Paakat
Revista de tecnología y sociedad

ISSN: 2007-3607

Universidad de Guadalajara
UDGVIRTUAL
suv.paakat@redudg.udg.mx
México

Internet y seguridad: los nuevos retos de un mundo globalizado

Juan Manuel Fernández Chico
jmfernandezchico@gmail.com
Universidad de Guadalajara

Paakat: Revista de Tecnología y Sociedad, "Redes sociales y diversidad".
Año 2, Número 3, septiembre-enero 2012-2013.

Recibido:16-08-2012
Aceptado para su publicación: 27-08-2012

Juan Manuel Fernández Chico, licenciado en sociología por la Universidad Autónoma de Ciudad Juárez (UACJ) y estudios sobre Estudios de Frontera y Latinoamericana por Universidad de Texas en El Paso (UTEP), actualmente estudiante de la Maestría en Ciencias Sociales en especialidad en comunicación por la Universidad de Guadalajara (UDG). Coautor del libro Correspondencias. Cartas, figuras y personajes: una respuesta a la modernidad, una aproximación a las sociedades contemporáneas, junto con Luis Alfonso Herrera, publicado por la Universidad Autónoma de Ciudad Juárez (2008), y autor del libro La mirada indiscreta: sobre la vigilancia anticipada, Editorial Vagón (2009).

Internet y seguridad: los nuevos retos de un mundo globalizado

Juan Manuel Fernández Chico

YALA'

Resumen

Internet es uno de los fenómenos tecnológicos de información más importante de todos los tiempos, transformando la economía, las relaciones sociales, la política y, sobre todo, la seguridad. Aquí se hace mención de tres aspectos importantes en esto último: el papel de la privacidad, los delitos cibernéticos y la cooperación internacional. En cada uno describiremos las implicaciones presentes y los retos de los Estados, concluyendo en la necesidad de un cambio de perspectiva en lo referente al territorio y el gobierno de Internet.

Palabras clave

Internet, sociedad de la información, seguridad, privacidad, delitos cibernéticos.

Abstract

Internet is one of the most important information technology phenomenon of all time, transforming the economy, social relations, politics and, above all, security. In this work there are three important aspects in the matter of security: the role of privacy, cybercrimes and international cooperation. In each, we will describe the implications and challenges of the State, concluding on the need for a change in perspective in relation to the territory and Internet governance.

Keywords

Internet, society of information, security, privacity, cybercrimes.

La sociedad de la información

-Sí, el lugar donde están, sin confundirse, todos los lugares del orbe, vistos desde todos los ángulos.
(...)
vi el Aleph, desde todos los puntos, vi en el Aleph la tierra, (...) vi mi cara y mis vísceras, vi tu cara, y sentí vértigo y lloré, porque mis ojos habían visto ese objeto secreto y conjetural, cuyo nombre usurpan los hombres, pero que ningún hombre ha mirado: el inconcebible universo.

Jorge Luis Borges, *El Aleph*.

Internet, breve boceto de su presente

El origen de Internet es para nada incierto. Fue parte de un trabajo de inteligencia del departamento de seguridad de los Estados Unidos que buscaba conectar sistemas informáticos en red. Pero lejos de su origen, Internet es un espacio con múltiples retos, pues se ha involucrado de manera profunda en muchas prácticas cotidiana (Bunyavejchewin, 2010; Everard, 2000). Poco a poco vemos cómo estas tecnologías de información, que giran en torno a la Internet, comienzan a tomar protagonismo en nuestra vida, donde pensadores como Manuel Castells abogan por un derecho universal a Internet (Revista ñ, 2010). Para algunos autores, esta serie de cambios tecnológicos describen una *sociedad de la información* que hace referencia a un mundo cada vez más comunicado entre sí por medio de redes tecnológicas (Mattelart, 2002; Sempere, 2008). Marshall McLuhan, quien intentó predecir una sociedad conectada por las nuevas tecnologías, le llamó la aldea global (McLuhan, 1996). Parecido, Raúl Trejo Delarbre tituló uno de sus libros *Viviendo en el Alpeh*, quien utiliza el eje narrativo del cuento del escritor argentino Jorge Luis Borges para describir Internet. Alberto Constante escribe que al presionar una tecla, el mundo es nuestro por lo que podemos tener miles de bits de información en cuestión de segundo (Constante, 2005).

