Sobre la privacidad

por

José Luis Garrido Labrador
y
Damián Gómez Chayán

Universidad de Burgos 10/2015

Índice de contenido

¿Qué es la privacidad?

Aunque la RAE define la privacidad como "el ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión[1]" su definición debería completarse, desde mi punto de vista la privacidad es más que eso, la privacidad también es el derecho al anonimato, el hecho de que nadie pueda conocer datos de ti con solo buscarte en Internet, algo que hoy en día es prácticamente imposible, ademas la definición de la RAE es demasiado ambigua pues cada persona puede tener una consideración diferente de lo que es la vida privada.

En este documento vamos a intentar poner un poco de luz sobre este tema que sin darnos cuenta forma una parte fundamental de nuestra vida y que cada día va disminuyendo para bien y para mal.

Redes sociales, ¿respetan la privacidad?

Las redes sociales ya son un cliché en nuestra sociedad, desde las más genéricas como Facebook o Twitter hasta las más específicas como LinkedIn o Instagram están por todos lados. Hoy en día prácticamente todo el mundo participa en alguna red social y estas se usan con cierta despreocupación. Sin embargo las redes sociales pueden ser muy perjudiciales para nuestra privacidad ya que en ellas publicamos prácticamente todo lo que hacemos o nos pasa. ¿Nos hemos preguntado alguna vez por que Facebook, Twitter, Tuenti o Instagram son gratuitas? Los servidores, la programación de la web, el almacenaje de datos entre otras muchas cosas que se utilizan para mantener la web en red tienen un coste y este es más elevado cuanto más usuarios utilizan la red, pues bien, lo que sucede es que nuestros datos una vez publicados ya no son completamente nuestros, ya que la página puede hacer con ellos lo que hayan estipulado en los términos y condiciones de servicios (esos que poca gente lee).

Por ejemplo, al usar Facebook[2] estamos autorizando que venda nuestra información e imagen para que esta se use por terceros para vender publicidad. Imagina que te gusta la marca "Z4p4till4s", y que a tu amigos le aparezca un anuncio en Facebook que pone "Nueva oferta de Z4p4till4s, a tu amigo le gusta esto". Esa información tuya se esta vendiendo con tu consentimiento y sin ninguna remuneración. Otra cosa importante en esta red y en otras muchas es que la configuración por defecto de la privacidad no protege tus datos, como se puede ver en el vídeo adjunto.

1 Privacidad en la RAE
2 TOS Facebook

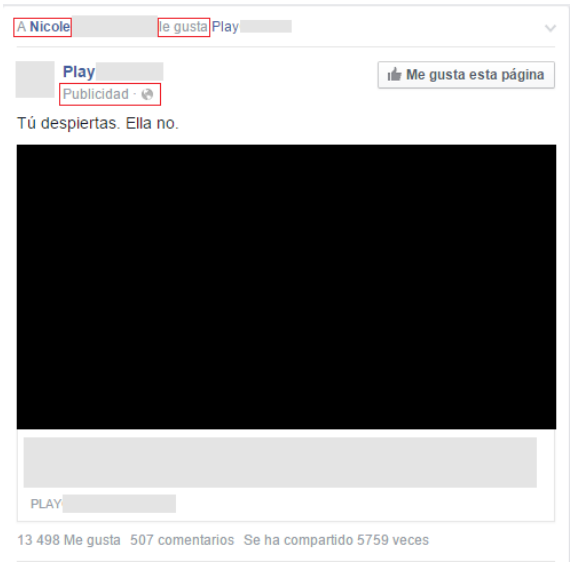

Ilustración 1: Ejemplo de uso de tu nombre para vender publicidad

Otro caso es Twitter[3] en el que todo lo que publicas es tuyo pero otorgas una licencia mundial a la empresa para utilizar tus datos con fines propios sin que tú recibas ninguna compensación. Además de que todo lo que publicas en Twitter es por defecto público y ya depende del usuario ser responsable de lo que publica.

