tsantsa
REVISTA DE INVESTIGACIONES ARTISTICAS
FACULTAD DE ARTES/ UNIVERSIDAD DE CUENCA
Nº 2 Diciembre 2014

# LA INFORMACIÓN Y PRIVACIDAD EN LA ERA DIGITAL

## INFORMATION AND PRIVACY IN THE DIGITAL AGE

Ernesto Antonio Santos León
Universidad de Cuenca (Ecuador)

Recibido: 27 de mayo del 2014
Aceptado: 30 de junio de 2014

**Resumen:**
*Con el desarrollo y evolución de Internet se generan nuevos planteamientos, en especial sobre los datos: ¿Cómo se maneja la información ahí almacenada?, ¿qué sucede con los datos privados de los usuarios?, ¿qué sucede con el contenido generado en Internet? En la última década el mundo ha escuchado diversas voces hablar sobre el tema, mostrando lo que hacen las empresas con la información.*
*La publicación es un análisis a la situación actual, es un incentivo a pensar críticamente sobre nuestra información y privacidad en el internet.*

**Palabras clave:** Internet, privacidad, Julian Assange, Edward Snowden, web, información, datos, derechos humanos, CIA, NSA, Web profunda.

**Abstract:**
*With the development and evolution of the Internet, it's generated new approaches, in particular about the data. How the information stored is handled there? What happens with the private data of users? What happens with the generated content in the Internet? In the last decade the world has seen several voices talking about it, showing what companies do with the information.*
*The publication is an analysis of the current situation; it's an incentive to think critically about our information and privacy in the Internet.*

**Keywords**: Internet, privacy, Julian Assange, Edward Snowden, web, information, data, human rights, CIA, NSA, deep web.

* * * * *

## 1. La información y privacidad en la era digital

Un gran debate se vive actualmente en el mundo sobre el manejo de la información y la privacidad desde que el australiano Julian Assange empezó a desclasificar información en su sitio *Wikileaks* en el año 2007, liberando información confidencial de algunos gobiernos, en especial sobre el accionar de los Estados Unidos en el mundo, las guerras en Irak, Afganistán y políticas de espionaje entre otros hechos. Dicho tema ha tenido mayor relevancia en lo que va del año cuando en 2013 Edward Snowden, que fue parte del personal de la CIA (Agencia Central de Inteligencia) y NSA (Agencia Nacional de Seguridad) de los Estados Unidos, desclasificó información relacionada al espionaje que llevaba a cabo los Estados Unidos en el mundo, incluyendo a sus países aliados.

La verdad, este tema no debería sorprendernos, ya que estos sucesos se han desarrollado desde hace mucho tiempo, pero recién le damos la relevancia debida. Muchos de los sistemas digitales en *Internet* que utilizamos de forma habitual, como *Outlook, Facebook, Google, Gmail, Instagram, LinkedIn*, de los cientos existentes, gratuitos por así decirlo, porque en realidad tienen un alto costo, los pagamos con uno de los capitales más valiosos, con nuestra información, con nuestro contenido. Este acto se realiza bajo nuestro consentimiento, en el momento en que aceptamos los Términos de Uso y/o Políticas de Privacidad al crear las cuentas en los diferentes servicios que, por lo general lamentablemente no procedemos a leer.

Dependiendo del tipo de sistema las políticas pueden variar. Sin embargo, hay términos comunes y relevantes entre ellos. A mi criterio los más importantes son dos:

- Los usuarios ceden los derechos sobre el contenido generado por ellos mismos en dichos sistemas de manera directa o indirecta. En casos como *Facebook, LinkedIn* o *Instagram*, permiten la transferencia de manera no exclusiva y la sub-licencia del contenido. Es decir, las empresas lo pueden utilizar a su conveniencia, para su promoción o en algunos casos su venta.

- La empresa puede proporcionar la información de los usuarios a terceros en situaciones de seguridad nacional, para investigar y prevenir actos criminales, ya sean empresas gubernamentales o privadas. Es decir, la CIA puede solicitar el historial de un usuario o grupos de usuarios si lo requiriese.

Una de las razones principales de entregar la información a terceros es la Ley Patriota en los Estados Unidos, promulgada en el mes de octubre del 2001. Luego de los atentados terroristas del 11 de septiembre de dicho año, la ley amplió la capacidad de control e investigación por parte de los Estados Unidos en cualquier tipo de sistema, sea análogo o digital, con motivo de descubrir y evitar posibles nuevos atentados terroristas. Antes de esa ley los diversos sistemas pregonaban nunca entregar la información de sus usuarios[1].