Nunca antes, en la historia de la humanidad, habían existido tantas posibilidades de acceder a tanta información, tan variada y de forma tan pública (Tre-

jo, 2006). Por eso Trejo Delarbre cree que la manera más gráfica para explicar la Internet es por medio de la figura del Aleph: "(...) todos los lugares de la Tierra están en el Aleph, ahí estarán todas las luminarias, todas las lámparas, todos los veneros de luz" (Jorge Luis Borges). La analogía de Trejo Delarbre no es para nada complaciente, pues para muchos *sin-acceso* son irrelevantes los avances o retrocesos de la Internet.

En una entrevista, Manuel Castells dice que estar desconectado es estar excluido (Revista ñ, 2010), por lo que Internet como una red totalitaria aún está lejos de ser evidente. El mismo Trejo Delarbre dice que cuatro de cada cinco mexicanos, por ejemplo, no tiene acceso a la Internet, lo que hace palpable eso que algunos han llamado *la brecha digital* (Serrano y Martínez, 2003). Pero habría que tener cuidado con esta expresión, pues el hecho de no tener acceso a Internet tampoco debería ser, por consecuencia, un des-conectado, pues muchas de las cosas que hacemos como ver televisión, llamar por teléfono celular, usar un cajero automático, o tener membrecía en alguna tienda departamental, están conectadas en redes similares a Internet (a veces basadas en Internet, como muchos canales de televisión). Pero el hecho de ser Internet la red informática más importante, el no estar conectado en ella es estar literalmente *desconectado*.

Pero del otro lado, los *conectados* se ven involucrados en un fenómeno sumamente reciente y que ha modificado aspectos esenciales de su vida, como es la rapidez de acceso a cantidades apabullantes de información, dependencia de nuevas tecnologías que facilitan tareas cotidianas, así como centrar una importante parte de su entretenimiento y tiempo de ocio en navegar en Internet. La revista *Time*, en el mes de noviembre de 2010, sacó una serie de artículos en donde presentaba una lista de malos hábitos causados por la adicción a Internet, como la impaciencia y la tendencia a olvidar las cosas. Manuel Castells, por otro lado, dice que estas tecnologías deben ser entendidas de manera contraria, pues argumenta que es benéfico estar en constante conexión y renovando nuestra información (Revista ñ, 2010). Independientemente de eso, el mundo parece tender a estar más conectado a través de Internet. De acuerdo al *Internet World Stats*, de los casi 7 mil millones de habitantes que tiene el mundo, para finales de 2011 habría 2,267,233,742, es decir, el 32.7%, con un incremento del 528.1% de 2000 a 2011. Cabe destacar que Medio oriente y África son las regiones con mayor crecimiento, y, a la vez, los más desconectados, África sólo tiene una penetración del 13.5%.

Los nuevos retos de seguridad

Privacidad

Bruce Schneier, en una conferencia sobre privacidad en Internet, dijo que la tecnología de la información actual tiende a crear sistemas que nunca olvidarán los datos que pasan por ellos, haciendo referencia a eso que generamos cuando hacemos uso de nuevas tecnologías de información: un teléfono celular, cualquier movimiento desde un buscador en Internet, alguna transacción bancaria desde la Red. Schneier dice que existen diferentes tipos de información personal acumulada en alguno de estos sistemas tecnológicos: la que producimos nosotros (fotografías, vídeos, textos); la que se genera por casualidad (por ejemplo la fotografía de una multitud en la que podemos estar nosotros, o la crónica de un evento al que asistimos); la que se genera a través de lo que hacemos (al dejar huellas digitales al momento de navegar en Internet); y, finalmente, la que surge al combinar todas las anteriores (BT Benelux and Skybox Security, 2010).

Schneier define la privacidad como la capacidad de controlar nuestra información, y de presentarla en los contextos que nos sea más conveniente, y el problema con la que se genera en Internet, es que el usuario pierde el control, convirtiéndolo en material a disposición de quien pueda y quiera tomarla. María Nieves Saldaña comparte la misma preocupación sobre el uso de la información, argumentando que la privacidad debe ser considerada como un nuevo reto frente a las tecnologías de información basadas en Internet, pues, dice, el usuario nunca debe perder su capacidad de controlar la información que genera (Nieves, 2007). Esta pérdida de privacidad es en parte generada por el incremento de usuarios que navegan en el ciberespacio y por un aumento de prácticas que exponen la privacidad de estos usuarios, impulsado por páginas dedicadas a vender información personal ofrecida voluntariamente (como es el caso de Facebook, en donde sus clientes pagan anuncios publicitarios en la página mientras los usuarios sigan externando su vida privada).

