La tensión entre privacidad y seguridad en el desarrollo de internet

Miguel Moreno Muñoz
Universidad de Granada

mm3@ugr.es

The Tension Between Privacy and Security in the Development of the Internet

Resumen: Los gobiernos y sus agencias de inteligencia disponen de un potencial tecnológico sin precedentes para invadir la privacidad de los ciudadanos en todos los países desarrollados. En la última década, las consideraciones de seguridad e interés nacional han debilitado hasta extremos inaceptables las garantías constitucionales que harían efectiva la protección de la privacidad. Este desequilibrio se explica en parte por el desajuste entre la evolución tecnológica de Internet y de las redes de comunicaciones digitales y las limitaciones de un marco regulador que sigue anclado en criterios y escenarios tecnológicos del siglo pasado. Es preciso incorporar al debate social las consecuencias de la convergencia de formatos en el soporte digital, la proliferación de dispositivos móviles de comunicación y la demanda creciente de servicios en la nube, sustentados en pautas de consumo o de ocio que implican el tráfico intensivo de datos de carácter personal entre países que carecen de reciprocidad en el reconocimiento del derecho a la privacidad.

Palabras-clave: Protección de la privacidad, seguridad, Internet, NSA, Edward Snowden, libertades civiles

Abstract: Governments and their intelligence agencies have an unprecedented technological potential to invade the privacy of citizens and create a surveillance state. Security considerations and national interest have weakened to unacceptable levels the constitutional guarantees that would effectively protect the right to privacy worldwide. This imbalance is partly explained by the mismatch between the technological evolution of the Internet and digital communication networks and the limitations of regulatory frameworks, most of them anchored in concepts, criteria and technological scenarios of the last century. The social debate should incorporate an in-depth analysis of digital media, the proliferation of mobile communication devices and the growing demand for cloud computing services, supported by consumption/entertainment patterns involving intensive data traffic of private information between countries without reciprocity in the recognition of the right to privacy

Keywords: Protection of privacy, security, Internet, NSA, Edward Snowden, civil liberties

ISSN 1989-7022

Introducción

Los casos que ponen a prueba el compromiso de cualquier gobierno con la defensa de las libertades civiles suelen ser aquellos que involucran a ciudadanos poco ejemplares, cuya defensa apenas tiene margen para cuestionar la calidad de las evidencias aportadas por la acusación y la atrocidad de los crímenes cometidos es manifiesta. Las garantías procesales tienen una importancia decisiva precisamente cuando la gravedad de los hechos parece dejar en segundo plano aspectos como el trato justo y equitativo que hasta los individuos más abyectos merecen.

En el desarrollo y configuración tecnológica de la Internet actual, las consideraciones preventivas en aras de la seguridad nacional han adquirido tal predominio sobre

Received: 27/04/2014
Accepted: 01/05/2014

ISSN 1989-7022
DILEMATA, año 6 (2014), nº 15, 181-193

otros derechos y libertades que los propios gobiernos, sus agencias de inteligencia y las grandes empresas tecnológicas con las que colaboran se han convertido en la mayor amenaza contra la privacidad de ciudadanos y usuarios en general.[1]

Se trata de una amenaza mundial, dado el alcance internacional de las redes digitales y de las infraestructuras de comunicación sobre las que las herramientas de interceptación y vigilancia operan; pero potenciada a raíz de las estrategias de seguridad puestas en marcha tras los atentados contra las torres del *World Trade Center* de Nueva York, el 11 de septiembre de 2001 (Brenna, 2009) y mediante instancias como el tribunal estadounidense de Vigilancia de Inteligencia Extranjera FISA, que suele responder dócilmente a las demandas de cobertura legal procedentes de las agencias de inteligencia y cuyas actuaciones han obligado a muchas de las compañías que prestan servicios críticos en las redes digitales o fabrican dispositivos avanzados de comunicaciones a proporcionar datos de millones de usuarios que hacen un uso legal de sus servicios.[2]

Lo novedoso ahora, en términos de ejemplaridad y garantías procesales, es que quienes han revelado los programas de vigilancia masiva y el acceso al contenido –no sólo a los metadatos– de las comunicaciones de millones de usuarios afrontan serias amenazas contra su integridad personal (*The Guardian* y *The Washington Post*, 6 de junio de 2013). Mientras, las personas y agencias responsables de tales abusos continúan sin someterse a mecanismos estrictos de rendición de cuentas ni asumir su responsabilidad por contribuir a un desequilibrio inaceptable en el respeto que merecen libertades y derechos civiles estrechamente conectados como la seguridad y la privacidad (*The Guardian* y *The Washington Post*, 6 de junio de 2013).