Hace pocos meses Richard Prince subastó fotografías de famosas que estaban colgadas en Instagram[4], cada una por la cantidad de cien mil dólares. Lo que hizo Prince no es muy ético pero no contradijo ninguna norma, la red social no ha tomado represalias por lo que hizo porque no contradijo las políticas de la red, ya que estas desde diciembre del 2012 permiten la venta de las fotos a terceros sin notificar o compensar al dueño.[5]

Las redes sociales están hechas para fomentar la comunicación entre personas de todo el mundo, desde foros, blogs comunitarios o las redes como Facebook, todas están enfocadas para la comunicación, eso significa que todo lo que publicas en ellas, ya sea un *post* en 4Chan, un artículo en Taringa o un vídeo en YouTube, todo está en la gran red de información y aunque lo tengas muy protegido, lo que publicas ya no es del todo tuyo. Tu historial de navegación se venderá para que veas publicidad acorde con lo que visitas. Si eres un fan de los caballos probablemente verás anuncios sobre caballos y pensarás "¿Cómo sabe YouTube que me gustan los caballos?" o "¿De dónde sale tanta publicidad sobre alquiler de establos?" y es porque esa información que creías secreta no lo es. Las redes sociales por defecto no respetan la privacidad, y aunque lo protejas por tu cuenta aun así esa información sigue guardada en una gran base de

3 TOS Twitter
4 Esta foto robada cuesta 100.000 dólares – El País
5 TOS Instagram

datos de la cual no se tiene ningún control.

Hay una frase en Mateo 10, 26 que dice *"Nada hay encubierto, que no haya de ser manifestado; ni oculto, que no haya de saberse"* y la verdad es que es una realidad, el hacker español Chema "Maligno" Alonso ha comentado que las redes sociales no son seguras debido a la cantidad de herramientas que existen[6] para obtener información de datos antiguos o que creemos borrados. Todo lo que se haya publicado en una red social, un blog o cualquier sitio de Internet no está oculto, es vulnerable a que se acabe desvelando o filtrando y si no tienes un control absoluto sobre el material en red puede también ser vendido a tu costa. Lo que pasa en Internet no es por definición privado. Los usuarios de Ashely Madison[7] creyeron que por borrar sus datos se eliminarían todos, pero no fue así ya que estos se expusieron al público, y ya sea por acción de la red social o de un pirata informático hay que ser cautelosos con lo que hacemos en linea.

No hay que ponerse paranoico con el tema ni mucho menos, más allá de acabar con las redes sociales sería mejor ponerse a pensar que es lo qué realmente queremos que se sepa de nosotros de manera pública y que lo qué queremos qué sea privado permanezca en privado. Las redes sociales no se hicieron ni se hacen para proteger nuestra privacidad y es nuestro deber estar al tanto de que es lo que hacemos en ellas.

Las redes sociales pueden ser muy útiles para el hombre de hoy en un mundo tan globalizado, pero es importante que se sea íntegro en las redes, comportarse en ellas de la misma manera que nos comportamos en la vida "real" para no tener ningún problema en el futuro del que uno se pueda arrepentir.

6 Chema Alonso: 'Soy uno de los mejores hackers de España y del mundo' | Salvados
7 'Hackean' Ashley Madison y amenazan con delatar a 37 millones de adúlteros – El Confidencial

¿Cuánto nos exponemos?