Paula Sibilia explica éste fenómeno con mayor precisión en su libro *La intimidad como espectáculo*, donde nos indica que una importante cantidad de usuarios en Internet hacen una práctica de *confesión*, en donde exponen su intimidad: blogs, redes sociales, espacios personales, comunidades en red de intercambio de archivos, etc. (Sibilia, 2008:32). Situación que pone en riesgo la con-

servación y control de la privacidad de los usuarios al subir información personal que luego puede ser utilizada para fines perjudiciales. El fenómeno explicado por Paula Sibilia parece ir en aumento, como lo muestra un reciente estudio de *Internet World Stats*, pues en casi seis años, Facebook ha logrado cautivar más de 517 millones personas en más de 212 países (*Internet World Stats*, 2010). Europa es la región con más usuarios, con 162'104'640 (es decir el 19.9%, casi una cuarta parte de los usuarios conectados al Internet), mientras en el norte de América, encabezado por Estados Unidos (con 132'810'940 de usuarios), cuenta con 149'054'040. América del Sur concentra 49'771'960, Asia 93'584'580, mientras en la cola se encuentra África (17'607'440) y Oceanía (11'596'660) (Internet World Stats, 2010). Los riesgos de pérdida de privacidad van en aumento de manera paralela, pues el mismo Facebook admite que su plataforma no es completamente segura (El Universal, "Facebook admite fallas en seguridad" 18/10/2010 The Jakarta Globe "Facebook overhauls privacy controls alter internal cranking" 27/05/2010).

Delitos cibernéticos

Junto con el aumento de la pérdida de privacidad, aumentan los riesgos de un ataque cibernético[1] gracias a diversas técnicas que se han adaptado a redes sociales como Facebook. Los riesgos provienen principalmente por aplicaciones falsas que son generadas de manera automática (como lo hacen los *worms*, que son virus informáticos que se multiplican de manera automática), principalmente por juegos o fotografías que los esconden (Perkel, 2010). Por lo que el crecimiento de las redes sociales también ha causado un aumento de la inseguridad en la Internet (Cobb, 2009).

Desde hace diez años, las agencias de seguridad de los países industrializados comenzaron a generar grupos especializados dentro de sus cuerpos policíacos encargados exclusivamente de defender el territorio virtual (Ruiloba, 2006; Cano, 2009; Gutiérrez, 2010). Internet se convirtió en otro campo de batalla, principalmente después de algunos ataques cibernéticos con magnitudes tan imponentes como los de las Olimpiadas de 2002 cuando un competidor surcoreano fue descalificado y hubo un ataque masivo de DoS[2]; en Estonia en 2007, al momento que se retiró una estatua de la resistencia soviética contra el nazismo; o el de Irán en 2010, para sabotear su programa de energía nuclear, entre otros. A los que debemos sumar además los ataques a las bases de datos de Google, laboratorios en universidades, páginas oficiales de gobiernos y computadoras personales (Acohido y Swartz, 2004). Jeffrey Perkel enfocó un estudio a los ataques perpetrados a centros universitarios, los cuales ganan popularidad como blancos de los delincuentes cibernéticos. La Universidad de San Diego, en California tuvo un promedio de 27'000 intentos de intrusión por día durante los primeros tres meses de 2010 (Perkel, 2010).

Byron Acohido y Jon Swartz escriben que con el hecho de estar conectado a Internet, exponemos nuestros sistemas informáticos a una serie incalculables de peligros. Basados en un trabajo de investigación hecho por Avantgarde, una computadora con procesador *Windows XP* tiene un promedio de 341 ataques si no cuenta con un firewall, que quiere decir corta fuego para contener ataques externos, mientras una computadora con procesador Mac sufrió 339 ataques en una hora. *Avantgarde* adelanta que 67% de los usuarios en Internet no usan nin-

1 Debe entenderse delito cibernético como todo delito que sucede en el ciberespacio. No existe un consenso sobre el término que mejor represente a estos actos delictivos en la Internet, algunos autores hacen diversos usos de términos, como *delitos informáticos* (Cano, 2009; López, 2007) o *delitos telemáticos* (López, 2007), *crímenes virtuales* (Grabosky, 2001), *amenazas a un sistema de información* (Gómez, 2010), *cibercrímenes* (Grabosky, 2001; Cano, 2009; Brenner, 2010), *ciberterrorismo* (más común Estados Unidos, principalmente después del 11 de septiembre de 2010, donde el Buró Federal de Investigación le ha definido como el ataque directo a un gobierno por medio de acciones informáticas) es un término que para ciertos autores integra delitos dentro de Internet pero con matices específicos, mientras otros autores los identifican de manera más general (Gable, 2010; Ford y Gordon, 2003; Ruiloba, 2006), pero por fines de compatibilidad con los documentos oficiales policíacos en México y la generalidad que abarca su matización, en este proyecto se usará delitos cibernéticos.

