmente poco se sabe de PRISM, puesto que el Gobierno ha prohibido publicar a The Washington Post toda la información que obtuvo de Snowden. En cualquier caso, se trata de un programa secreto usado desde 2007 por la Agencia de Seguridad Nacional (NSA) y que tiene como objetivo a ciudadanos sospechosos de terrorismo que viven fuera de Estados Unidos y a aquellos nacionales que han mantenido contacto con ellos. En principio, PRISM escruta correos electrónicos, vídeos, chat de voz, fotos, direcciones IP, notificaciones de inicio de sesión, transferencia de archivos y detalles sobre perfiles en redes sociales. Snowden también desveló presiones del Gobierno de Estados Unidos al operador Verizon para que éste entregara a la NSA todos los registros de llamadas telefónicas de sus clientes.

servicios en Internet. Éste ha sido un duro golpe a la confianza de las personas y de las empresas en la seguridad de sus datos personales". Todo viene originado, re-

temas informáticos como un arma de defensa más. Víctor Domingo, presidente de la Asociación de Internautas, coincide al señalar que "esto se sabía".

Dilema para las grandes firmas: o cumplen con sus usuarios o lo hacen con el Gobierno de los Estados Unidos

mático, de tan solo 29 años y que en ese momento trabajaba subcontratado en la Agencia de Seguridad Nacional (NSA en sus siglas en inglés) y en la CIA, saltó a la fama al ofrecer detalles a la prensa de los sistemas de espionaje que aplican estos organismos y con los que obtienen millones de registros de llamadas telefónicas y navegación de particulares que acceden a servicios de Google, Microsoft, Apple o Facebook, y que está almacenada en los

Tirada: 9.425	Channel PARTNER LA WEB DEL RESELLER DE TECNOLOGÍAS DE LA INFORMACIÓN	Superficie 1.102,00 cm²	 
Difusión: 8.837		Ocupación: 100%	
(O.J.D)	Nacional	Valor: 3.500,00	3 / 4
Audiencia: 30.929	Tecnología/Informática	Página: 60	
Ref: 5059409	1ª Edición	01/10/2013	

www.channelpartner.es octubre 2013

a fondo *espionaje*

servidores de estas compañías. Esto lo logra la NSA gracias, entre otras cosas, a un programa conocido como PRISM, que le permite ingresar directamente en los servidores de las nueve mayores empresas de Internet del país (y por lo tanto del mundo) e identificar contactos con sospechosos de terrorismo. A los pocos días de hacerse públicas las revelaciones de Snowden, Microsoft y los gigantes de Silicon Valley reconocieron que en los últimos tiempos han tenido muchas peticiones de información residente en sus servidores. En concreto, Facebook tuvo más de 9.000 solo en el segundo semestre de 2012, mientras que Microsoft reconoció que en el mismo periodo recibió más de 6.000 órdenes judiciales o citaciones relacionadas con causas criminales o con asuntos de terrorismo que afectaban a más de 30.000 personas. Además, la documentación del propio Snowden ha demostrado que el Gobierno estadounidense gratificó con millones de dólares a esas mismas compañías que le cedían los datos. Por su parte, el presidente **Obama** le quitó hierro al asunto asegurando que son prácticas normales para agencias de seguridad como la que denuncia Snowden y que hay que hacer "pequeñas concesiones" en la privacidad para luchar contra el terrorismo. En esta línea, el jefe de la NSA, **Keith Alexander**, ha asegurado que estos programas de seguimiento han evitado "docenas y docenas" de potenciales ataques terroristas y que su equipo está haciendo lo correcto para proteger a la población. Otra vez el eterno dilema entre seguridad y privacidad.