Actualmente el nivel de exposición de nuestra persona es muy elevada, llegando a publicar numerosos detalles de nuestra vida privada en Internet, un buen ejemplo de esto son las redes sociales, como *"*Facebook o Twitter*"* en las que publicamos no solo comentarios de lo que hacemos en nuestro día a día si no también fotos y vídeos, a esto hay que incluir los datos que le facilitamos a los administradores de la red social para crear nuestro perfil, y los datos que estos almacenan automáticamente referidos a búsquedas recientes, gustos personales, etc. datos que pueden ser usados en el mejor de los casos para mostrarnos anuncios personalizados y en el peor de los casos pueden ser vendidos a otras empresas interesadas. El problema que estamos teniendo en las redes sociales es que no somos conscientes de las consecuencias que puede tener lo que estamos publicando, es algo nuevo y por lo tanto el impacto que tienen estas cosas se esta empezando a ver ahora, con demandas por uso de fotos[8] en Facebook, etc

Google multa a sus usuarios[9] de fibra óptica por descargar contenidos con copyright, ¿hasta que punto es legal y moralmente permisible que los ISP puedan analizar nuestro trafico de datos, webs que visitamos, descargas que realizamos y demás? Este análisis del trafico de datos por parte del ISP no deja de ser algo parecido a lo que la NSA hace con los ciudadanos estadounidenses, pues el proveedor de Internet, en este caso Google, tendría no solo información sobre que webs visitas, también a tus conversaciones VoIP y videollamadas, correos, chats, etc. En España la norma es más ventajosa para el usuario ya que el ISP requiere de orden judicial para mostrar el trafico de datos de un cliente.

Hay una noticia[10] reciente referida a este tema, en la que se pone de manifiesto la vulnerabilidad de nuestros datos, no solo los que difundimos por voluntad propia, también los datos que las páginas almacenan sobre nosotros. En esta noticia el tribunal de Irlanda invalida el tratado "safe harbor" que permitía a grandes empresas tecnológicas de fuera de Europa almacenar datos de sus usuarios europeos fuera de Europa, algo que esta prohibido por la ley de protección de datos europea; en el tratado "safe harbor" aparecen nombres como Facebook, Google...

El estudiante de derecho Max Schrems fue el que interpuso la denuncia, alegando que si los datos privados de los ciudadanos europeos se almacenaban en EEUU, agencias como la NSA podrían tener un fácil acceso a estos datos, ya que como filtro Edward Snowden la NSA tenia acceso directo a los servidores de grandes empresas del sector, tanto redes sociales como empresas de telecomunicaciones.

El caso de la NSA destapado por Edward Snowden fue uno de los casos más famosos

8 Una mujer demanda a la DEA por utilizar sus fotos en un perfil falso de Facebook - ABC
9 Google fiber sends automated privacy "fines" to suscribers – TorrentFreak
10 Ireland, Facebook's European base, pushed to act on 'safe harbour' ruling – The Guardian

referentes al espionaje por parte de órganos del gobierno a sus ciudadanos, contando incluso con varios libros y una película[11] (ganadora del Oscar al mejor documental largometraje en 2014), Snowden dio a conocer que la NSA registraba datos de millones de ciudadanos, incluso pudiendo grabar conversaciones de teléfonos VoIP, (también menciona otros métodos de espionaje que gobiernos como el británico llevaba a cabo con sus ciudadanos) el descubrimiento del espionaje de la NSA y su escudo en la ley patriota dio lugar a uno de los debates mas grandes respecto a este tema, "¿qué es más importante? ¿La privacidad o la seguridad?"

Pero no solo las empresas pueden manipular y usar datos sobre nosotros como quieran, otro ejemplo son los hacker, personas capaces de romper la seguridad de servidores y dispositivos electrónicos,. Recientemente un grupo de hackers chinos accedió a Looppay (misma empresa tras Samsung Pay), dejando ver una brecha de seguridad en aplicaciones de pago NFC de numerosos dispositivos móviles, obteniendo los datos bancarios y tarjetas de crédito de sus usuarios, esto se podría equiparar a robar la cartera a millones de personas al mismo tiempo. El debate que se realiza ahora es "¿Es seguro usar este tipo de aplicaciones?", empresas como Samsung (proveedores de este tipo de aplicaciones[12]) en unas declaraciones recientes[13] insisten en que ni sus usuarios ni sus datos corren peligro, sin embargo este tipo de servicios tienen menos clientes que antes del hackeo, creo que si es cierto que existe un riesgo en usar este tipo de aplicaciones, pero ese riesgo también se aplica en menor medida al simple hecho de tener una cuenta bancaria, ya que todos tus datos se almacenan en sus servidores, a los cuales se puede acceder de forma ilegal para obtener sus datos.

