

PRÁCTICA 4

“EL GRAN HERMANO, VIGILANDO AL MUNDO” SEGURIDAD, PRIVACIDAD E INTERNET



Fuente: *La voz del sandinismo* <<http://www.lavozdelsandinismo.com/>>

Autores:
Montes Mariano, Daisy
Oca Domínguez, Andrea
Pérez Álvarez, Lucía
Pérez Seijo, Sara
Portela Rodríguez, Pablo

“LA NOCHE TEMÁTICA: TÉRMINOS Y CONDICIONES DE USO”

Resumen:

El video de “Términos y Condiciones de uso” se trata de una pieza audiovisual de una hora y cuarto de duración aproximadamente. El género de tal obra se corresponde con el documental, siendo rodado en lengua inglesa, aunque el video al que nosotros accedimos estaba doblado al castellano. El tema sobre el que trata, al que hace referencia en el título, es la privacidad existente a día de hoy con las nuevas tecnologías.

A lo largo de toda la pieza se suceden una lista de expertos y autores que exponen el problema sobre el que trata la línea argumental: nuestros datos están expuestos a todo el que los quiera. Además, los mismos autores nos enseñan evidencias del control que sufrimos por parte de estados y grandes compañías. Los primeros vigilan nuestras comunicaciones, acceden a todo lo que la red almacena sobre nosotros sin nuestro consentimiento. Espían cada mensaje, cada tuit, cada palabra, con la excusa de que es por nuestro bien. Los segundos, capturan todo lo que pueden y lo utilizan para lucrarse. Compran, venden, intercambian, todo por dinero. Conocen nuestros gustos, y así pueden orientar la publicidad y bombardearnos con *pop-up's*, *spam* y muchos otros medios. Por encima, pese a que en Europa existe una legislación que regula los derechos de privacidad, la incumplen sin consecuencias, siendo Estados Unidos el mayor exponente, ya que manejan al gobierno para evitar leyes que les puedan perjudicar.

Fuentes:

- Aho Williamson, Debra. Analista jefe *eMarketer*. <www.emarketer.com> [Consulta 17 noviembre 2013].
- Aldridge, Pete. Subsecretario de Defensa entre el año 2001 y el 2003. Fue uno de los defensores del programa *Control total de la información*.
- Anderson, Chris. Es considerado una de las personas más influyentes en EEUU. Además de periodista y editor en jefe de la revista *Wired* desde 2001 hasta 2012, Anderson es también escritor, físico y conferenciante. En 2004, publicó un controvertido artículo titulado “The Long Tail”, para criticar el nuevo modelo de negocio en internet.
- Anderson, Harvey. Vicepresidente de desarrollo y asuntos legales de Mozilla. <<http://www.mozilla.org/es-ES/>> [Consulta 17 noviembre 2013].
- ARRINGTON, Michael: “AOL Proudly Releases Massive Amounts of Private Data”. *TechCrunch*, 6 agosto 2006. <<http://techcrunch.com/2006/08/06/aol-proudly-releases-massive-amounts-of-user-search-data/>> [Consulta: 9 noviembre 2013]. El buscador AOL saca a la luz miles de datos privados de sus usuarios.
- Assange, Julian. Fundador y máximo representante de Wikileaks, organización que publica en su página web contenido secreto gubernamental. Ha desvelado información sobre temas polémicos como el comportamiento del ejército estadounidense en la guerra de Irak, entre otros.
- Bambord, James. Periodista y escritor. *The Puzzle Palace: Un informe sobre la agencia más secreta de Estados Unidos*, Houghton Mifflin, 1982. Esta fue su primera obra sobre los servicios de seguridad estadounidenses, a la que siguieron otras con la misma temática.
- BARBARO, Michael y ZELLER, Tom: “A Face Is Exposed for AOL Searcher No. 4417749”. *The New York Times*, 9 agosto 2006. <<http://www.nytimes.com/2006/08/09/technology/09aol.html?pagewanted=all>> [Consulta: 9 noviembre 2013]. Gran facilidad para detectar al usuario concreto que está detrás de las búsquedas en AOL.
- Boyd, Danah. Investigadora superior de Microsoft. Autora del libro aún por salir al mercado, *It's Complicated: The Social Lives of Networked Teens*, Yale University Press.. Además de otros artículos que podemos consultar en su web <<http://www.danah.org/>>. [Consulta 17 noviembre 2013].