El debate actual es si debemos o no permitir el acceso a nuestra información por parte de terceros, ¿Qué sucede con nuestra privacidad?, ¿Qué hacen los sistemas y/o empresas con nuestra información? En diciembre del 2011, en una rueda de prensa, Julian Assange desclasificó 287 archivos de espionaje a nivel mundial, mostrando como la información se vende al mejor postor, tanto a naciones democráticas como

[1] Hoback, Cullen, *FILM Terms and Conditions May Apply*, 2007.

dictatoriales[2]. Es decir, a pesar que existen leyes que permiten de una u otra manera acceder a la información y vulnerar la privacidad, igual nos espían. Una forma de realizarlo es mediante un denominado DPI, *Deep Packet Inspection* (Paquete profundo de inspección)[3], un algoritmo que discrimina la información en *Internet* que se ha utilizado en sistemas como *Carnivore* -luego renombrado DSC1000- por parte del FBI o el *Narus*, usado por la NSA.

El historiador cultural de nuevos medios Siva Vaidhyanathan, habla de unos ejemplos de control de información por parte de *Google*: la "googlización" del todo. Google, además de ser el buscador más utilizado en el mundo, es dueño de diversos sistemas que también son los más usados en *Internet.* Por citar a algunos, *Google Analytics* (Estadísticas de sitios *Web*), *Gmail* (Servicios e-mail), *Youtube* (Videos) y *DoubleClick* (Anuncios y publicidad)... Con toda la información que almacena *Google* se pueden generar perfiles psicográficos, delimitar nuestros gustos y las preferencias que tenemos sobre las cosas. Poseen el contenido más valioso en *Internet*, que es la información de las personas (Vaidhyanathan), y de igual manera poseen la información que está inmersa en la *Web*, a razón de su sistema de indexación de contenido, el cual rastrea todos los sitios en la *Web* y guarda automáticamente un respaldo de todos ellos. Es decir, por más que borrásemos la información de un sitio o todo el sitio, existiría el respaldo de dicha información en la memoria Caché de *Google*, a la que no tenemos acceso para su modificación.

Con respecto a la información en los medios digitales, Henry Jepkins en su *libro La cultura de la convergencia*, define que con la masificación de *Internet* en los años 90, el nuevo modelo de conocimiento es la inteligencia colectiva. Citando a Pierre Lévy "*Ninguno de nosotros sabe todo, cada uno de nosotros sabe algo, por tanto todo el conocimiento está en la humanidad*" [4]; *Internet* no es más que computadores conectados compartiendo información, y quien tenga acceso a toda esa información, tiene acceso a todo su conocimiento.

En TED (Tecnología, Educación y Diseño), que es un evento a nivel mundial de charlas magistrales de expertos en temáticas relacionadas al desarrollo de la humanidad, en marzo del 2014 Richard Ledgett, subdirector de la NSA, luego del debate generado por Edward Snowden, le responde al mundo aseverando que la NSA debe monitorear *Internet* como uno de sus deberes en búsqueda de la seguridad Nacional [5]. Una afirmación errónea justificada equívocamente por un grupo de leyes en los Estados Unidos que no deberían regir a todo el mundo. Ante ello han existido otros frentes. Por ejemplo, la Unión Europea, que está consciente del valor que posee la privacidad para las personas, en el año 2012 aprobó una ley regulando que las páginas web que posean sistemas de recolección de la información de los usuarios como *Cookies*, han de solicitar permiso a los usuarios para el debido rastreo, de igual manera en el año 2014, en la Unión Europea se ha presentado una reforma a la legislación de protección de datos personales. Se espera que sea aprobada hasta mediados del 2014 y busca proteger los datos privados de los usuarios de un manejo ilícito y abusivo por parte de las empresas.

[2] Amin, Rima. *Youtube* <www.youtube.com/watch?v=Q3zpLefXOP4> (Mayo de 2014).
[3] Paganini, Pierluigi y Richard Amores, *Deep Web*, USA: Smashwords, 2012.
[4] Jenkins, Henry, *Convergence Culture: Where Old and New Media Collide*, USA: NYU Press, 2008, Localización Kindle 210-211.
[5] Ted.Com. *TED* <www.ted.com/talks/richard_ledgett_the_nsa_responds_to_edward_snowden_s_ted_talk> (Marzo del 2014).