Abusos en el acceso de las agencias gubernamentales a datos privados

Diversos informes recientes han analizado la relación entre seguridad y privacidad tanto en las prácticas y casos que permiten apreciar tendencias (en los últimos 5-7 años muy condicionadas por el auge de los servicios *en la nube* o *cloud computing*) como en la evolución del marco jurídico de los países con una infraestructura tecnológica de comunicaciones avanzada.

ISSN 1989-7022

DILEMATA, año 6 (2014), nº 15, 181-193

Restringido al contexto europeo, merece destacarse el estudio encargado por el Comité del Parlamento Europeo para las Libertades Civiles, Justicia e Interior (Directorate General for Internal Policy, 2012). Con anterioridad a las revelaciones de Edward Snowden sobre las prácticas abusivas de los países integrados en la alianza *Five Eyes* de los servicios de inteligencia,[3] los autores del estudio señalaban la descoordinación entre instituciones, servicios y grupos de expertos de la UE encargados de la ciberdelincuencia. El resultado es una percepción inadecuada de los riesgos en relación con el derecho a la protección de datos, las cuestiones de jurisdicción, la responsabilidad y la regulación de las transferencias de datos a terceros países. En términos generales, las políticas y estrategias de la UE no han contribuido a favorecer un equilibrio satisfactorio entre privacidad y seguridad:

- Han descuidado aspectos críticos relativos a la soberanía de la UE sobre los datos de sus empresas, administraciones y ciudadanos, debilitando la protección de los derechos de los ciudadanos en el actual escenario tecnológico, caracterizado por el predominio de servicios en la *nube* (*data centres* y *cloud computing*).
- Por diversas razones –incluyendo la carencia de un concepto operativo de ciberdelincuencia en la UE y el tipo de estándares sobre protección de datos aplicable– dejan un amplio margen de incertidumbre jurídica para delimitar la jurisdicción de la que se depende, las garantías en la protección de datos que merecen los ciudadanos y que deben garantizar a los usuarios las empresas que prestan servicios de comunicaciones o de almacenamiento en la *nube*, en especial cuando implican transferencias de datos a terceros países (Estados miembros, Comisión Europea, EUROPOL).
- Las instituciones concernidas de la UE continúan ligadas a un esquema obsoleto en lo que consideran *delitos informáticos* y subestiman el riesgo para la privacidad de usuarios y ciudadanos de los servicios que implican almacenamiento de datos en la *nube*.
- Los principales foros de las instituciones europeas concernidos con la ciberdelincuencia han dejado en segundo plano o han dado un tratamiento inadecuado al asunto de la protección de datos, ignorando el alcance de los principios democráticos y la protección a los derechos humanos involucrados que exigen los sucesivos desarrollos del marco regulador de referencia en la UE.
- Las negociaciones que han llevado al marco jurídico heterogéneo que define el conjunto de relaciones mediadas por tecnologías de computación en la *nube* (*cloud computing technologies*) no garantizan un equilibrio razonable entre los intereses de ciudadanos, empresas privadas y administraciones públicas. En general, no se terminan de asumir las limitaciones de un sistema legal de transferencias de datos entre países que llevaba en vigor casi 50 años, pero que los servicios y bases de datos en la *nube* han dejado obsoleto y compromete gravemente los derechos individuales de los ciudadanos de la UE.
- El creciente número de servicios, compras e interacciones por Internet implica para los consumidores someterse a un complejo entramado de contratos entre entidades privadas, que con frecuencia difumina aspectos competenciales y de jurisdicción

ISSN 1989-7022
DILEMATA, año 6 (2014), nº 15, 181-193

básicos, dificultando la atribución de responsabilidades y obligaciones legales a los responsables del tratamiento de los datos y la determinación de los derechos de quienes proporcionan los datos que merecen ser protegidos.[4]