- Brown, Barrett. Portavoz extraoficial del grupo de “hacktivistas” Anonymous y fundador del Proyecto PM, que investiga e informa sobre los asuntos relacionados con la industria de la contratación de inteligencia. Niega haber sido su portavoz, pese a lo que decía la prensa. Se mostró crítico con el programa *Control Total de la información*.
- Bryan, Leigh. Ciudadano de Reino Unido que es detenido cuando se disponía a embarcar rumbo a EEUU por un tweet (comentario en Twitter) que fue considerado por el Gobierno estadounidense como un posible atentado.
- Bush, George. Presidente de los Estados Unidos entre el año 2001 y 2009. Autorizó a la Agencia de Seguridad Nacional (NSA) a interceptar comunicaciones internacionales de personas vinculadas con Al Qaeda y otras organizaciones terroristas relacionadas.
- Carrier IQ. Empresa fundada por Konstantin Othmer, que creó un programa capaz de extraer información de dispositivos móviles y, así, transmitirla al FBI.
- Cheng, Christopher. Vicepresidente de Ingeniería en Celebrate USA, empresa que vende herramientas para extraer información de móviles de grandes agencias estadounidenses.
- Control total de la información. Programa puesto en marcha por el Gobierno estadounidense en enero 2002 (fue cancelado). Misión: registrar toda la información digital imaginable.
- Corbett, Ellen. Senadora del Estado de California. Cumple su segundo mandato, fue elegida líder de la mayoría del Senado por sus compañeros demócratas en 2010. Propuso una ley- *SB 242 Corbett* (no se llegó a aprobar) para aumentar la seguridad en la red sobre la información privada y robos de identidad.
- Court, Jamie. Presidente de Consumer Watchdog (una asociación de consumidores). Autor del libro *The Progressive's Guide to Raising Hell: How to Win Grassroots Campaigns, Pass Ballot Box Laws, and Get the Change We Voted For*. Perfil de Jamie Court en la página oficial de Consumer Watchdog.org. <<http://www.consumerwatchdog.org/>> [Consulta: 12 noviembre 2013].
- Cutler, Amy. Mujer que participó en un flashmob el día de la boda de los Príncipes de Cambridge, manifestándose en contra de la Boda Real.
- DAILY MAIL REPORTER: “ Now TomTom apologises for selling customer satnav data... which police used to set up speed traps”, *Daily Mail*, 28 abril 2001. <<http://www.dailymail.co.uk/sciencetech/article-1381491/TomTom-apologise-selling-customer-satnav-data-used-police-speed-traps.html>> [Consulta: 9 noviembre 2013]. La empresa de navegadores TomTom enviaba a la policía los datos relativos a la posición geográfica de los usuarios.
- Davidson, Alan. Exdirector de Políticas Públicas de Google para América del Norte y del Sur. Ha escrito y hablado extensamente sobre cuestiones de política de Internet, incluyendo la privacidad, la libertad de expresión, el cifrado, la neutralidad de la red y los derechos de autor en línea. Antes de unirse a Google, Alan fue director asociado del Centro para la Democracia y la Tecnología, un grupo de interés público que promueve las libertades civiles en internet.
- Drake, Thomas. Ex-ejecutivo de la Agencia de Seguridad Nacional. En 2011 fue condenado a un año de libertad condicional por filtrar documentos al *The Baltimore Sun*, en los que se hablaba de los métodos de espionaje de la agencia.
- Ellsberg, Daniel. Denunciante de prácticas ilegales. Filtró a los medios *Los papeles del Pentágono*, un documento sobre la participación de Estados Unidos en la guerra de Vietnam.
- Glanz, William. Especialista en tecnología del *Washington Times*.
- Grant, Hugh. El actor fue víctima de las escuchas ilegales del periódico *News of the World*, que tuvo que pagarle una indemnización. También donó una cantidad de dinero a la organización “Hacked off”, que lucha por la regulación de la prensa en esta materia.
- Heidt, Frank. Director ejecutivo de la empresa Leviathan Security Group. Es experto en seguridad en la red e incluso trabajó para el Departamento de Defensa norteamericano. La compañía de seguridad elabora y desarrolla aplicaciones para garantizar la seguridad de los usuarios de la web.

- Hoback, Cullen.. Director y productor del programa *Terms and Conditions may apply* que hemos visionado.
- Johnson, Hank. Congresista de EEUU por el Partido Demócrata y miembro del Comité Judicial de la Cámara de Representantes que investiga sobre el espionaje a los periodistas de AP.
- Kapow: <<http://www.kapowsoftware.com/>> [Consultado: 11 noviembre 2013]. Software que canaliza todas las redes sociales y busca palabras clave.
- Kennish, Brian. Exingeniero de Google. Fundador de *disconnect.me*, una web que permite al usuario descubrir y bloquear las páginas webs invisibles que le están siguiendo la pista de sus actividades en la red.
- Kerry, John. Secretario de Estado en la actualidad y senador por el distrito de Massachusetts en el momento del discurso del documental.
- Klein, Mark. Extrabajador de la empresa de telecomunicaciones *AT & T Inc.* Filtró las relaciones de su empresa con la Agencia de Seguridad Nacional estadounidense para controlar las comunicaciones a distancia de los ciudadanos.
- Knight, Chris. Profesor de Antropología (expulsado de la East London University por participar en las protestas contra el G-20) y una de las figuras más destacadas del anarquismo británico. Es miembro de grupos como “Occupy London” o “X Network”.
- Lapinta, Vito. Alumno de la Truman Secondary School, al cual el Servicio Secreto de Tacoma lo interrogó por escribir un post en su blog personal tras ser considerado una amenaza al presidente estadounidense Barack Obama.
- Lawler, Brian. Tipógrafo. Profesor de la Universidad Estatal Politécnica de California (<http://www.calpoly.edu/>). Autor del blog *The Lawlers.com* y de los libros *Official Adobe Print Publishing Guide*, Adobe Press, 2006 y *The Complete Guide to Trapping*, Hayden Books, 1995. [Consulta 17 noviembre 2013].
- Lipari, Joe. Humorista al cual la SWAT (equipo o unidad de élite incorporado en varias fuerzas de seguridad) lo visitó por escribir un comentario en Facebook con una frase de la película “*El Club de la Lucha*”, cambiando el lugar que se mencionaba originalmente por “Apple Store”.
- Los Dowlers (matrimonio). Padres de Milly Dowler, una niña desaparecida en 2002 y que luego fue hallada muerta. El periódico *News of the World* pinchó el teléfono de la familia.
- McCullagh, Declan. Redactor jefe de política de *Cnet News.com*. Además es programador informático, según comenta en su web. <<http://www.mccullagh.org/>> [Consulta 17 noviembre 2013].
- Murdoch, Rupert. Magnate australiano de la comunicación, principal accionista del grupo *News Corporation*. Conocido por el escándalo de su periódico *News of the World*, que tuvo que ser cerrado por sus prácticas ilegales (escuchas telefónicas o sobornos) de obtención de información.
- Obama, Barack. Actual presidente de los Estados Unidos.
- Página web de negocios de EEUU: <www.fedbizopps.gov> [Consultado: 11 noviembre 2013].
- Palfrey, John. Profesor de Derecho en Harvard. Autor de *Born Digital: Understanding the First Generation of Digital Natives*. Basic Books, 2008.
- Pariser, Eli. Autor de *The Filter Bubble: What The Internet Is Hiding From You*. Penguin, 2011 y director ejecutivo de *Upworthy.com*. Explica la idea de su libro en el siguiente enlace: <http://www.ted.com/talks/lang/es/eli_pariser_beware_online_filter_bubbles.html> [Consulta 17 noviembre 2013].
- Reitman, Rainey. Directora de la fundación Fronteras Electrónicas <<https://www.eff.org>>, además de cofundadora de *Freedom of the Press Foundation* <<https://pressfreedomfoundation.org/>> [Consulta 17 noviembre 2013].
- Robertson, Timi. Madre de Vito Lapinta.
- Rockefeller, Jay. Representante del Estado de Virginia en el Senado estadounidense. Se ha pronunciado en numerosas ocasiones en contra de Facebook debido a la cantidad de niños que lo usan, estando expuestos a contenidos que no considera adecuados.