Reacción en Europa

El debate ha tenido desigual acogida a ambos lados del Atlántico. En Estados Unidos la opinión mayoritaria está de acuerdo con el espionaje si eso supone tener un país más seguro, y como mucho sus ciudadanos piden saber a qué se exponen y que políticos, jueces y policías no actúen a sus espaldas. Sin embargo, en Europa el rechazo es clamoroso. A muchos políticos, y desde luego a muchas organizaciones ciudadanas y de usuarios, no les han gustado nada las filtraciones de Snowden. Al poco de conocerse las revelaciones del informático, la comisaria europea **Viviane Reding** pidió explicaciones al Gobierno estadounidense y desde Bruselas han advertido de que las cosas podrían poner incluso en entredicho las relaciones entre ambas partes. Sin embargo, Víctor Domingo, de la Asoc-



Los expertos no creen que vaya a haber una desbandada de usuarios de las redes sociales y servicios espionados

Motivos para preocuparse

Aunque el Gobierno estadounidense ha dicho que su objetivo son los terroristas, el alcance masivo de sus herramientas hace que cualquiera con información alojada en los servidores de gigantes como Google, Facebook, Microsoft, Skype o Apple pueda ser espiado porque la legislación estadounidense lo permite. En este punto, hay que decir que de nada sirven las normas españolas, de las más protectoras en protección de datos y que tiene el derecho a la intimidad consagrado en la Constitución Española, si los servidores que guardan la información están sujetas a otra legislación. Y es que aunque las leyes españolas reiteran que la protección de datos es un derecho fundamental y autónomo, esa misma regulación establece que serán las regulaciones del país donde se hace el tratamiento de los datos las que sean vinculantes. De esta manera, como recuerda el abogado **Alejandro Touriño**, de Écija, quedan desatendidos los derechos de los ciudadanos de la UE o de España cuando los datos son tratados en EEUU, donde la seguridad ha ganado la batalla a la privacidad después del 11-S y la aprobación de la Patriot Act. Enrique Dans lo pone muy crudo cuando sugiere que un funcionario al otro lado del Atlántico puede escrutar nuestros hábitos de navegación o los contactos y mensajes que enviamos. "Puedes ser juzgado ya no por lo que hagas, sino por lo que otros, con tendencia a la paranoia, puedan pensar que pretendes hacer. Es completamente demencial", avisa el bloguero y profesor.

ciación de Internautas, cree que los ciudadanos occidentales están convencidos de que si no tienen nada que ocultar no tienen por qué preservar su privacidad, lo que facilita que los Gobiernos actúen "con total impunidad". Enrique Dans dice que un procedimiento automatizado de registro de correos y llamadas sin una orden judicial específica es "intolerable" y que si

hay ciudadanos que lo consienten, entonces habrá que "reeducarlos". El abogado Touriño, del despacho Écija, le quita hierro al asunto y cree que las revelaciones de Snowden no van a cambiar nada. "Es cierto que el asunto PRISM ha dado para escribir ríos de tinta, pero no menos de los que en su día se generaron con las llamadas 'puertas traseras' en programación

Tirada: 9.425	Channel PARTNER LA WEB DEL RESELLER DE TECNOLOGÍAS DE LA INFORMACIÓN	Superficie 1.102,00 cm²	 
Difusión: 8.837		Ocupación: 100%	
(O.J.D)	Nacional	Valor: 3.500,00	4 / 4
Audiencia: 30.929	Tecnología/Informática	Página: 62	
Ref: 5059409	1ª Edición	01/10/2013	

www.channelpartner.es octubre 2013

a fondo *espionaje*

de sistemas como Netscape o Windows, los cuales, como en su momento se decía, permitían acceder a quienes habían desarrollado el código a la información distribuida a través de esos sistemas".

Los dilemas de Silicon Valley

Las revelaciones de Snowden también han abierto un debate en los grandes de servicios de Internet y en sus millonarias bases de usuarios. Compañías como Google, Facebook, Skype o Twitter están entre la espada y la pared, puesto que por un lado deben preservar los datos de sus clientes, pero por otro tienen que cumplir con las autoridades estadounidenses y con la

gente normal no se preocupa demasiado por estas cuestiones y seguirá cómoda y como hasta ahora mientras siga pensando que no tiene nada que ocultar. "Pasó lo mismo con las cámaras de seguridad en las ciudades, y los sistemas de control de voz como Sitel". Para Enrique Dans, los usuarios no deberían tomarla con las empresas, puesto que estas "son el es-

ra operar en Europa", señala Chema Alonso. Román Martín, de Interbel, cree que las compañías deberían "pensarlo dos veces" antes de dejar sus datos en un proveedor alojado fuera de Europa. Por su parte, Enrique Dans considera que los gigantes de Internet deberían impedir la violación de los derechos fundamentales rechazando toda petición de información