- La persecución de los ciberdelitos, en especial de aquellos que requieren investigaciones a través de servicios en la *nube*, se realiza sin una cobertura legal que pueda considerarse adecuada para garantizar la privacidad y protección de los datos personales o corporativos, lo que deja un amplio margen para que agencias e investigadores abusen de sus competencias, en detrimento de la protección legítima que los ciudadanos merecen.
- Las infracciones y abusos de mayor gravedad se cometen al amparo de medidas excepcionales justificadas en nombre de la seguridad y de la eficacia de la lucha contra el terrorismo, puesto que en la práctica permiten justificar prácticas abusivas de los servicios de inteligencia (espionaje industrial, vigilancia masiva, apropiación de datos privados –no sólo metadatos– y grabación de comunicaciones sin relación con delito alguno). Casi todos los países de la UE se han visto sometidos a la presión de demandas inspiradas en la *Patriot Act* estadounidense, o de su enmienda a la *Ley de Vigilancia de Inteligencia Extranjera* (*US Foreign Intelligence Surveillance Amendment Act, FISAA*), de 2008. Es a estos efectos donde resulta más obvia la inadecuación del marco jurídico vigente en la UE para las transferencias de datos a terceros países.[5]

En octubre de 2012, casi un año antes de que E. Snowden aportara los detalles para comprender el alcance de las amenazas contra las libertades civiles del programa de vigilancia masiva desarrollado por la NSA, los expertos advertían al Parlamento Europeo del alcance del programa de vigilancia al amparo de la *FISAA* y de sus implicaciones para la protección de los derechos de los ciudadanos en la UE:

> «The scope of surveillance acted in the above described FISAA, and the fact that it has been extended beyond interception of communications to include any data in public cloud computing as well, has **very strong implications on EU data sovereignty and the protection of its citizens' rights**. The implications for EU Fundamental Rights flow from the definition of "foreign intelligence information", which includes *information with respect to a foreign-based political organization or foreign territory that relates to the conduct of the foreign affairs of the United States*. **In other words, it is lawful in the US to conduct purely political surveillance on foreigners' data accessible in US Clouds**.»[6]

Mientras las instituciones europeas seguían centradas en las estrategias de lucha contra la ciberdelincuencia, su interés por la seguridad no facilitaba una adecuada percepción de los riesgos contra la privacidad y de su estremecedor alcance. En las negociaciones diplomáticas que llevaron a establecer el marco de cooperación vigente hasta octubre de 2013 con las agencias de inteligencia extranjeras se había pasado por alto que "los ciudadanos de la UE podían ser objeto de vigilancia

ISSN 1989-7022 DILEMATA, año 6 (2014), nº 15, 181-193

por razones políticas simplemente por tener sus datos accesibles en servidores/ centros de datos bajo jurisdicción estadounidense". El derecho a la privacidad de los ciudadanos estadounidenses, sin embargo, había de entenderse protegido por las exigencias de la *Fourth Amendment*.[7]

El Congreso de EEUU respaldó esta extensión abusiva de las competencias de las agencias de inteligencia mediante modificaciones aparentemente sutiles (FISAA §1881a en 2008, que autorizaba la vigilancia masiva de ciudadanos extranjeros –residentes fuera del territorio USA–, pero cuyos datos eran almacenados o procesados dentro de la jurisdicción USA; y la cláusula §1880, que incorpora a la definición de *proveedor de servicios de comunicaciones electrónicas* la prestación de "servicios de computación a distancia").[8]

En la práctica, esto supuso que Estados Unidos extendía el alcance de la vigilancia más allá de la interceptación de las comunicaciones, para incluir todos los datos en los servidores públicos de *cloud computing*. Y se justificaba aplicando sólo a sus ciudadanos las garantías en la protección de los derechos constitucionales que el mero interés comercial del país justificaría vulnerar cuando se trata de *data-at-rest* –datos en cualquier soporte de almacenamiento electrónico, diferenciado de *data-in-use*– de ciudadanos extranjeros.[9]

En caso de disputa, la UE llevaría el asunto al Tribunal Internacional de la Haya, cuya jurisdicción Estados Unidos no reconoce. Se refuerza, por tanto, un escenario sin garantías en los tratados internacionales para un grado de reciprocidad satisfactorio en el reconocimiento del derecho a la privacidad, que pudiera contemplar excepciones sólo para circunstancias y casos determinados. En la UE se ha producido una cesión inaceptable de soberanía sobre los datos almacenados en la *nube*, y E. Snowden ha dado detalles bastante precisos sobre cómo afectan a ciudadanos, empresas e instituciones europeas.