- Rushkoff, Doug. Escritor, columnista en *New York Times* y experto en cibercultura.
- Ryan Calo. Exdirector de Privacidad y Robótica en el Stanford Center de Internet y Sociedad, donde sigue afiliado. Co-preside el Comité de la Asociación Americana de Abogados de Robótica e Inteligencia Artificial. Su trabajo ha aparecido en diferentes medios como *The New York Times*, *San Francisco Chronicle*, *Business Week*, *The Associated Press*, *el Wall Street Journal*.
- Sartinsky, Christopher. Subdirector de la Agencia Central de Inteligencia (CIA). Vivió la monitorización secreta de muchos usuarios para comprobar la cantidad de datos personales que se comparten en la red.
- Schaar, Peter. Comisario alemán de protección de datos. Apoya la propuesta de la Eurocámara de no transferir datos bancarios a EE UU en el marco de la lucha antiterrorista hasta que se aclare el escándalo de espionaje.
- Schmidt, Eric. Según la propia página de google, es presidente ejecutivo de esta compañía, además de asesor del presidente de Estados Unidos, Barack Obama y del primer ministro de Reino Unido.
<<http://www.google.es/intl/es/about/company/facts/management/>>. [Consulta 17 noviembre 2013].
- Schrems, Max. Estudiante de Derecho austriaco. Promovió la campaña “Europa contra Facebook” para aclarar posibles infracciones con respecto a la privacidad.
- Scott, Orson. Escritor de ciencia ficción. Autor del libro *El juego de Ender*, del que se ha estrenado la adaptación cinematográfica el 8 de noviembre del presente año.
- Shearer, Michael. Experto en seguridad digital (criptografía, privacidad, seguridad inalámbrica...). Ha contribuido en varias obras sobre seguridad informática, la más reciente: *Defensa Contra las Artes Negras: cómo los hackers hacen lo que hacen y cómo protegerse*, CRC Press, 2011.
- SINGEL, Ryan: “Twitter’s Response to WikiLeaks Subpoena Should Be the Industry Standard”, *Wired.com*, 1 octubre 2011 . <<http://www.wired.com/threatlevel/2011/01/twitter/>> [Consultado: 11 noviembre 2013].
- Soghoian, Chris. Investigador de la privacidad en internet y activista en favor de estos derechos. Autor de artículos como “The spies we trusts”; “You can see me now”; “Certified lies” y otros tantos que podemos consultar en su web <<http://www.dubfire.net>>.
- Spielberg, Steven: *Minority Report*. Amblin Entertainment, 2002. Película que trata sobre arrestos por “precrímenes”, crímenes que no han sido cometidos aún pero que iban a suceder en el futuro. Muy relacionado con el argumento que el Gobierno de EEUU usa para justificar su “espionaje”.
- Stuart, Alan. "Al" Franken, político, escritor y humorista estadounidense. Desde 2009 es senador junior del estado de Minnesota.
- Swan Mueller III, Robert. Actual director de la Oficina Federal de Investigación (FBI) de los EEUU. Se alistó en el cuerpo de Marines de su país y también participó, a principios de los 70, en la Guerra de Vietnam.
- The Wall Street Journal: “The Surveillance Catalog. Where governments get their tools”, *Projects.wsj.com*, 7 febrero 2012. <<http://projects.wsj.com/surveillance-catalog/#/>> [Consultado: 11 noviembre 2013].
- Tice, Russel. Exanalista de la NSA que ha confirmado el acceso de la Agencia a las comunicaciones de los americanos. Dio información a *The New York Times* sobre escuchas telefónicas.
- Timoner, Ondi. Directora del documental *We live in public*, que trata sobre la pérdida de privacidad en esta nueva era de internet.
- Tufekci, Zeynep. Profesora de Sociología de la Universidad de Baltimore. escribe en su sitio personal <<http://technosociology.org/>> [Consulta 17 noviembre 2013].
- Turkle, Sherry. Profesora estudios sociales de ciencia y tecnología del Massachusetts Institute of Technology (MIT). Es una psicóloga y socióloga experta en las relaciones hombre-ordenador. Autora, de entre otros, de *Alone Together*. Basic Books, 2011.

- Vaidhyathan, Siva. Autor de *La googlización de todo*, Océano, 2010, Profesor de Derecho y estudios Mediáticos de la Universidad de Virginia.
- Valentino-DeVries, Jennifer. Asistente de editores del medio The Wall Street Journal. Desde 2010 ha sido miembro del equipo de *What they know*, una serie del medio de larga duración sobre la privacidad digital, que además fue finalista para el premio Pulitzer en Periodismo Explicativo en 2012.
- Wayback Machine: <<http://archive.org/web/>>. Página web dedicada al archivo de diferentes contenidos de sitios web. [Consulta 17 noviembre 2013].
- Zuckerberg, Mark. Creador de la red social Facebook, nacida en 2007.

“INFORME SEMANAL: EL ESPIONAJE GLOBAL”

Resumen:

“El espionaje global” es un reportaje de Informe Semanal que se centra en la inseguridad y la vulneración de la privacidad dentro del entorno online. Pese a que el tema no es ninguna novedad, ha saltado de nuevo a la palestra mediática gracias a las revelaciones de Edward Snowden, un antiguo consultor tecnológico de la Agencia de Seguridad Nacional (NSA), según las cuales la administración norteamericana ha interceptado millones de comunicaciones no sólo de ciudadanos sino también de líderes mundiales como la canciller alemana Angela Merkel o el presidente francés François Hollande. El gobierno de los Estados Unidos, a través de grandes empresas de capital norteamericano como Facebook, Google, Microsoft, Youtube o Apple, accedería a metadatos que los propios usuarios cedemos a las compañías. Tamaña transgresión de la intimidad tiene sus orígenes en la *Patriot Act*, en vigor, bajo pretexto de la lucha contra el terrorismo, tras los atentados a las Torres Gemelas en el año 2001.

