

¿PRIVACIDAD O COMODIDAD? EL USO IRREMEDIABLE DE LAS TI

Por José Juan Gálvez Percasteguí.

La alta demanda de las tecnologías de información ha propiciado el desarrollo de sistemas con gran capacidad de almacenamiento y respuesta. Gracias al gran desarrollo de dichos sistemas, y a la dependencia contemporánea, el ciberespacio es un vasto lugar que además de presentar grandes beneficios, también puede funcionar como medio para todo tipo de actividades ilícitas. Aunque internet sea la herramienta del siglo y nos facilite la vida en gran medida, este puede ser un instrumento muy inseguro si es que no se utiliza con precaución.

En pleno siglo XXI y bajo la revolución tecnológica, el uso de las tecnologías de información ha propiciado el desarrollo de sistemas con gran capacidad de almacenamiento y respuesta. En este sentido, los gobiernos y las empresas han sabido explotar el incremento exponencial de la tecnología. Pero de igual forma se debe invertir en sistemas seguros que aporten fiabilidad y privacidad para el usuario.

El cibercrimen es un problema que nos compete a todos. En un mundo globalizado, con el alance y penetración de las tecnologías de información es necesario estar bien informado para evitar ser víctimas de alguno de estos ataques. La privacidad en la web es un tema muy delicado. No solo el cibercrimen es un tema de controversia mundial, también el espionaje revelado por parte de Edward Snowden ha propiciado la desconfianza de los usuarios de internet. Saber que el gobierno puede interferir en tu vida privada a través de la web, es un dilema ético de gran escala y de diferentes vertientes. Ante esta situación de gran complejidad, existe un gran conflicto de interés de diversas partes. Por un lado, el gobierno intenta brindar una solución a la seguridad nacional y con esta idea justifica el espionaje realizado a la población. Por otra parte se encuentran las grandes empresas tecnológicas como Google, Facebook, Yahoo!, etc... Que se ven participantes prioritarios en la seguridad y tratamiento que le brindan a nuestra información personal, y que reniegan de trabajar con el gobierno para la extracción y posesión de datos. Por último, nosotros los usuarios que representamos la mayoría agraviada en esta situación, pero que denotamos una clara irresponsabilidad e ignorancia sobre nuestro derecho digitales.

En un mundo en donde las tecnologías de información son utilizadas a nivel mundial prácticamente en cualquier gestión de actividades, la seguridad en este medio representa un factor de vital importancia.

VENTAJAS Y DESVENTAJAS.

A pesar de que las TI son de extrema utilidad, estas mismas han creado un espacio para nuevas amenazas a la privacidad y seguridad, debido a que el funcionamiento y control de diversas empresas y gobiernos reside propiamente en estos sistemas.

De acuerdo con Maroto (2009), “Las infraestructuras críticas, compuestas de instituciones públicas y privadas, constituyen el sistema nervioso de las naciones desarrolladas. El ciberespacio es fundamental para su funcionamiento y, por ello, para la seguridad de la nación”. La integración de la tecnología en estos sistemas críticos, los hacen vulnerables, al ser alcanzables desde cualquier punto. “Un ataque contra el sistema informático de una infraestructura crítica puede generar muchos daños con un riesgo mínimo para el atacante” (Maroto, 2009). El factor distancia y dificultad de identificación permea a los agresores a realizar este tipo de acciones.

A pesar de las vulnerabilidades y el factor crítico en dichos sistemas, Medero (2013) argumenta que “Las TIC han ocasionado una revolución sin precedentes. La globalización ha sacudido los pilares de las instituciones y las bases de nuestra sociedad, hasta el punto de sugerir el nacimiento de otra sociedad paralela, que se conoce como Sociedad de la Información y Comunicación”. En este sentido, es bien sabido que internet nos facilita la vida en gran medida debido a su facilidad y prontitud informativa.

Sin embargo, el uso en gran medida de los servicios tecnológicos afecta a gran escala si es que estos no se encuentran con la seguridad adecuada para su funcionamiento. Los daños provocados por una falla de seguridad en dichas sistemas van más allá de la obtención de información. Maroto (2009) afirma que “estas redes también controlan instalaciones físicas, como estaciones transformadoras de electricidad, centrales hidroeléctricas, bombas de oleoductos y gasoductos, mercados de valores, etc.” De modo que la economía y seguridad son blancos secundarios inmediatos.

CIBERCRIMEN Y CIBERESPIONAJE

La ciberdelincuencia y el ciberespionaje son problemas latentes en mundo virtual. Los gobiernos y empresas internacionales cada vez se preocupan más por la seguridad de sus sistemas. Desafortunadamente, el crecimiento exponencial de los usuarios de internet, abre la puerta a un mayor número de “ciberdelitos”, haciendo imposible manejar la seguridad de cada una de las personas.

En este sentido Maroto (2009) afirma que “Actualmente se han generalizado los ataques en el ciberespacio. Así, India sufrió en el año 2008 problemas de infiltración en páginas web gubernamentales. Según sus analistas, el Consejo de Seguridad Nacional y el Ministerio de Asuntos Exteriores fueron violados por hackers chinos”. Ejemplos como este generan la desconfianza de gobiernos internacionales. Tras una cumbre de un día en Brasilia este mes de febrero, los negociadores de Brasil y Europa llegaron a un acuerdo para tender un cable de fibra óptica de \$ 185 millones que abarca las 3.476 millas entre Fortaleza y Lisboa. El cable será construido por un consorcio de empresas españolas y brasileñas. De acuerdo con Economist (2014) “según la presidente de Brasil, Dilma Rousseff, será "proteger la libertad." Ya no será el tráfico de Internet de América del Sur encaminado a través de Miami, donde los espías estadounidenses podrían verlo”.