Un *universo paralelo* de impunidad en el acceso a datos privados

Los desajustes en la regulación del equilibrio entre privacidad y seguridad y el desarrollo tecnológico de las infraestructuras de servicios en Internet no se restringen al territorio UE. La revista *International Data Privacy Law* publicó en noviembre de

ISSN 1989-7022

DILEMATA, año 6 (2014), nº 15, 181-193

2012 una serie de análisis sobre las leyes y prácticas de nueve países (Australia, Canadá, China, Alemania, India, Israel, Japón, Reino Unido y EE.UU.) en lo que concierne al acceso sistemático de los gobiernos a datos personales en poder del sector privado.[10] La convergencia en las leyes y prácticas de esos nueve países es manifiesta, y permiten identificar tendencias que no invitan al optimismo:

- *Aumentan las demandas de los gobiernos para acceder a bases de datos del sector privado de un modo extensivo y sistemático*, sin depender de la interacción con el personal de la entidad privada titular de los datos.
- Se constata una *falta de transparencia continuada acerca de las actuaciones realizadas y de las leyes relativas al acceso sistemático a los datos en poder del Estado*.
- Se constata un grado de *coincidencia sorprendente en los principios y conceptos fundamentales contenidos en las leyes sobre privacidad de los datos* aprobadas por la mayoría de los países estudiados, incluyendo el hecho de sustraer al alcance de las leyes generales de protección de datos la recopilación de información personal con el fin de hacer cumplir las leyes y en interés de la seguridad nacional.
- En todos los casos se constatan *inconsistencias significativas entre lo que establecen las leyes y lo que los Estados hacen* o están dispuestos a revelar que hacen.
- El retroceso inaceptable en la protección del derecho a la privacidad queda constatado cuando señalan que el principal modo por el que *los Estados consiguen acceso sistemático a la información del sector privado es aprovechando su "voluntarismo sistemático"*, sin recurrir a medidas coercitivas.[11]

Como señalan Kuner et al. (2013: 218-219), mientras gobiernos y Estados han avanzado rápidamente aprovechando el potencial tecnológico consolidado en la última década para recopilar datos y realizar análisis de señales de inteligencia, la perspectiva en el debate social sobre el equilibrio entre privacidad y seguridad sigue anclada en esquemas de finales del siglo pasado. Las actuaciones relativas a la obtención e intercambio de datos de vigilancia electrónica para hacer cumplir la ley parecen más propias de un *universo paralelo*, donde los responsables funcionan al margen de los estándares que las leyes de protección de datos exigen aplicar.

Resulta preocupante la falta de transparencia sobre cómo funcionan las cosas en este dominio y el tipo de justificación con el que las agencias gubernamentales legitiman prácticas tan lesivas del derecho a la privacidad. No parece aceptable promover el interés por la seguridad minando la confianza de los ciudadanos en el imperio de la ley y en la profesionalidad de las empresas e instituciones públicas o privadas con las que interaccionan a través de las redes digitales.[12]

ISSN 1989-7022

DILEMATA, año 6 (2014), nº 15, 181-193

Los programas de vigilancia masiva desvelados por Edward Snowden

Han sido escasos y poco creíbles los intentos de enfatizar el carácter limitado y focalizado en ciudadanos extranjeros del arsenal de herramientas de interceptación de comunicaciones electrónicas desplegado por la NSA y otras agencias de inteligencia. Las declaraciones de sus responsables y del presidente Obama sobre la legalidad de sus actuaciones han quedado en evidencia por sucesivas filtraciones de Snowden. Y chocan con numerosos precedentes (el programa *Echelon*,[13] conocido a finales de los años ochenta; el programa *Carnivore*,[14] para interceptar, filtrar, capturar y descifrar las comunicaciones digitales a través de Internet mediante dispositivos colocados en las instalaciones de los proveedores de servicios de Internet) que prueban la *continuidad de programas destinados a consolidar infraestructuras tecnológicas de alcance mundial cada vez menos selectivas*, con capacidad creciente para interceptar todos los flujos de información que Internet y los operadores de telecomunicaciones hacen posible.

El sistema de vigilancia electrónica PRISM (en clave, SIGAD US- 984XN) es un programa clandestino de vigilancia electrónica y minería de datos desarrollado por la NSA desde 2007. Permite extraer datos de las comunicaciones por Internet registradas en los servidores de empresas como Google Inc. y Apple Inc. que coinciden con los términos de búsqueda aprobados por el tribunal de Vigilancia de Inteligencia Extranjera FISA (conforme a la sec. 702 de la Enmienda a la Ley FISA de 2008).