Fuentes:

- Brehmer, Ulrich. Miembro de la presidencia de la Asociación Alemana para la Seguridad en la Economía. Afirma que una de las funciones de los servicios secretos de Rusia y China es el espionaje industrial.
- De Juan Espinosa, Manuel. Director del Instituto de Ciencias Forenses y Seguridad de la UAM. Asegura que el presupuesto dedicado por Alemania a ciberseguridad asciende, aproximadamente, a los 80.000 millones de euros. En España dicho presupuesto puede oscilar entre los 10.000 millones y los 40.000 millones de euros.
- García Sánchez, Fernando. Jefe del Estado Mayor de Defensa del Estado español. Considera a los Estados Unidos como un aliado importante pese a los documentos revelados por Snowden.
- Gómez Bule, Juan Antonio. Presidente del consejo asesor de “S21 sec”. También es consejero del Instituto Choiseul, dedicado a la investigación de las principales cuestiones de política internacional tal y como indica su ficha de linkedin: <<http://www.linkedin.com/profile/view?id=104569141>> [Consulta: 15 noviembre 2013].
- Gurpegui, José Antonio. Catedrático de Filología Inglesa y director del Instituto Franklin de Estudios Norteamericanos de la Universidad de Alcalá (UAH), ha publicado numerosas obras de carácter divulgativo y científico sobre la literatura y aspectos sociales de los Estados Unidos, algunas de las cuales podemos consultar en <<http://dialnet.unirioja.es/servlet/autor?codigo=545175#Libros>> [Consulta: 15 noviembre 2013].
- Hollande, François. Actual presidente de la República Francesa. Uno de los primeros líderes políticos en quejarse por las escuchas de la NSA.
- Martínez, Lorenzo. Director de tecnología y fundador de la Consultoría y Auditoría en seguridad informática “Securizame”. Titulado en Ingeniería Superior en Informática por la Universidad de Deusto (Vizcaya) cuenta con

formación específica en el ámbito de la seguridad cibernética tal y como se especifica en su página personal < <http://www.lorenzomartinez.es/>> [Consulta: 15 noviembre 2013].

- Merkel, Angela. Actual canciller de la República Federal Alemana. Considera que el gobierno de los Estados Unidos ha violado la soberanía alemana.
- Obama, Barack. Actual presidente de los Estados Unidos. Afirma la necesidad de perder privacidad para garantizar la seguridad.
- Patriot Act. Ley aprobada en los Estados Unidos durante el mandato de George W. Bush. La *patriot act* permite el control de las comunicaciones de los ciudadanos con el fin de proteger la seguridad nacional de posibles terroristas. Fue aprobada tras los atentados a las Torres Gemelas en el año 2001.
- Rajoy, Mariano. Actual presidente de España. Afirma que se toma muy en serio las escuchas de la NSA en territorio español.
- Rueda, Fernando. Doctor en Periodismo por la Universidad Complutense de Madrid, imparte docencia en la Universidad San Pablo Ceu, y ha trabajado en numerosos medios de comunicación como *Onda Cero* o *Interviú*. Ha escrito ampliamente sobre el espionaje en obras como *Por qué nos da miedo el Cesid* o *Servicios de Inteligencia: ¿fuera de la ley?*, convirtiéndose en un experto consagrado sobre el tema en nuestro país tal. Sus obras se pueden consultar en < <http://www.esferalibros.com/autor/fernando-rueda/>> [Consulta: 15 noviembre 2013].
- Sanz, Félix. Director del Centro Nacional de Información (CNI) desde el año 2009, ocupó con anterioridad el cargo de Jefe de Estado Mayor de la Defensa. El director del CNI ha asegurado que la colaboración con el gobierno de los Estados Unidos en cuanto al intercambio de información, se ha limitado a fuera de las fronteras del Estado español.
- Teijeira, Pablo. Director general de “Sophos”, empresa que provee servicios de seguridad informática. < <http://pabloteijeira.wordpress.com/>> [Consulta: 15 noviembre 2013].

Informe:

Introducción:

“Estados Unidos espía al mundo”, “Cuestionada la privacidad de los estadounidenses”, “Dirigentes políticos bajo la lupa de Estados Unidos” y muchos otros titulares similares son los que podrían comenzar este informe. Las noticias recientes sobre las prácticas de organismos estadounidenses como la Agencia de Seguridad Nacional o el Centro de Inteligencia Nacional hacen que el país sea protagonista de miles de noticias alrededor del mundo. Gracias a la visión de los documentales “La noche temática: Términos y condiciones de uso” e “Informe Semanal: El espionaje global” hemos podido conocer datos objetivos en los que se basan aquellos que acusan al gobierno de EEUU. Pese a manejar un gran número de fuentes y de explicaciones al problema del espionaje, hemos querido profundizar en el tema haciendo una indagación propia. Veremos así el papel que tienen las compañías que operan en la red para ser acusadas de fraude, así como las actividades de aquellos que ostentan el poder. Seguridad, libertad, privacidad y legalidad son las claves de esta búsqueda. ¿Actúan los políticos protegiendo la seguridad estatal? ¿En qué rincón queda la libertad individual? ¿Sigue salvaguardada la privacidad? ¿Se acerca o se aleja el asunto del límite de lo legal? Nuestro objetivo es que en las siguientes palabras todo esto quede más claro en la mente del lector, basándonos en hechos, no en opiniones personales.

Espionaje de las compañías:

Facebook, la red social creada por Mark Zuckerberg, dice en su política de uso de datos: “Podemos utilizar la información que tenemos sobre ti para: los anuncios que tú y otros usuarios veis; operaciones internas, incluidas la investigación; para proteger los derechos o la propiedad de Facebook” (Facebook, 2013). “También podemos acceder, conservar y compartir información cuando creamos de buena fe que es necesario para: detectar, prevenir y abordar actividades fraudulentas o ilegales; protegernos a nosotros mismos, a ti y a otros, incluso como parte de investigaciones, y para evitar muertes o daños físicos inminentes” (Facebook, 2013). Por su parte, Google, el gigante virtual, dice: “Compartiremos tus datos personales con empresas, organizaciones o personas físicas ajenas a Google si consideramos de buena fe que existe una necesidad razonable de acceder a dichos datos o utilizarlos, conservarlos o revelarlos para: cumplir o atender cualquier requerimiento de un órgano administrativo o judicial; proteger los derechos, los bienes o la seguridad de Google; detectar o impedir cualquier fraude o incidencia técnica o de seguridad” (Google, 2013).