2 DoS quiere decir Denied of service, que en español es Negación de servicio, que consiste en mandar mensajes o conexiones falsas a un sistema informático hasta que se satura y colapsa. La magnitud de éste tipo de ataque se mide por el número de veces que fue mandada una falsa conexión, por lo que se hace uso de un ejército de *script kiddies*, que son usuarios aficionados que se unen a la causa del ataque, pero sin tener grandes conocimientos de hackeo, donde lo único que deben hacer es mandar la señal desde sus computadoras personales. Esta técnica, que se ha utilizado para sabotear sistemas informáticos de gobiernos o grandes empresas, aparte de ser sumamente efectiva, es imposible de rastrear, pues los falsos mensajes pueden venir de cualquier parte del mundo.

Desde hace diez años, las agencias de seguridad de los países industrializados comenzaron a generar grupos especializados dentro de sus cuerpos policíacos encargados exclusivamente de defender el territorio virtual

gún tipo de *firewall*, lo que expone a un sistema a esa cantidad de ataques. Los autores concluyen que nunca la Internet había sido tan insegura como lo es actualmente (Acohido y Swartz, 2004).

Pero no se pueden limitar los delitos cibernéticos sólo a lo que ocurre en un sistema informático como es la computadora, o en la simple acción de navegar en Internet, pues el avance tecnológico también ha provocado que muchas de las vulnerabilidades antes discutidas migren a otras tecnologías de comunicación. Hillie Koskela se suma a las voces que prestan mayor atención a la telefonía móvil, argumentando que ésta ha comenzado a infiltrarse en mayor medida a la vida cotidiana al reducir su tamaño y su costo, así como el aumentar sus aplicaciones y usos al momento de conectarlo a la Red. Los celulares sirven como máquinas de registro fácilmente adaptables y que pueden ser usados por cualquiera (Koskela, 2004). Lo cual debe ser entendido como otro reto a la privacidad, pues toda la información que genera un teléfono móvil (mensaje, llamadas, fotografías, vídeos) puede perder su rastro y multiplicarse indefinidamente. De acuerdo a un estudio realizado por *Symantec*, 87% de las personas que encuestaron se sienten inseguras al navegar por sus teléfono móviles al percibir que no existen garantías de seguridad (Net Security, 2010).

Acuerdos internacionales de intercambio de información

Uno de los puntos nodales en la seguridad de Internet, es la cooperación internacional. El modelo nacionalista de la seguridad a través de la defensa de la soberanía, envergadura que le corresponde a un cuerpo gobernante y policíaco, no parece adecuarse a la realidad actual. Muchos de los ataques cibernéticos provienen de países extranjeros, a veces con distanciamientos políticos que nos les permiten actuar con facilidad (Astier, 2005; Eriksson y Giacomello, 2006). Para autores como Stéphane Astier, el gobierno sobre Internet debe trascender a las fronteras territoriales si es que en verdad quiere convertirlo en un espacio seguro, y propone que sean las Naciones Unidas el organismo responsable (Astier, 2005). Otros como David L. Carter proponen que sean las policías de los países quienes comiencen a generar trabajos de cooperación entre sí, pues aunque el Estado-nación, y sus formas territorialistas y nacionalista de operar están en decadencia (Bauman, 2006; Beck, 2005), para éste autor el Estado sigue siendo el único responsable de garantizar y mantener la seguridad, ya sea en el espacio físico o en el virtual (Carter, 2009). Eriksson y Giacomello proponen que exista una mayor cooperación internacional en lo referente a acuerdos, pero que sean los Estados quienes los pongan en práctica (Eriksson y Giacomello, 2006; Gable, 2010). Los autores explican cómo naciones como Rusia, China y Estados Unidos, después de la Guerra Fría, comenzaron a crear cuerpos especializados para cuidar y medir la seguridad en Internet, lo que es un esfuerzo plausible, pero ineficiente, pues la Guerra Fría inaugura una transición de una sociedad industrial a una de información, provocando un aumento de usuarios que navegan por la Internet (usuarios lícitos e ilícitos), haciendo que esta sea imposible de controlar completamente desde un solo país (Eriksson y Giacomello, 2006). Por lo que Internet debe ser entendido como un espacio multiterritorial, y público, en donde la política del Llanero solitario no tiene cabida (Astier, 2005), pues jamás las naciones habían estado tan vulnerables (Gable, 2010). Kelly Gable escribe que éstos grupos delictivos que pretendan perpetrar ataques cibernéticos no necesitan de una gran infraestructura para hacerlo (Gable, 2010). Como lo dijo el director de seguridad doméstica en Estados Unidos, Tom Ridge, los terroristas ahora pueden paralizar la economía global o apagar un generador de electricidad sentado frente a una computadora (Eriksson y Giacomello, 2006). Esta estrategia de ataque debe ser analizada por tres puntos: la creciente ola de nuevas tecnologías de información que avanzan mucho más rápido de lo que lo hacen los sistemas de seguridad; la capacitación cada vez más accesible para aprender a manipularla; y, por último, que se puede sumar más gente a la causa ideológica del ataque, reduciendo los riesgos de perder la vida o ser capturado (Dartnell, 2006). Éste último punto ha sido poco estudiado, pues como en el caso de Estonia (2007) muchos jóvenes rusos, con poco conocimiento en uso de tecnologías informáticas, cooperaron en el ataque de DoS contra las páginas del gobierno, congelando al país por casi una semana. Incluso habría que imaginar el escenario de de miles de usuarios a lo largo del mundo atacando un mismo objeto bajo una insignia. Jose Nazario, un experto en delitos cibernéticos, dice que el caso