A través de PRISM la NSA consigue acceder a comunicaciones cifradas en su tránsito por los nodos troncales de Internet y obtener datos fáciles de manejar, aunque este tipo de datos pueden originar muchos falsos positivos y desencadenar actuaciones desproporcionadas. Lo más relevante del programa PRISM es el patrón de actividad sistemática, globalizada y criminal al que responde, puesto que exigía la colaboración forzosa de empresas como Microsoft (propietaria de Skype), Google (YouTube), Yahoo, Facebook, AOL, Apple y PalTalk (un servicio de chat de AVM Software), para tener acceso a mensajes de correo electrónico, videoclips, fotos y llamadas de voz y vídeo, datos de redes sociales, e inicios de sesión y otros datos de acceso a los servicios con mayor demanda en Internet.[15]

Pese a las declaraciones de los responsables de la administración Obama y de la NSA insistiendo en que sus actuaciones se limitaban a recopilar "metadatos" (y sólo bajo requerimiento judicial incluirían el contenido de las comunicaciones), E. Snowden

ISSN 1989-7022

DILEMATA, año 6 (2014), nº 15, 181-193

reveló la existencia del programa MYSTIC, diseñado para rastrear y grabar el 100% de las llamadas telefónicas (y analizar su contenido desde al menos un mes atrás). El programa se inició en 2009 y alcanzó su máxima capacidad en 2011, permitiendo el acceso sin restricciones al contenido de las comunicaciones.[16]

Limitaciones de la Directiva 2006/24/EC y su impacto en las legislaciones nacionales

El arrojo de E. Snowden parece haber abierto los ojos al ejecutivo federal en Alemania[17] y al Tribunal de Justicia de la Unión Europea, que dictó una resolución (08/04/2014) contra la directiva 2006/24/EC aprobada por la Comisión por motivos de seguridad (en reacción a los atentados de Nueva York, Madrid y Londres e influida por la *Patriot Act* de George W. Bush). Esta directiva permitía inicialmente pinchar teléfonos de forma indiscriminada, sin orden judicial, y obligaba a las *telecos* a guardar información de los usuarios durante dos años. La enmienda considera que esa directiva atenta contra los derechos fundamentales y constituye "una injerencia de gran magnitud y especial gravedad en los derechos fundamentales", no limitada a *lo estrictamente necesario*.

Con la perspectiva de los dos últimos años, resulta especialmente llamativo el desdén con el que el propio Tribunal Supremo español aborda el asunto y rechaza el recurso interpuesto por la Asociación de Internautas contra la normativa que regula la interceptación de las comunicaciones.[18] El TS argumenta que los datos del tráfico de llamadas telefónicas, posición geográfica y otros detalles asociados a la comunicación son elementos "accesorios", que no afectan a la intimidad de las personas y que no requieren orden específica de un juez para que las operadoras los cedan a las fuerzas de seguridad.[19]

Pero el Tribunal de Justicia de la Unión Europea considera que los datos de tráfico no pueden considerarse accesorios porque aportan indicaciones muy precisas sobre la vida privada de las personas: "los hábitos de la vida cotidiana, los lugares de residencia permanente o temporal, los desplazamientos diarios, las actividades realizadas, las relaciones sociales y los medios sociales frecuentados", además de aspectos como "la frecuencia de las comunicaciones con determinadas personas durante un periodo concreto".[20]

ISSN 1989-7022

DILEMATA, año 6 (2014), nº 15, 181-193

Resulta desconcertante la frágil cultura de protección en relación con el derecho a la privacidad que permitió la aprobación de la Directiva 2006/24/EC, puesto que presentaba problemas sustanciales:

- Tiene un alcance desproporcionado, pues abarca en general a *todos* los individuos, a *todos* los medios de comunicación electrónica y a *todo* el tráfico de datos, sin ninguna diferenciación, limitación o excepción a tener en cuenta en la lucha contra los delitos graves.
- No establece ningún criterio objetivo para asegurar que los datos sean accesibles únicamente a las autoridades nacionales competentes y que los vayan a usar sólo con fines legítimos.
- No indica los períodos de conservación de datos aplicables a las diferentes categorías de datos ni las personas concernidas o el uso de los datos, dejando sin concretar los criterios para determinar que el período de retención se limite a lo estrictamente necesario.
- No proporciona una garantía suficiente para asegurar protección efectiva contra posibles abusos (los proveedores de servicios podrían tener en cuenta meras consideraciones económicas para determinar el nivel de seguridad, y ésta no estaría garantizada).
- No exige que los datos se conserven en la UE.[21]