De igual manera, frente al control generado en *Internet*, existe la denominada *Web* Profunda (*Deep Web*). Es todo el contenido que no se encuentra indexado por los navegadores (*Google*, *Yahoo*, entre otros), y al que no se puede acceder de la manera tradicional. La información inmersa es difícil y en algunos casos imposible de rastrear. A este contenido se puede tener acceso de diferentes maneras: mediante sistemas que oculten nuestra IP (el número que identifica a nuestro computador en la red y le permite ser rastreado), se lo puede hacer mediante un PROXY (suplantar un IP), VPN (Red Privada Virtual), o el más utilizado por personas que no quieren lidiar con configuraciones complejas: TOR (*The Onion Routing Project*, o bien, en español Proyecto Ruta Cebolla). Dicho nombre, asignado porque se navega en la red *Onion* o Cebolla, se caracteriza porque al final del nombre del dominio se utiliza el .ONION[6]. El contenido en este nivel muchas veces es asociado con el mundo de crimen, terrorismo, venta de información y pornografía. La verdad es que no es muy diferente del contenido que también se puede encontrar en la *Web* indexada, en la cual dichos elementos también están presentes. En la ética de los medios digitales (ESS) nos comenta que internet es solo una herramienta que es utilizada por las personas para representar todas las facetas ya existentes de nuestra humanidad, sean buenas o malas.

Navegar en la web profunda nace de la necesidad de controlar nuestra privacidad, un lugar donde no seamos monitoreados, dónde no nos tomen como un producto cuantificable, estadístico, de promoción y explotación para el beneficio de otros; exponer nuestra información, es vulnerar y violar parte de nuestros derechos como personas e individuos.

Existe la otra cara de la moneda, los que pregonan que la privacidad no existe en el internet, personas y usuarios que no poseen conflicto en entregar su información, sus datos, su contenido, en algunos casos con el argumento que no tienen nada que esconder en la información generada. Frente a eso pregunto: ¿serían capaces de permitir la entrada a cualquier persona a su casa?, ¿mostrarían las cosas que ahí tienen? Claro, asumiendo que no haya nada que ocultar, nada malo en su poder, ¿serían capaces de entregar su celular todos los días para que un extraño lo revise y copie los datos registrados? El principio de privacidad, sea o no en un sistema digital, seguirá siendo el mismo: la definición de privacidad en la Real Academia Española es el "*Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión*"[7].

También están los usuarios que apoyan el sentido estricto de la evolución de *Internet*. La *Web* semántica, los datos que obtienen los usuarios en la *Web* se desarrollan en base a sus preferencias de búsqueda. El sistema determina qué es lo relevante para cada usuario, es decir, la *Web* semántica es un sistema inteligente que nos muestra la información en base a nuestros gustos y necesidades. Siendo una de las características de la denominada y actual *Web* 3.0, la *Web* semántica debe recopilar nuestros datos e información para su desarrollo como un sistema inteligente. Ese no es el problema, sino los usos posteriores de la recopilación de información por parte de las empresas, por parte de entes gubernamentales para un control y monitoreo.

Personalmente, y no soy el único en pensarlo, los estados deben comprender la problemática actual, la necesidad de generar nuevas normativas y leyes que protejan nuestros datos, nuestra privacidad, dentro de un marco legal común para todos,

[6] Paganini, Pierluigi y Richard Amores, *Deep Web*, USA: Smashwords, 2012.
[7] Española, Real Academia. *Real Academia Española* <www.rae.es> ( Mayo de 2014).

fundamentándonos en la Declaración Universal de los Derechos Humanos. Como lo indica el artículo 12 "*Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques*"[8]. *Internet* no lo hace un grupo de personas, un estado o un solo continente, sino todos los participantes inmersos: toda la humanidad. *Internet* no es para un grupo, es para todos... "*Yo soy, porque todos somos*"[9].

**Bibliografía:**

Amin, Rima. *Youtube* <www.youtube.com/watch?v=Q3zpLefXOP4> (Mayo de 2014).
Española, Real Academia. *Real Academia Española* <www.rae.es> (Mayo de 2014).
ESS, Charles, *Digital Media Ethics*, USA: Polity Press, 2014.
Hoback, Cullen, *FILM Terms and Conditions May Apply*, 2007.
Jenkins, Henry, *Convergence Culture: Where Old and New Media Collide*, USA: NYU Press, 2008.
Paganini, Pierluigi y Richard Amores, *Deep Web*, USA: Smashwords, 2012. Ted.Com. *TED* <www.ted.com/talks/richard_ledgett_the_nsa_responds_to_edward_snowden_s_ted_talk> (Marzo del 2014).
Unidas, Naciones. *Declaración Universal de los Derechos Humanos* <www.un.org/es/documents/udhr> (Mayo de 2014).
Vaidhyanathan, Siva. *La Googlización del todo*. México: Océano, 2012.

[8] Unidas, Naciones. *Declaración Universal de los Derechos Humanos*. <www.un.org/es/documents/udhr> (Mayo de 2014).
[9] Este lema, proveniente de la ética sudafricana "Ubuntu", enfocada en la comprensión de la existencia propia en relación con la de los demás, es representativo también de un sistema operativo homónimo (UBUNTU) distribuido con software libre.