de Estonia en 2007 fue un parteaguas en la seguridad cibernética, pues ésta ha comenzado a ser una preocupación para los países que se ve reflejada en la inversión que hacen para desarrollar tecnología y capacitación de personal en defensa de su seguridad nacional (CNET News, "Cyberattack in Estonia—what it really means", 29/05/2007).

Conclusiones

Internet nos debe obligar a pensar de otras formas y bajo otros medios. No sólo por las implicaciones en seguridad (que brevemente han sido explicadas aquí), sino en un contexto general, pues una sexta parte del mundo está conectada a ésta enorme Red, y muchos, un importante número de éstos, dependen de alguna u otra forma de ella. Poco a poco nos enfrentamos ante nuevos retos a los que no estábamos acostumbrados, como es el caso de *Wikileaks*, que he dejado aparte por lo enorme y actual del tema, que necesitaría ser abordado de manera exclusiva. Hay que pensar qué tan vigentes son los modelos de seguridad basados en el territorio, ante un mundo cada vez más conectado.

Referencias

ACOHIDO, B. y J. Swartz, (2004). "Unprotected PCs can be hijacked in minutes". *USA Today*. Estados Unidos, Recuperado el día 29 de noviembre de 2004, de http://www.webcitation.org/query.php?url=http://www.usatoday.com/money/industries/technology/2004-11-29-honeypot_x.htm&refdoi=10.1186/gb-2005-6-9-119

ASTIER, S. (2005). "Ethical regulation of the Internet: the challenges of global governance". *International Review of Administrative Science*. Número 71; pp. 133.

BAUMAN, Z., (2006). *La sociedad sitiada*. Argentina: Fondo de Cultura Económica.

BECK, U. (2005). *La mirada cosmopolita o la Guerra es la paz*. España: Paidós.

BUNYAVEJCHEWIN, P. (2010). "Internet politics: Internets as a political tool in Thailand". *Canadian Social Science*. Volumen 6, número 3, 2010; pp. 67-72.

CANO, J. (2009). *Computación forense. Descubriendo los rastros informáticos*. México: Alfaomega.

CARTER, D. y J. G. Carter. (2009). "Intelligence-Led policing: conceptual and functional considerations for public policy". *Criminal Justice Policy Review*. Volumen 20, número 3. Septiembre 2009; pp. 310-325.

COBB, M. (2010). "Risk of social networking: preparing for e-discovery issues, threats". *Search Security*. Gran Bretaña, recuperado el día 26 de agosto de 2009, de: http://searchsecurity.techtarget.co.uk/tip/0,289483,sid180_gci1366092,00.html

CONSTANTE, A. (2005). "En el reino del bit o la historia de un crimen". en Islas, O y Claudia Benassini (comp.), *Internet, columna vertebral de la sociedad de la información*. México: Instituto Tecnológico y de Estudios Superiores de Monterrey.