Conclusión

Queda un largo camino por recorrer para que pueda considerarse razonablemente alcanzado el necesario equilibrio entre la protección de la privacidad y los requerimientos en materia de seguridad. El alcance global de Internet y de las redes de comunicaciones, sumado a la convergencia de formatos en el soporte digital y a la demanda creciente de servicios *en la nube*, sustentados en pautas de consumo o de ocio que implican el tráfico intensivo de datos de carácter personal, proporciona a los gobiernos y agencias de inteligencia un potencial sin precedentes para invadir la privacidad de millones de ciudadanos en los países tecnológicamente más desarrollados.

Los Estados, sus agencias de inteligencia y las empresas con las que colaboran constituyen hoy la principal amenaza contra la privacidad. Las restricciones de cada agencia para recopilar información de los ciudadanos de su propio país son vulneradas con total impunidad, permitiendo la actividad de las agencias extranjeras aliadas, a las que ampara el secreto de sus acciones en territorio extranjero y la

ISSN 1989-7022

DILEMATA, año 6 (2014), nº 15, 181-193

legitimidad para actuar con toda su capacidad fuera de sus fronteras.

La distopía orwelliana descrita en 1984 se ha transformado desde su contexto político y tecnológico inicial –las actividades de los servicios de inteligencia durante la Guerra Fría– hasta adquirir un potencial estremecedor en la era de Internet, las redes digitales, las comunicaciones móviles y los servicios en la *nube*. El debate social impulsado por la actitud responsable y valiente de informantes como Edward Snowden debe contribuir a enriquecer una cultura de protección de la privacidad que, en demasiados aspectos, continúa anclada en esquemas, valores y escenarios tecnológicos obsoletos.

Referencias

Brenna, R. G. (2009). Los ciudadanos de cristal: vigilancia, privacidad y derechos humanos. *Revista de La Asociaciòn de Escribanos Del Uruguay*, (7), 187–197. Retrieved from http://alfa-redi.org/node/8864

Directorate General for Internal Policy. (2012). *Fighting Cyber Crime and Protecting Privacy in the Cloud* (p. 63). Brussels. Retrieved from http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/study_cloud_/study_cloud_en.pdf

Kuner, C., Cate, F. H., Millard, C., & Svantesson, D. J. B. (2013). PRISM and privacy: will this change everything? *International Data Privacy Law*, *3*(4), 217–219. doi:10.1093/idpl/ipt020

Kuner, C., Cate, F. H., Millard, C., & Svantesson, D. J. B. (2014). Systematic Government Access to Private-Sector Data Redux. *International Data Privacy Law*, *4*(1), 1–3. Retrieved from http://idpl.oxfordjournals.org

Kuner, C., Cate, F. H., Millard, C., & Svantesson, D. J. B. (2014). Systematic Government Access to Private-Sector Data Redux. *International Data Privacy Law*, *4*(1), 1–3. doi:10.1093/idpl/ipt039

Madsen, W. (1997). White House Internet surveillance: combatting conspiracy. *Computer Fraud & Security*, *1997*(2), 6–7. doi:http://dx.doi.org/10.1016/S1361-3723(97)85242-6

Madsen, W. (1999). Barr offers congressional oversight amendment on ECHELON. *Network Security*, *1999*(8), 18–19. doi:http://dx.doi.org/10.1016/S1353-4858(00)80037-9

Madsen, W. (2000). Carnivore's voracious appetite. *Network Security*, *2000*(10), 6–7. doi:http://dx.doi.org/10.1016/S1353-4858(00)10016-9

Madsen, W. (2001). Carnivore Documents Reveal Enhanced Tapping Abilities. *Network Security*, *2001*(1), 5. doi:http://dx.doi.org/10.1016/S1353-4858(01)00111-8

Nabbali, T., & Perry, M. (2004). Going for the throat: Carnivore in an ECHELON world - Part II. *Computer Law & Security Review*, *20*(2), 84–97. doi:http://dx.doi.org/10.1016/S0267-3649(04)00018-4

Schwartz, P. M. (2012). Systematic government access to private-sector data in Germany. *International Data Privacy Law*, *2*(4), 289–301. doi:10.1093/idpl/ips026

ISSN 1989-7022

DILEMATA, año 6 (2014), nº 15, 181-193

Bibliografía

Aceto, G., Botta, A., de Donato, W., & Pescapè, A. (2013). Cloud monitoring: A survey. *Computer Networks*, *57*(9), 2093–2115. doi:http://dx.doi.org/10.1016/j.comnet.2013.04.001

Bagby, J. W. (2009). Balancing the Public Policy Drivers in the Tension between Privacy and Security, 164–183. doi:10.4018/978-1-60566-326-5.ch008.