Como vemos en estos dos gigantes de la era digital, entre los que se reparten los datos confidenciales de medio planeta, las compañías virtuales de hoy en día se reservan el derecho de compartir nuestros datos a terceros, muchas veces sin nuestro consentimiento. Por exigencias de las autoridades, sin que haga falta poseer una orden judicial, le pueden ceder nuestros datos “por buena fe”. Además, están libres de difundir nuestros datos con fines publicitarios, con la simple razón de enriquecerse. De que las compañías nos puedan ofrecer los productos que más se ajusten a nuestras búsquedas. De que nos conozcan como ni nosotros mismos nos conocemos, ya que “compartiremos tus datos personales con empresas, organizaciones o personas físicas ajenas a Google. Tu consentimiento será necesario para compartir datos personales especialmente protegidos” (Google, 2013). Siendo esta información la relacionada con: “raza u origen étnico, creencias religiosas, ideología política o sexualidad” (Google, 2013), sin que se mencione el nombre o dirección, como un dato confidencial especialmente protegido. Además, en ninguna de las políticas de privacidad de las mencionadas empresas proveedoras de servicios *online*, hace alusión alguna del uso que los terceros hacen de la información facilitada. Este hecho, puede derivar a que los terceros, que de una manera han conseguido la información relativa a nuestros gustos y costumbres; sobre nuestros amigos y familia; sobre nuestro trabajo; y sobre muchas otras cosas, con fines comerciales como puede ser la publicidad, se puedan convertir en empresas proveedoras de datos personales. Por otro lado, esas mismas políticas que recogen información por doquier, nos permiten recibir un tipo de publicidad adaptada a nuestros gustos, a nuestras preferencias reales, y no a lo que manifestamos en un cuestionario. Observa dónde hacemos clic, qué nos interesa, qué llama nuestra atención, y nos lo trae.

Por otra parte, en el gigante Google, el peligro es más grande, ya que en ocasiones puede ser peligroso que ellos mismos recojan información. Tal y como nos cuenta Eli Pariser en un video, en el que explica su libro *The Filter Bubble*, Google adapta los resultados de sus búsquedas en función del perfil que tenga de nosotros. Así, cuando realicemos una búsqueda, eliminará ciertos resultados considerándolos fuera de nuestro interés, lo que deriva en una gran desinformación, ya que sólo nos acabará mostrando lo que deseamos ver. Evitará, en cierta medida, el contraste de información, que nos creemos una conciencia crítica. A día de hoy, Google es el motor de Internet, es la herramienta más utilizada, porque si Google nos oculta algo, es muy probable que no lo lleguemos a ver. Por otra parte, el lado bueno, es que facilita nuestras búsquedas. Sabe que cuando ponemos “blog”, lo mismo buscamos nuestro blog, o ese que consultamos habitualmente, por lo que nos lo enseñará de primero. Nos ordena los resultados, evitando que cuando ponemos USC, nos lleve a la Universidad de South California.

Espionaje gubernamental

Los gobiernos, y en estos documentales, concretamente el de EEUU, se aprovechan de las herramientas facilitadas por estas compañías de las que hablábamos en el apartado anterior. El gobierno norteamericano se ve envuelto en un caso de espionaje sin precedentes, que puede desembocar en graves problemas diplomáticos. La polémica reside, al igual que en el caso de Wikileaks, en el debate entre la privacidad y la seguridad de los ciudadanos. Las revelaciones del ex-técnico de la CIA, Edward Snowden, o las filtraciones de las guerras de Irak, Afganistán y Vietnam, han encendido todas las alarmas.

Echamos la vista atrás y hacemos un breve repaso cronológico en este escándalo:

Octubre 2001: George Bush promulga la “Ley Patriótica” tras los atentados del 11-S, con el fin de proteger la seguridad nacional de posibles terroristas a cambio del control de las comunicaciones de los ciudadanos.

Diciembre 2005: G. Bush reconoce haber autorizado a la NSA pinchar teléfonos de personas vinculadas a terroristas.

2007: “Ley Protect America”, en la que se desarrolla el PRISM, el programa por el que se puede interceptar comunicaciones a extranjeros sin necesidad de orden judicial.

Mayo 2011: el presidente Obama promulga una extensión de la “Ley Patriótica”, hasta junio de 2015.

Mayo de 2013: La agencia *Associated Press* denuncia en una carta al Departamento de Justicia que el gobierno espió a varios de sus periodistas.

6 de junio 2013: Gracias a Edward Snowden, el diario *The Guardian* divulga que la NSA tenía una orden judicial secreta para acceder a registros telefónicos y en Internet de millones de usuarios de la compañía telefónica Verizon.

7 de junio 2013: Snowden filtra a *The Guardian* y *The Washington Post* dos programas de espionaje secretos: uno que registra los datos de llamadas telefónicas de Verizon y otro (PRISM) que permite acceder a servidores de compañías como Microsoft, Google, Facebook, Skype, YouTube o Apple para recabar datos.

Octubre 2013: Snowden filtra otro documento según el que la NSA habría espiado conversaciones telefónicas de 35 líderes mundiales y embajadas.

Pero, ¿qué procedimiento utiliza el gobierno estadounidense para invadir nuestra privacidad?

Según *The Washington Post* y *The Guardian*, el gobierno se atiene a una orden judicial (FISA) por la que podrían pinchar los números de teléfono de la compañía Verizon e intercambiar los datos y duración de las llamadas, aunque no su contenido. Este proceso se encuentra dentro del programa secreto de vigilancia PRISM, por el que también se podrían utilizar los datos procedentes de las principales empresas de Internet. Estas empresas lo niegan, al igual que el gobierno. Tras la publicación de las filtraciones, el director de la agencia de Inteligencia estadounidense, James Clapper, negó que el sistema PRISM espíase a ciudadanos americanos, pero no se pronuncia sobre los extranjeros. Esta afirmación, sin embargo, supone ya el reconocimiento de la existencia de dicho programa secreto.