Otro tema actual con respecto a la privacidad y seguridad de nuestros datos son las nubes, como se menciona en The Guardian[14] las compañías intentan "vender" la nube como solución a los problemas de espacio en nuestros dispositivos, sin embargo nunca mencionan que estas nubes son objetivo de numerosos hackers, pues en un solo lugar se almacenan datos (mensajes, fotos, vídeos..) de millones de personas. Un ejemplo reciente con bastante repercusión mediática fue el hackeo de iCloud[15] del año pasado.

La nube es una gran herramienta para liberar espacio de tu disco duro pero hay que usarla con prudencia, lo ideal es evitar la sincronización de fotos privadas de manera automática para que estas no se suban a la nube, donde son más vulnerables, además hay servidores de "nube" mas seguros que otros según su cifrado.

11 Citizenfour Official Trailer 1 (2014) - Edward Snowden Documentary HD
12 Samsung Pay
13 Chinese Hackers Breached LoopPay, Whose Tech Is Central to Samsung Pay – New York Times
14 How we talk about the cloud shapes the way we perceive internet privacy – The Guardian
15 Gang of hackers behind nude celebrity photo leak routinely attacked iCloud – The Guardian

¿Es posible la privacidad en Internet?

Actualmente hay pocas formas de navegar de forma anónima por Internet, y ninguna es infalible. Entre las más conocidas se encuentra el navegador Tor[16], conocido como el navegador cebolla[17], este navegador de código abierto es completamente gratuito y puede descargarse desde su pagina web. El navegador cebolla se hizo popular en los últimos años como el navegador definitivo para navegar y realizar transacciones en la *deepweb* ya que la mayor parte de cosas que podemos encontrar en esta web son ilegales, desde venta de productos robados, armas, drogas, etc, hasta vídeos de asesinatos, crueldad animal o pornografía infantil. Sin embargo el *onion routing* en el que se basa Tor no nació con estos objetivos, nació como un proyecto de la marina de los estados unidos con fines militares, este origen militar es lo que causa que mucha gente desconfíe de la privacidad que ofrece Tor.

El *onion routing* es un método por el cual en lugar de acceder directamente a los servidores de una pagina web o servicio, lo hacemos mediante servidores intermediarios, nuestros paquetes solicitando acceso a la web se manda de forma cifrada por capas (como una cebolla) de esta forma cada servidor descifra una capa y cifra la anterior hasta llegar a la última que contiene el servidor al que queremos llegar de manera que se obtiene una conexión mucho mas segura pero no infalible. A pesar de la alta seguridad del navegador cebolla este no es el navegador predeterminado de nadie, pues aunque su seguridad sea muy alta es a costa de la velocidad de conexión, pues el acceder a los servidores mediante intermediarios alarga mucho el tiempo de espera hasta que puedes acceder a la pagina web, ademas el uso de *plugins* o aplicaciones de terceros tienen el efecto contrario eliminando todo lo conseguido con Tor, ya que algunas aplicaciones difunden nuestra IP al conectarse, u otras como FlashPlayer que tiene numerosos agujeros en su sistema de seguridad.[18]

Además de en su versión navegador hay una distribución Linux (TAILS) que basa todas sus conexiones a Internet en el sistema *onion routing* de Tor, garantizando de esta forma que ninguna aplicación recolecte o difunda datos en Internet que puedan comprometer nuestro anonimato. TAILS como casi todos las distribuciones Linux es gratuita siendo posible su descarga desde su pagina web. (TAILS tiene un problema de compatibilidad con sistemas UEFI[19]). Otro método sería mediante el uso de *proxys*, que no deja de ser lo que hace el navegador Tor pero de forma manual, es decir, nosotros escogemos que intermediarios usar al conectarnos a determinados servidores.