Bradbury, D. (2014). Can we make email secure? *Network Security*, *2014*(3), 13–16. doi:10.1016/S1353-4858(14)70032-7

Burmester, M., Desmedt, Y., Wright, R., Yasinsac, A., Avenue, P., & Park, F. (2002). Security or Privacy , Must We Choose ? *Symposium on Critical Infrastructure Protection and the Law*, 1–8. Disponible en: http://www.cs.fsu.edu/~yasinsac/Papers/BDWY01.pdf.

Di Salvo, P. (2013). Revolutions between digital utopianism and the "cascade effect." *Studies in Communication Sciences*, *13*(1), 103–104. doi:http://dx.doi.org/10.1016/j.scoms.2013.04.009

Giles, J. (2013). The truth behind the Big Data hype. *New Scientist*, *217*(2905), 48–49. doi:http://dx.doi.org/10.1016/S0262-4079(13)60507-2.

Euripidis Loukis, Ann Macintosh, Yannis Charalabidis, 2012: e-Participation in Southern Europe and the Balkans. London: Routledge.

Everett, B. (2013). Optically transparent: the rise of industrial espionage and state-sponsored hacking. *Computer Fraud & Security*, 2013(10), 13–16. doi:http://dx.doi.org/10.1016/S1361-3723(13)70093-9.

Landau, S. (2013). Making sense from snowden: What's significant in the NSA surveillance revelations. *IEEE Security and Privacy*, *11*(4), 54–63. Disponible en: http://www.scopus.com/inward/record.url?eid=2-s2.0-84881509020&partnerID=40&md5=6dde6b8c9ce768dd67cf0a828cde4c0e

Mansfield-Devine, S. (2014). Editorial. *Computer Fraud & Security*, *2014*(3), 2. doi:http://dx.doi.org/10.1016/S1361-3723(14)70466-X

Morozov, E. (2011). From internet freedom to oppression. *New Scientist*, *209*(2802), 30–31. doi:http://dx.doi.org/10.1016/S0262-4079(11)60501-0

Pearson, S. (2012). *Privacy , Security and Trust in Cloud Computing*. Springer. Disponible en: http://www.hpl.hp.com/techreports/2012/HPL-2012-80R1.pdf

Pinkerton, A., Young, S., & Dodds, K. (2011). Weapons of mass communication: The securitization of social networking sites. *Political Geography*, *30*(3), 115–117. doi:http://dx.doi.org/10.1016/j.polgeo.2010.02.011

Robinson, N., Valeri, L., Cave, J., Starkey, T., Europe, R., Graux, H., & Creese, S. (2010). *The Cloud : Understanding the Security , Privacy and Trust Challenges Final Report* (p. 137). Disponible en: http://cordis.europa.eu/fp7/ict/security/docs/the-cloud-understanding-security-privacy-trust-challenges-2010_en.pdf.

Selmier II, W. T., & Frasher, M. (2013). Differing views of privacy rights in the EU and U.S., and the resulting challenges to international banking: An interview with Joseph Cannataci. *Business Horizons*, *56*(6), 779–786. doi:http://dx.doi.org/10.1016/j.bushor.2013.08.005

Servaes, J. (2013). The many faces of (soft) power, democracy and the Internet. *Telematics and Informatics*, *30*(4), 322–330. doi:http://dx.doi.org/10.1016/j.tele.2013.04.001

Shakarian, P., Shakarian, J., & Ruef, A. (2013). Chapter 3 - How Cyber Attacks Augmented Russian Military Operations. In P. Shakarian, J. Shakarian, & A. B. T.-I. to C. Ruef (Eds.), (pp. 23–32). Boston: Syngress. doi:http://dx.doi.org/10.1016/B978-0-12-407814-7.00003-8

ISSN 1989-7022

Shirazi, F. (2014). Interrogating Iran's restricted public cloud: An Actor Network Theory perspective. *Telematics and Informatics*, *31*(2), 228–236. doi:http://dx.doi.org/10.1016/j.tele.2013.08.005.