Debemos insistir en que este procedimiento no es ilegal. El gobierno se ha hecho con autorizaciones judiciales y parlamentarias para actuar de acuerdo con estas prácticas. A pesar de las múltiples denuncias ciudadanas, el presidente Barack Obama alega, al igual que su antecesor, que es la única vía para prevenir posibles ataques terroristas y garantizar la seguridad nacional. Sin embargo, esta postura no sólo es apoyada por dirigentes y exdirigentes, empresarios americanos también la apoyan. El jefe de Oracle (una de las mayores compañías de software del mundo), Larry Ellison, ha declarado en más de una ocasión que apoya el programa de espionaje, ya que serviría para minimizar ataques como el de Boston.

Ante las filtraciones del programa PRISM, los dirigentes europeos, se reunieron indignados en Bruselas para pedir explicaciones, al entender que eso significaba una traición entre países amigos. No lo considera así el primer ministro británico, James Cameron, que cree fundamentales las labores de los servicios secretos y se posicionó en contra de los medios de comunicación que filtraron la información.

En Europa sí contamos con una Ley de Protección de Datos (cuya modificación tiene fecha límite de aprobación en mayo de 2014), que refuerza la privacidad de los usuarios europeos ante las empresas y las autoridades. Esta ley es vinculante, por lo que el gobierno español también debe atenerse a ella. Es más, según una infografía del portal web *Venturebeat*, España es uno de los cinco países que respetan más la privacidad de sus ciudadanos en Internet, ya que el gobierno protege la libertad de expresión, tiene leyes sobre privacidad y sanciona a los que las violen.

En principio, parece que los usuarios europeos gozamos de privacidad en la red, pero las empresas estadounidenses se rigen por la leyes estadounidenses. Y, si es así, ¿quién nos garantiza que estamos seguros? ¿Podemos prevenir posibles ataques a nuestra intimidad?

Posibles soluciones:

Los documentos revelados por Snowden han puesto en el foco público un problema de enorme calado tanto por su trascendencia económica como por la transgresión de derechos políticos que comporta: la desprotección de datos en la red. **¿Cuáles son las posibles soluciones? ¿Cómo prevenir o contrarrestar los ataques cibernéticos?**

-El primer paso es la concienciación de la necesidad de protegerse, lo cual derivaría en un incremento de la demanda y el uso de programas y sistemas de seguridad en el entorno online. Además de sistemas antivirus, el usuario puede utilizar proveedores de email que cifran las comunicaciones como Kolab o Rise-up. También puede usar buscadores como DuckDuckgo o Ixquick cuyas políticas de uso garantizan la privacidad del cibernauta.

- La comunidad tecnológica debe dar respuesta a este gran reto, lo que implica una mayor inversión en I+D destinados al propósito de mejorar y actualizar los sistemas de seguridad.
- La nacionalización de los activos digitales es otra de las soluciones barajadas. Gobiernos como el de Brasil ya han optado por desarrollar e implantar sus propias redes y servicios de software en la administración pública.
- Es deseable una mayor colaboración entre los servicios secretos europeos frente a la injerencia estadounidense.
- La ruptura de los organismos rectores de Internet (ICANN) con el gobierno estadounidense en aras de una auténtica red neutral.

Conclusión sobre el tratamiento de la información:

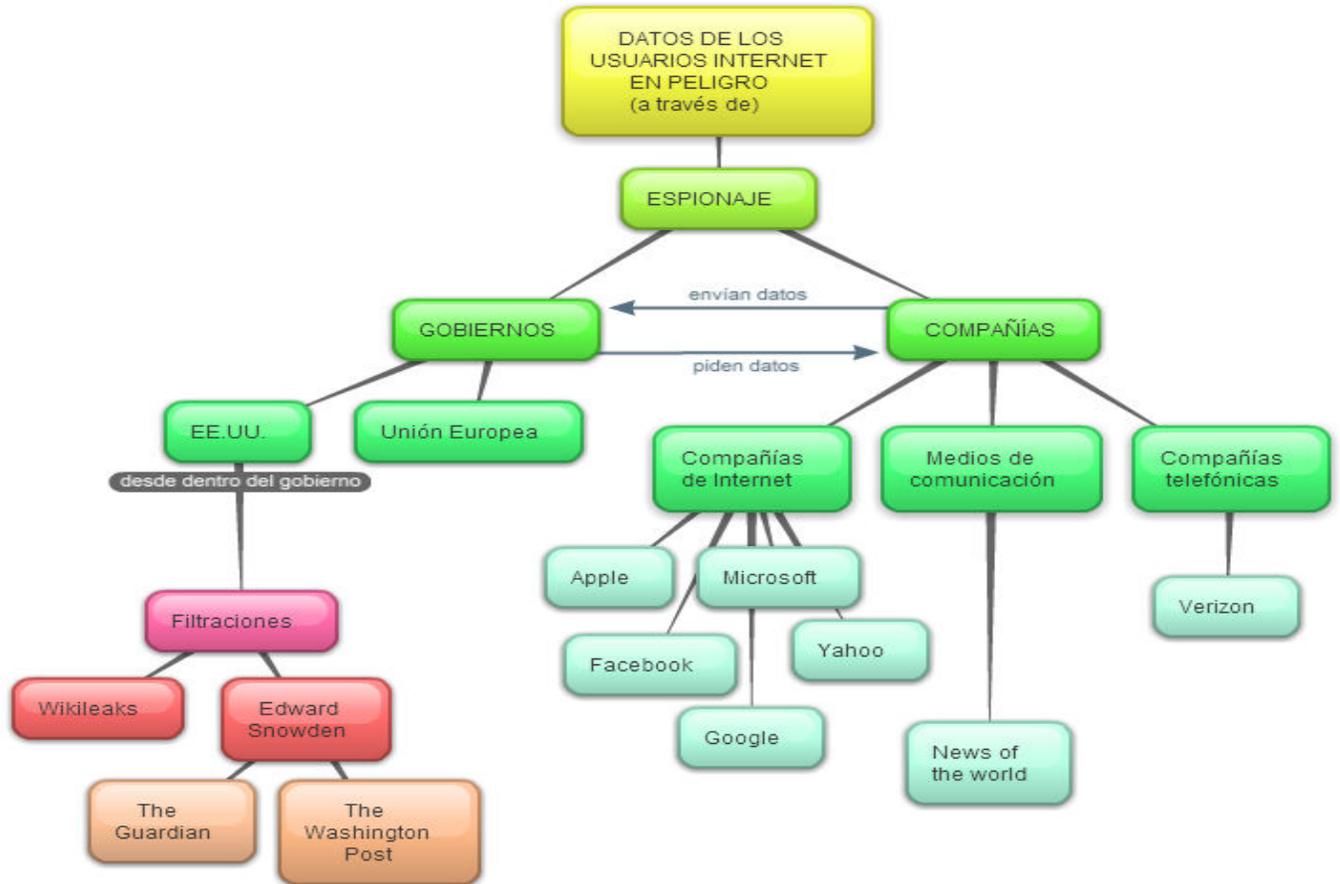
Nos espían y no, no podemos evitarlo. Esa es la perfecta conclusión a la que todos, tras haber visionado “La noche temática: Términos y condiciones de uso” e “Informe Semanal: El espionaje global”, o mismo otros documentales de temática similar, podemos llegar. Nos espían, a la vez que cuatro políticos al mismo tiempo dan una rueda de prensa explicando como la privacidad en Internet es muy importante y, además, existen y tienen mecanismos excelentísimos para evitar la vulneración de la privacidad individual. Mientras hurgan en nuestra intimidad, nos dicen con el orgullo y la mentira en boca, que no existe el espionaje. Toda esta situación se acentuó con el escándalo de Edward Snowden, exanalista de la CIA, tras sus revelaciones de que el Gobierno estadounidense accedía a la información de los ciudadanos a través de Internet. La población mundial se llevó las manos a la cabeza: ¿Pueden espiarnos? ¿Pueden leer nuestras conversaciones en Facebook? ¿Pueden saber a qué páginas webs accedemos? Esas son las preguntas que todos se hacían tras conocer la noticia. Snowden confesó que, en efecto, la Agencia de Seguridad Nacional de Estados Unidos emplea una herramienta llamada XKeyscore para recopilar información personal de los usuarios de Internet. Pero no solo en EEUU, sino en todo el mundo.