16 Lo que Google no ve – El País
17 Así funciona Tor – El País
18 El Incibe alerta de un fallo de seguridad en Adobe Flash Player que puede provocar pérdida de información – 20 Minutos
19 ¿Qué es UEFI?

El último método para conectarse a Internet de forma anónima seria configurando manualmente cualquier navegador para usar *proxys*. Cabe mencionar que todos estos métodos de navegación privada son inútiles al identificarnos en paginas de redes sociales, pues de este modo estamos proporcionando nuestros datos de forma voluntaria.

Mucha gente opina que estos métodos para navegar de forma anónima no deberían existir, ya que el anonimato fomenta el hacer cosas que no se deben, como venta de productos robados, drogas, armas, pornografía infantil... pero yo considero que Tor y otras formas de privacidad están ahí para los usuarios que quieren privacidad, la gente que actualmente usa el navegador cebolla para esos actos ilegales encontraría otra forma de seguir haciéndolo, volverían a hacerlo como antes de existir Internet. Además el crecimiento de estos negocios ilegales se debe en gran parte al uso del *bitcoin*, una moneda virtual con la que se puede pagar en la *deepweb* sin ser rastreado hasta el momento de cambiarlo a monedas física, lo cual se hace difícil debido a un sistema de “blanqueo” de por el cual tus *bitcoins* son cambiadas por otras del mismo valor (menos la comisión) que estaban alojadas en el servidor. De esta forma se hace mucho mas difícil rastrear la procedencia de esos *bitcoins*.

Privacidad y bien común ¿qué debe primar?

Un gran dilema moral que se tiene respecto a la privacidad, es en los casos en que la privacidad afecta al bien común. La ley ampara que para resolver un delito o crimen se puedo eliminar el derecho a la intimidad, ya sea para obtener historiales médicos, imágenes de vigilancia, *cookies* del navegador etc[20]. Además la *Constitución Española* limita el uso de la informática para proteger la intimidad de las personas[21]. Sin embargo la situación puede ir mucho más allá. En Estados Unidos, tras los acontecimientos del 11-S se crearon muchas leyes para evitar sucesos parecidos, entre ellas, las que nos ocupa es la Ley Patriota[22], que reduce la privacidad de las personas en aras de combatir el terrorismo, actualmente en Francia tras lo acontecido en el semanario *Charlie Hebdo,* se ha aprobado una ley que permite sin control judicial interceptar comunicaciones[23].

Es bueno que un estado cree infraestructuras contra el terrorismo pero ¿debe ser a costa de la intimidad de las personas? Tras el 11-S se crearon otras muchas leyes para evitar el mismo desastre, y muchas de ellas no atentaban contra la privacidad. Es cuestión de buscar medios útiles no perjudiciales para la mayor cantidad de personas.

Sin embargo, la privacidad tiene un problema implícito y es que, sobre todo en Internet, lo que se hace a escondidas generalmente es malo. Para muestra el experimento que hizo Chema Alonso en el que se observa que la mayoría de la gente que utilizó un *proxy* no lo hacía con buenas intenciones[24]. En este caso vemos que la privacidad atenta contra el bien común.

Estos dos términos no son contrarios ya que la privacidad puede contribuir al bien común, ejemplo de esto son las nubes como *MEGA* o *Google Drive* que aportan una gran movilidad, estas nubes están bien cifradas para que nuestros archivos sigan siendo privados. Ahora bien, ¿qué hay que hacer para tener ambas cosas simultáneamente? Pienso que lo ideal sería primero crear un organismo regulador de Internet a nivel mundial que tenga las mismas leyes y normas para todo el mundo y que la privacidad solo pudiese ser eliminada por una causa mayor justificada por la justicia, como es el caso español[1] a diferencia del francés[5]