*Para Enrique Dans,
estamos ante una
evidente ruptura del
contrato social*

Patriot Act. Por el momento han respondido reconociendo el espionaje y pidiendo que las autoridades sean más transparentes a la hora de realizar estas prácticas. Pero, como recuerda el bloguero experto en seguridad Chema Alonso, tienen muy poco margen de maniobra e incluso en las notas de prensa que han elaborado para reconocer la intervención de sus servidores no pueden revelar, por imperativo

*Para el abogado
Tourinho, las revelaciones
de Snowden no van a
cambiar muchas cosas*

legal, todo lo que saben. El abogado Alejandro Tourinho, del bufete Écija, cree que si una norma exige este tipo de revelaciones, el contrato que vincula a los usuarios de una red social no se rompe y no se vulnera el deber de confidencialidad, aunque reconoce que si el control de las comunicaciones persiste los usuarios irán perdiendo confianza.

El usuario medio queda al margen

En cualquier caso, nadie espera una desbandada de usuarios de redes sociales o servicios de correo a causa de las revelaciones de Snowden. Alonso cree que la

labón débil de la cadena de responsabilidad que se inicia en el presidente Obama y que continúa por toda su administración". Donde sí pueden cambiar las cosas es entre Gobiernos y empresas, como ha demostrado la actitud exigente de la Unión Europea. "La UE está demandando más información, y en función de los resultados de la Comisión es probable que se endurezcan las leyes de privacidad pa-

que no vaya acompañada de una "petición judicial expresa". Sin embargo, la mayoría de consultados están convencidos de que las tecnológicas no tienen mucho margen para ello hoy en día, a no ser que una legislación internacional en la materia tomara cuerpo. La pelota sigue, pues, en el tejado de los Gobiernos (y de los ciudadanos si se ponen serios piden explicaciones a los políticos).

Espionaje en el Reino Unido

Estados Unidos no está solo en esta historia. Los espías estadounidenses también tienen alumnos aventajados en el Reino Unido, donde no sólo potenciales terroristas están en el punto de mira, sino diplomáticos y embajadas de países europeos y de la Unión. La delegación de políticos turcos que asistió la reunión del G-20 en Londres en 2009 fue espía desde que pusieron pie en territorio británico. En el Reino Unido, este tipo de actos está amparado por una ley aprobada en 1994 que pone el interés económico nacional por encima de la cortesía diplomática. Edward Snowden también ha desvelado que el espionaje británico pincha los cables de fibra óptica que pasan por su territorio y que forman parte del mallado mundial de comunicaciones.

Poco margen para el Gobierno español

El espionaje masivo que hacen las fuerzas de seguridad estadounidenses ha sido muy criticado en Europa. Aunque solo sea de cara a la galería, los dirigentes del viejo continente han criticado la opacidad de la administración de Obama en este terreno. Es la línea que se han manifestado los altos funcionarios de la propia Unión Europea y dirigentes como Ángela Merkel, la canciller alemana, que ha dicho que las escuchas al personal de embajadas por parte de los servicios de inteligencia de Estados Unidos y del Reino Unido son "intolerables" y propias de la guerra fría. "Creo que Europa endurecerá las leyes de privacidad para sistemas cloud", pronostica Chema Alonso. Por el momento, el Gobierno español no se ha pronunciado de forma clara sobre el asunto. Además, según los consultados, tiene poco margen. Víctor Domingo, de la Asociación de Internautas, cree que está deslegitimado en este asunto por cuanto ha puesto en marcha un software (Sitel) que intercepta llamadas y navegación de Internet y que "no está regulado por una ley orgánica" que dé garantías de que siempre va a estar bajo supervisión de un juez. Román Martín, de Interbel, propone que el Gobierno español haga como el sueco, que ha prohibido el uso de programas de Google en la nube, como Gmail o Calendar, por no poder garantizar la confidencialidad de la información que se deposita en ellos.