DARTNELL, M. (2006). *Insurgency online: web activism and global conflict*. Canadá: University Toronto Press.

EVERARD, J. (2000). *Virtual states.* Estados Unidos: Routledge.

GABLE, K. (2010). "Cyberterrorism and using universal jurisdiction as a deterrent". *Vandebilt Journal of Transnational Law*. Volumen 43; pp. 57.

GÓMEZ, J. (2010). *Guía de campo de hackers*. México: Alfaomega.

GORDON, S. y R. Ford. (2003). "Cyberterrorism" en Symantec. Recuperado el día 19 de agosto de 2008, de http://www.symantec.com/avcenter/reference/cyberterrorism.pdf

GRABOSKY, P. (2001). "Virtual criminality: old wine in new bottles?". *Social and Legal Studies*. Número 10; pp. 243.

GUTIÉRREZ, G. (2010). "Control y vigilancia en la nueva sociedad de la información". *Razón y palabra*. Número 37. México, disponible en: http://www.razonypalabra.org.mx/anteriores/n37/fgutierr.html

JEFFREY, P. (2010). "Cybersecurity: how safe are your data?". *Nature*. Recuperado el día 28 de abril de 2010, de http://www.nature.com/news/2010/100428/full/4641260a.html
JOHAN, E. y G. Giacomello. (2006). "The information revolution, security, and international relations: (IR)relevant Theory?". *International Political Science Review*, volumen 27, número 3, 2006; pp. 221-244.
KOSKELA, H. (2004). "Webcams, TV shows and mobil phones: empowering exhibitionism". *Surveillance and society,* 2004.
MATTELART, A.(2002). *Historia de la sociedad de la información*. España: Paidós.
MCLUHAN, M. y B. R. Powers. (1996). *La aldea global. Transformaciones en la vida y los medios de comunicación mundiales en el siglo XXI.* España: Gedisa editorial.
NIEVES SALDAÑA, M. (2007). "La protección de la privacidad en la sociedad tecnológica: El derecho constitucional a la privacidad de la información personal en los Estados Unidos". *Araucaria*, año 9, volumen 9, número 18, Universidad de Sevilla, 2007; pp. 85-115.
RUILOBA, J. C. (2006) ."La actuación policial frente a los déficits de seguridad de Internet". *Primer congreso sobre Internet, derecho y política: las transformaciones del derecho y la política en la sociedad de la información*. Número 2, Revista de Internet, Derecho y Política.
SEMPERE, P. (2008). *McLuhan en la era Google. Memorias y profecías de la Aldea Global*. España: Editorial Popular.
SERRANOS, A y E. Martínez. (2003). *La brecha digital*. México: Universidad Autónoma de Baja California.
SIBILIA, P. (2008). LA INTIMIDAD COMO ESPECTÁCULO. México: Fondo de Cultura Económica.
TREJO D. R. (2006). *Viviendo en el Aleph. La sociedad de la información y sus laberintos*. España: Gedisa.

Revistas y páginas electrónicas consultadas

Internet World Stats, Usage and population statistics (2011). Recuperdado el día 1 de enero de 2012, de http://www.internetworldstats.com/
BT (2010). Disponible en: http://www.bt.com/ Recuperado el día 20 de noviembre de 2010.
Revista ñ. (2010). "Internet debe ser un derecho universal" en *Revista ñ* [En línea]. Argentina. Recuperado el día 1 de agosto de 2010, de http://www.revistaenie.clarin.com/notas/2010/08/01/_-02206423.htm
El Universal. Recuperado el día 18 de octubre de 2007, de: http://www.eluniversal.com.mx/articulos/61125.html
The Jakarta Globe. Recuperado el día 20 de noviembre de 2010, de http://www.thejakartaglobe.com/home/facebook-overhauls-privacy-controls-after-internal-cranking/377387
Net Security. Recuperado el día 20 de noviembre de 2010, de http://www.net-security.org/secworld.php?id=10064
CNET News. Recuperado el día 29 de mayo de 2007, de http://news.cnet.com/Cyberattack-in-Estonia-what-it-really-means/2008-7349_3-6186751.html#ixzz15kKxk6tp

¿Cómo citar?
FERNÁNDEZ CHICO, J. M. (2012, septiembre). Internet y seguridad: los nuevos retos de un mundo globalizado, en *Paakat: Revista de Tecnología y Sociedad*. Año 2, Número 3, septiembre-enero 2012-213.