Internet debe ser un sitio transparente, que cada usuario sepa qué es lo que hace y cuanto se expone, sin necesidad de tener grandes conocimientos informáticos. Hoy en día. cuando te conectas a una web que contenga algo más allá que simple código HTML, puedes estar dando mucha información al servidor que visitas, tus IP, tu navegador, tu sistema operativo, etc. y esta información no tiene por que serte perjudicial pero no tienes la obligación de darla. El bien

20 Ley Orgánica 6/1985
21 Constitución Española
22 USA Patriot Act
23 EL PAIS – *Francia aprueba la ley que permite espiar sin control judicial*
24 Hacking y anonimato: para pasar un buen rato: Chema Alonso at TEDxRetiro Desde el minuto 8

común tiene que ir siempre por encima de todo. Al final, eso es lo que llamamos moralidad, pero no tiene que convertirse en la escusa para obtener información de los ciudadanos. Existen muchas alternativas legales que se pueden aplicar para evitar el terrorismo sin interferir en las personas que no tienen nada que ver con el. Como respuesta a la pregunta diría que es bien común pero no como fin que justifica unos medios intrusivos.

Un ejemplos de alternativa para evitar invadir la privacidad a parte de las ya citadas[1,3] puede ser la ley de protección de datos[25], que protege la información recolectada ya sea por videovigilancia o por cualquier otro medio y además se puede ejercer el derecho a que esta sea eliminada.

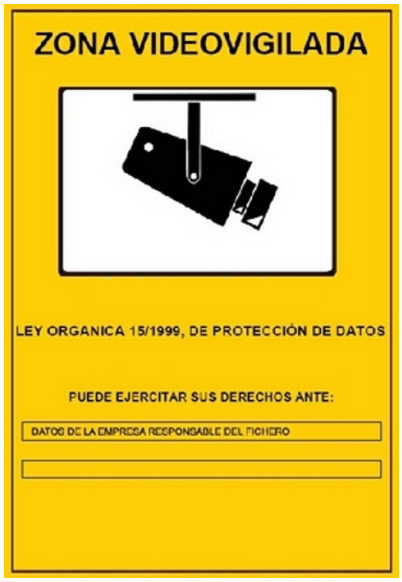

Ilustración 2: Cartel de aviso de videovigilancia

25 Ley Orgánica 5/1999

¿Hasta qué punto debe de llegar la privacidad?

Este quizás es el punto más controvertido ya que trae un debate mayor enfocado mucho a la opinión personal. ¿Qué debe ser privado y que debe ser público? Una respuesta sencilla sería "lo que dicte la ley" pero en este caso es insuficiente ya que existen muchas leyes diferentes en tantos países del mundo que hace imposible utilizar esta respuesta. Además las leyes no avanzan tan rápido como los cambios en la tecnología que se están viviendo.

Existe una teoría, de Jennifer Jacquet expuesta en su libro *Is shame necessary*, en la que defiende que el acto de ser observado provoca que la persona sienta vergüenza de no cumplir con los convenios sociales. Un ejemplo que expuso en el programa de Science Channel (Discovery Communications) *Through the Wormhole* capítulo Nº 41, "Is poverty genetic?", consistía en que un grupo de personas anónimas entre si debían meter un dólar en un fondo común y este se multiplicaría y se repartiría a partes iguales entre los participantes. El resultado fue que cuando eran anónimos varios sujetos no daban dinero al fondo común pero sí obtenían su parte del dinero multiplicado, pero ante la amenaza de desvelar quién sería el que menos ha dado provocó que se hicieran menos trampas. ¿Qué quiero exponer con esto? Que en el caso de que tu actividad sea pública, el miedo a la vergüenza provoca que te cuides de hacer "trampas".

Esta teoría se puede enlazar con otra con un nombre similar creada por John Braithwaite llamada "Teoría de la vergüenza reintegrativa"[26] que consiste en utilizar la vergüenza para redimir y no para estigmatizar al "avergonzado".