¿Entonces...

- **... actúan los políticos protegiendo la seguridad estatal?** En EEUU absolutamente no. En Europa, quizás, o al menos hasta que se revele lo contrario. EEUU hace trampa. El Gobierno norteamericano cuenta con el programa secreto de vigilancia conocido como PRISM -aunque se intente negar, aún a día de hoy, su existencia- por el que puede pinchar números de teléfono o utilizar datos procedentes de las principales empresas de Internet, pero para evitar conflictos legales cuenta con una serie de autorizaciones judiciales y parlamentarias que los eximen de intromisiones ilícitas en la privacidad. Se preguntarán, ¿y el fin de este “espionaje”? Ellos, los de arriba, los del Gobierno de EEUU, afirman que lo hacen para evitar ataques terroristas. Mientras, los ciudadanos, los de abajo, quedan vulnerados y desprevenidos. Pero, por mucho que cueste creerlo, Europa parece ser la menos polémica en estos asuntos, al contar con la ley de Protección de Datos, que refuerza la privacidad de los usuarios europeos ante las empresas y las autoridades. O, al menos, eso dicen ellos.
- **... en qué rincón queda la libertad individual? ¿Sigue salvaguardada la privacidad?** Ambas, libertad individual y privacidad, están en peligro. La herramienta de la que antes hablábamos, XKeyscore, permite recopilar datos de cualquier usuario en la red. Pero, ¿qué datos? Os preguntaréis. Todo lo que os podáis imaginar: correos electrónicos, actividad en las redes sociales, vuestro historial web... Así, los analistas de inteligencia, pueden rastrear por nombres, dirección IP, palabras clave... Es decir, por todos los criterios imaginables.
- **... se acerca o se aleja el asunto del límite de lo legal?** EEUU se ampara en proceso judiciales y parlamentarios pactados para evitar acusaciones de intromisiones ilegítimas en la privacidad individual. Una trampa que, hasta el momento, le funcionaba. Ahora, con las revelaciones de Snowden, el asunto está sobre la mesa, la pregunta es, ¿qué pasará ahora? ¿Qué nuevo mecanismo idearán para seguir espiándonos sin saltarse la “ley” vigente?

Mapa conceptual:

VIGILADOS: PERSON OF INTEREST?



Bibliografía empleada para ampliar la información:

- ALANDETE, David. "Obama declara una guerra implacable a las filtraciones". *Elpais.com*, 1 agosto 2011. <http://elpais.com/diario/2011/08/01/internacional/1312149603_850215.html> [Consulta: 12 noviembre 2013].
- Agencia EFE. "Berlín advierte a EE UU que expulsará a sus diplomáticos si se confirma que espionaron". *20minutos.es*, 29 agosto 2013. <<http://www.20minutos.es/noticia/1962029/0/berlin-advierte-eeuu/expulsion-diplomaticos/espionaje/>> [Consulta: 12 noviembre 2013].
- Agencia EFE. "Brasil usará sistemas de seguridad propios en internet a partir de marzo". *El diario.es*, 5 noviembre 2013. <http://www.eldiario.es/politica/Brasil-sistemas-comunicacion-propios-internet_0_193531193.html> [Consulta: 17 noviembre 2013].
La implementación de tecnología digital nacional en Brasil.