En estos argumentos se encuentra un dilema ético importante. Por una parte tenemos a los gobiernos que aluden de cuidar a seguridad nacional por encima de la privacidad personal. Y por otra parte, la desconfianza internacional entre los países debido al espionaje que existe entre ellos. En cierto modo, ambos argumentos generan controversia ya que basados en una ética utilitarista (el mejor bien para el mayor número de personas), no hay forma de concluir si es bueno o malo el ciberespionaje.

CASO SNOWDEN.

Las acciones emprendidas por el ex analista y experto en informática Edward Snowden, ex empleado de la CIA y ex contratista de la NSA, han puesto en peligro el delicado balance de la seguridad internacional en diversos aspectos. Las acusaciones hechas

al gobierno norteamericano por espío de a personalidades de varios países y a millones de ciudadanos, ponen en cuestionamiento el actuar de diversas entidades internacional.

Son diferentes las formas de cuestionamiento que se la adjudican al actuar de Snowden. Por un parte tenemos la justificación ética. De acuerdo con Nusshold (2013) “Trabajar no sólo es producir sino transformar el mundo y transformarse a sí mismo. La posibilidad de discutir y repensar las reglas con las que trabajamos no sólo nos permitirá generar mejores resultados a nivel profesional sino también aportar al mundo aquello que está bien.” Quizá bajo este argumento Snowden justifica su actuar. Al saber del programa PRISM, sus principios éticos y valores personales lo llevaron irremediamente a revelar dicha información. Por otra parte, desde el punto de vista ético-profesional, Snowden actuó incorrectamente. Esto, desde la perspectiva de Núñez (2013) “No actuó apegado a los códigos deontológicos que amparan su profesión. Si ciertamente se pudiera alegar que Snowden actuó con libertad, por otra parte se afirmaría que no lo hizo con responsabilidad. Para ser un hombre libre, primero hay que ser responsable”.

A pesar de ser acusado de espionaje y traición Snowden justifica su actuación señalando los derechos de libertad de expresión y privacidad que los ciudadanos tienen. El espionaje de los servidores de Google, Facebook, Yahoo! y otras grandes empresas de tecnologías de la información y la comunicación, contradicen y agreden dichos estatutos. Se sabe que el gobierno de EUA promueve acciones controversiales desde una perspectiva de derecho internacional, derechos humanos, acuerdos y violación a la soberanía de otros Estados.

CONCLUSIÓN.

Son diversos los puntos tratados en este ensayo, asimismo las soluciones ante estas situaciones parte en diversos ámbitos. En primer lugar, la educación de los usuarios es fundamental en esta problemática. Si bien no es necesario ser unos expertos en el área, si es importante tener nociones y conceptos mínimos de seguridad, más que nada buenas costumbres cuando navegamos por la red. Por otra parte, la inversión que el gobierno representa para el desarrollo tecnológico juega un papel importante. Si bien son las empresas

las cuales desarrollan y administran dicha tecnología, el gobierno es el encargado de postular y sobre todo legislar sobre derechos digitales. La red es una extensión de nuestros quehaceres cotidianos y como cualquier otro medio de uso masivo, debe de ser regulado por las instancias correspondientes. Más allá del morbo de las filtraciones y el tema de la privacidad, Ligorria (2013) sugiere que “el punto central de la reflexión se mueve en torno al manejo de la información sensible”. En esta era digital en donde el poder gira en torno a datos, el problema de nuestra sociedad gira en torno al uso que le damos a la tecnología.

Bibliografía

Allard Young, C. (2013). Evolutions in Cyberlaw. *Signal*, 14.

Economist. (2014). Thieves in the Night. *Economist*, 84.

Ligorria, J. (7 de Marzo de 2013). *América economía*. Obtenido de Análisis Y Opinión:
<http://www.americaeconomia.com/analisis-opinion/el-caso-snowden-el-protagonismo-de-la-etica-y-el-crimen>

Matthews, O. (2015). Russia's Greatest Weapon May Be Its Hackers. *Newsweek*.

Núñez, R. (1 de Julio de 2013). *Diario Libre*. Obtenido de Diario Libre:
<http://www.diariolibre.com/opinion/el-caso-snowden-asunto-de-traicin-y-tica-BCDL390652>

Nusshold, P. (1 de Septiembre de 2013). *LA NACION*. Obtenido de Economía:
<http://www.lanacion.com.ar/1615843-el-dilema-etico-de-snowden>

Singer, P. W. (2015). Nowhere to Hide. *Popular Science*, 58-63.

Sorcher, S. (2015). Hacker Challenge Helps NSA Develop Future Cyberwarriors. *Christian Science Monitor*.

Yan, L. (2015). Is a Cyberwar Coming? *Beijing Review*.

Maroto, J. P. (2009). El ciberespionaje y la ciberseguridad. In *La violencia del siglo XXI. Nuevas dimensiones de la guerra* (pp. 45-76). Instituto Español de Estudios Estratégicos.

Medero, G. S. (2013). El ciberespionaje. *Derecom*, (13), 9.