Bajo estas dos premisas mi opinión es que la privacidad no debe proteger a las personas que han desobedecido el código moral, pero tampoco debe degradar a las personas "públicas" por "desobediencia" si no buscar una reparación del daño creado. Ejemplo de esto es la publicación de la lista de deudores por parte del ministro de hacienda español Cristóbal Montoro[27], una lista que es pública, que tiene como objetivo acabar con el fraude creando tanto vergüenza para los defraudadores y que tengan que pagar lo debido,evitar reincidencias por parte de los imputados y persuadir de cometer el mismo delito a otras personas.

Esto en lo referente a las personas, pero hay que ir más allá, hay que ir a una privacidad que tienga como fin no proteger la información, si no ocultar información. Quiero arrancar con los famosos casos de las filtraciones de Snowden, ¿es legitimo que se filtre información confidencial? Al fin y al cabo se trata de información privada de una entidad como la NSA pero una gran mayoría de ciudadanos están de acuerdo en lo que hizo estaba bien pero, ¿por qué? Porque desvelaban información que perjudicaba a los ciudadanos. Es lícito que se descubra información que perjudica a una gran parte de la población, ya que es un deber moral denunciar

26 LA TEORÍA DE LA VERGÜENZA REINTEGRATIVA DE JOHN BRAITHWAITE por Miguel Langon Cuñarro

27 Montoro sacará pecho en periodo electoral con la lista de morosos – El Mundo

la injusticia y que esta sea conocida por la gente. A esto se pueden sumar las filtraciones de Wikileaks que han denunciado casos como las torturas de Guantánamo[28].

Es importante concebir un método que convierta lo lícito en legal porque aunque desvelar la injustícia sea lícito es muchos casos, como hemos podido observar[29], es ilegal.

Sin embargo, queriendo enlazar con el principio de este apartado, estas filtraciones deben ser no para estigmatizar, si no para redimir a los culpables y reparar los daños creados. Esto se ha podido ver en la reciente reforma de la NSA que acota los poderes de la misma y la prensa lo a catalogado como un "triunfo parcial de Snowden"[30]. La reforma según el diario español El País pone en manos de las telefónicas y no de la NSA la información, esto crea un sistema parecido a la ley judicial española mencionada anteriormente que permite que solo la información necesaria se obtenga sin perjudicar a una gran cantidad de personas.

28 Las cinco filtraciones de Wikileaks que más incomodaron a Estados Unidos – La Tercera
29 EEUU acusa a Snowden de espionaje y pide a Hong Kong que lo arreste – 20 Minutos
30 La reforma de la NSA es un triunfo parcial de Snowden – El País

Bibliografía

Miguel Lagon Cuñarro – *Teoría de la vergüenza reintegrativa de John Braithwaite* www.revistafacultadderecho.edu.uy

Jennifer Jacquet (2015) *Is Shame Necessary?: New Uses for an Old Tool* – Pantheon ISBN 978-0-30-790757-8

Discovery Communication - *Is poverty genetic?* (2014) Through the Wormhole Temporada 5 episodio 3 (Capítulo 41)

Diccionario online de la Real Academia Española – dle.rae.es

Términos y condiciones de Facebook

Términos y condiciones de Twitter

Términos y condiciones de Instagram

Portal Microsoft Windows – windows.microsoft.com

Congreso de los EE.UU. - www.congress.gov

Noticias Jurídicas – noticias.juridicas.com

New York Times - www.nytimes.com

20 Minutos – www.20minutos.es

El País – elpais.com

The Guardian - www.theguardian.com

La Tercera – www.latercera.com

ABC – www.abc.es

Torrentfreak - torrentfreak.com

El Mundo - www.elmundo.es

El Confidencial - www.elconfidencial.com

Canal TecnoXplora - www.youtube.com/user/tecnoxplora

Canal TedX Talks - www.youtube.com/channel/UCsT0YIqwnpJCM-mx7-gSA4Q

La Biblia de Jerusalén – Edición “Casa de la Biblia”