- Centro Nacional de Información. “Secretario de Estado Director (SED): biografía” <http://www.cni.es/es/bienvenida/biografia/> [Consulta: 15 noviembre 2013].
Datos biográficos de Félix Sanz.
- CERVERA, José. “Después de Snowden: un esbozo de cómo quedará el mundo”. *El diario.es*, 6 noviembre 2013. http://www.eldiario.es/turing/vigilancia-y-privacidad/Despues-Snowden-esbozo-queda-mundo_0_193881500.html [Consulta: 17 noviembre 2013].
Consecuencias del caso Snowden en el ámbito empresarial y político.
- DONCEL, Luis. “Cameron se desmarca de sus socios y enarbola su apoyo a Washington”. *El país.com*, 25 octubre 2013. http://internacional.elpais.com/internacional/2013/10/25/actualidad/1382710688_180951.html [Consulta: 12 noviembre 2013].
- El Mundo. “Las claves del escándalo de las escuchas ilegales del 'News of the world'”. *El mundo.es*, 19 julio 2011 <http://www.elmundo.es/elmundo/2011/07/07/comunicacion/1310060131.html> [Consulta: 12 noviembre 2013].
- EP. “Los líderes europeos, unánimes en su indignación por el espionaje de EEUU”. *Europapress.es*, 24 octubre 2013. <http://www.europapress.es/nacional/noticia-lideres-europeos-unanimes-indignacion-espionaje-eeuu-20131024181529.html> [Consulta: 12 noviembre 2013].
- FRESNEDA, Carlos. “Hugh Grant: 'Hay que plantar cara a los matones de la prensa sensacionalista'”. *El mundo.es*, 21 noviembre 2011. <http://www.elmundo.es/elmundo/2011/11/21/comunicacion/1321892103.html> [Consulta: 12 noviembre 2013].
- GONZÁLEZ, Miguel “El jefe del CNI garantiza “al 99,9%” que Rajoy no fue espiado por EE UU” , *El País*, 7 noviembre 2013. http://politica.elpais.com/politica/2013/11/06/actualidad/1383770213_863823.html [Consulta: 15 noviembre 2013].
Félix Sanz asegura en el Congreso que no ha entregado información de ciudadanos españoles a la administración norteamericana.
- Hatrack river, the official web of Orson Scott Card. <http://www.hatrack.com/> [Consulta: 12 noviembre 2013].
- HOBACK, Cullen. “Our data is our digital identity - and we need to reclaim control”. *Theguardian.com*, 19 septiembre 2013. <http://www.theguardian.com/technology/2013/sep/19/data-digital-identity-cullen-hoback> [Consulta: 12 noviembre 2013].
- Johnson, Hank. “Declaración del Congresista Hank Johnson sobre la divulgación del programa de vigilancia telefónica NSA”. *Hankjohnson.house.gov*, 14 junio 2013. <http://hankjohnson.house.gov/declaraci%C3%B3n-del-congresista-hank-johnson-sobre-la-divulgaci%C3%B3n-del-programa-de-vigilancia-telef%C3%B3nica> [Consulta: 12 noviembre 2013].
- KELLY, Meghan. “These 5 countries were ranked best for privacy (infographic)”. *VentureBeat*, 13 octubre 2013. <http://venturebeat.com/2013/10/13/countries-privacy/> [Consulta: 12 noviembre 2013].
Infografía que explica por qué esos son los cinco países con más seguridad en Internet.
- LÓPEZ AGUILAR, Juan Fernando. “Por fin una ley europea de protección de datos (I)”. *HuffingtonPost.es*, 24 octubre 2013. http://www.huffingtonpost.es/juan-fernando-lopez-aguilar/ley-europea-de-proteccion-de-datos_b_4148971.html [Consulta: 12 noviembre 2013].
Explicación de la Ley Protección de Datos europea.
- MÁIQUEZ, Miguel. “Vidas no tan privadas: las claves del espionaje del Gobierno de Obama a los ciudadanos”.

20minutos.com, 16 junio 2013. <<http://www.20minutos.es/noticia/1843571/0/espionaje/eeuu/privacidad/>> [Consulta: 12 noviembre 2013].

Claves del caso de espionaje de EE.UU.

- PARISER, Eli: “Eli Pariser: cuidado con la "burbuja de filtros" en la red”, *Ted.com*, 2011. <http://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles.html> [Consulta 17 noviembre 2013]. Eli nos explica en persona cómo Google orienta nuestras búsquedas en función de nuestras preferencias.
- Perfiles del equipo de Leviathan Security Group. <<https://www.leviathansecurity.com/team/>> [Consulta: 12 noviembre 2013].
- Piovesana, Enrico. “La revuelta de Londres según el antropólogo británico Chris Knight”. *Rebelión.org*, 2011. <<http://www.rebelion.org/noticia.php?id=133897>> [Consulta: 12 noviembre 2013].
- Políticas de Uso de Datos: “Información que recibimos sobre ti”, Facebook, 2013. <<https://www.facebook.com/about/privacy/your-info#public-info>> [Consulta 17 noviembre 2013]. El uso que da Facebook a nuestros datos.
- Políticas de Uso de Datos: “Otras cosas que debes saber”, Facebook, 2013. <<https://www.facebook.com/about/privacy/other>> [Consulta 17 noviembre 2013]. Algunos usos no especificados en el resto de puntos de las políticas de privacidad de Facebook.
- Políticas y Principios: “Política de Privacidad”, Google, 2013. <<https://www.google.es/intl/es/policies/privacy/>> [Consulta 17 noviembre 2013]. Uso que da el buscador a los datos que posee sobre nosotros.
- RIESTRA, Laura. “¿Cómo espía EE.UU.?: guía para ver hasta dónde llegan los tentáculos de Washington”. *ABC.com*, 20 octubre 2013. <<http://www.abc.es/internacional/20131030/abci-claves-espionaje-eeuu-201310292139.html>> [Consulta: 12 noviembre 2013]. Clave del caso de espionaje de EE.UU.
- RT Actualidad. “El jefe de Oracle, a favor del espionaje de la NSA”. *RT Actualidad*, 14 agosto 2013. <<http://actualidad.rt.com/actualidad/view/102915-corporaciones-estadounidenses-favor-espionaje-nsa>> [Consulta: 12 noviembre 2013]. Larry Ellison a favor del programa de espionaje estadounidense.
- RTVE. “El ‘pinchazo’ telefónico a una niña asesinada, ¿la gota que colma el vaso de los tabloides ingleses?”. *RTVE.es*, 2011. <<http://www.rtve.es/noticias/20110705/las-escuchas-telefonicas-una-nina-asesinada-hacen-tambalearse-imperio-murdoch/445718.shtml>> [Consulta: 12 noviembre 2013].
- URÍA, Ibon. “Siete trucos para (intentar escapar) del espionaje informático” *Infolibre.es*, 15 julio 2013. <http://www.infolibre.es/noticias/politica/2013/07/11/siete_trucos_para_intentar_escapar_del_espionaje_informatico_5783_1012.html> [Consulta: 17 noviembre 2013]. Algunos trucos para mejorar la privacidad de las comunicaciones en la red.