Schneier, B. (2003). *Beyond fear. Thinking Sensibly About Security in an Uncertain World*. Copernicus Books (Springer Verlag).

Notas

1. Para la discusión sobre el uso de "privacidad" en lugar de "intimidad", me remito al análisis morfológico y semántico de J.A. Díaz Rojo, *Privacidad: ¿neologismo o barbarismo?* Disponible en: http://pendientedemigracion.ucm.es/info/especulo/numero21/privaci.html.

2. "In brief". (2014). *Computer Fraud & Security*, 2014(3), 4. http://dx.doi.org/10.1016/S1361-3723(14)70468-3

3. Integran la alianza *Five Eyes* la agencia NSA de Estados Unidos, el Government Communications Headquarters (GCHQ) del Reino Unido; el Defence Signals Directorate (DSD) de Australia; la Communications Security Establishment Canada (CSEC) de Canadá y la Government Communications Security Bureau (GCSB) de Nueva Zelanda. Los miembros del núcleo duro –la denominada comunidad UKUSA– tienen los mayores privilegios en el acceso a la información compartida y disponen de margen de acción para actuar en territorio extranjero, sobre todo allí donde la legislación impide a otras agencias de la alianza actuar contra sus propios ciudadanos.

4. Véanse (en Directorate General for Internal Policy, 2012) las págs. correspondientes al *Executive summary* (8-9) y los aspectos señalados en la sección *Key findings* (10-11).

5. Cfr. *ibid*., págs. 14, 27, 34-35 y 48.

6. *Ibid*., p. 34. Énfasis presente en el original.

7. Cfr. PETITION FOR REVIEW OF A DECISION OF THE UNITED STATES FOREIGN INTELLIGENCE SURVEILLANCE COURT, Aug. 22, 2008. Pág. 6. Disponible en: http://www.fas.org/irp/agency/doj/fisa/fiscr082208.pdf.

8. Cfr. págs. 33-35 (y anotaciones en p. 34) del estudio citado en la nota 3.

9. La cláusula FISAAA 1881a habilita a diversas instancias para acceder a cualquier dato que pueda circular por las redes digitales y centros de datos bajo jurisdicción USA, con el propósito de promover el interés general de los EE.UU. en política exterior (y no exclusivamente para la lucha contra delitos graves: terrorismo, blanqueo de capitales, etc.).

10. Patrocinados por la organización sin ánimo de lucro *The Privacy Projects.* Cfr. (Kuner et al., 2014).

11. Cfr. el editorial de Kuner, Cate, Millard y Svantesson (2014: 1).

12. *Ibid*.

13. Cfr. Madsen, 1999Georgia Republican Congressman Bob Barr successfully introduced an amendment to the Intelligence Authorization Act that would require the Department of Justice, the National Security Agency (NSA. La amenaza de *Echelon* fue objeto de análisis en el Parlamento Europeo en 2001, a partir del *Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)* (2001/2098(INI)), PE 305.391 A5-0264/2001.

ISSN 1989-7022

DILEMATA, año 6 (2014), nº 15, 181-193

14. Cfr. Nabbali & Perry, 2004; Madsen, 1997, 2000, 2001.

15. Los detalles aportados por el informante E. Snowden aparecen en los dossiers difundidos por *The Guardian* y *The Washington Post* a partir del 6 de junio de 2013.

16. Cfr. http://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html.

17. Alemania (cfr. Schwartz, 2012) ha tomado algunas medidas significativas, entre ellas un nuevo proyecto de ley federal para la "declaración de residencia", el abandono del proyecto ELENA (*Elektronisches Entgeltnachweis-Verfahren*, la mayor base de datos oficiales, en su mayoría de los empleados del gobierno federal, que permitiría agilizar pagos y trámites que requieren procesos de verificación electrónica) y la propuesta de una *Bundes-Cloud* (*nube federal*) destinada a mantener los datos personales de los alemanes en centros de datos de las corporaciones estadounidenses.

18. Sentencia 44/2008 de 5 de febrero.

19. Cfr. http://www.internautas.org/sincanon/html/8210.html.

20. Cfr. http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf; el fallo completo en: http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=406846.

21. Cfr. http://www.mcguirewoods.com/Client-Resources/Alerts/2014/4/EU-Court-of-Justice-Declares-Data-Retention-Directive-Invalid.aspx.