

ETICES

Boletín de Bioética

Ética en las redes sociales



Boletín trimestral de Bioética
Facultad de Medicina y Departamento de Humanidades
Grupo de Investigación ETICES
Volumen 2, número 4
Octubre – Diciembre de 2010



UNIVERSIDAD CES

Un Compromiso con la Excelencia

Resolución del Ministerio de Educación Nacional No. 1371 del 22 de marzo de 2007

ISSN: 2145 - 3373

ETICES

Volumen 2, número 4: octubre - diciembre de 2010.

©Universidad CES

ISSN 2145-3373

Hechos todos los depósitos que exige la ley

Diagramación:

Oficina Proyección Corporativa - Universidad CES

ÉTICA EN LAS REDES SOCIALES

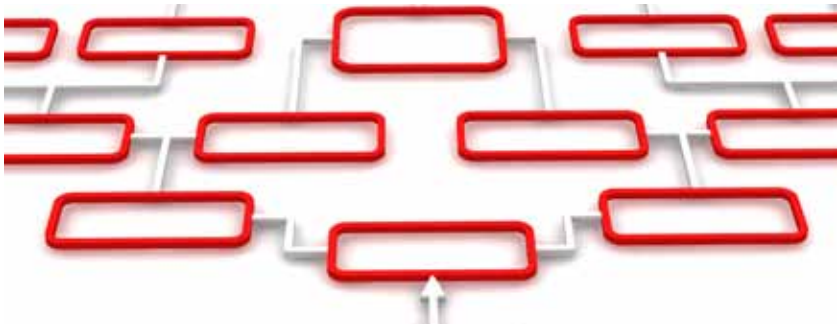
Diego Martín Buitrago Botero¹

Ricardo Lopera Jaramillo²

INTRODUCCIÓN

La conducta del hombre en sociedad tiene muchas características y muchas formas. En la actualidad con el avance de las tecnologías de la información y la comunicación (TIC's) el comportamiento del hombre ha explorado nuevos horizontes y nuevos caminos; uno de ellos es el mundo virtual y en especial el de las redes sociales³.

Según Patricia Wallace *"Internet no es una tecnología que nos haya sido impuesta y ante la cual solo podamos reaccionar de dos maneras: aceptarla tal cual es o evitarla por completo. De hecho, tenemos más poder para influir en este entorno que el que nunca hemos llegado a tener para influir en la televisión o en el teléfono, porque somos al mismo tiempo sus creadores, sus productores y sus usuarios"* ⁴. Estas palabras marcan un sendero de orientación de lo que es la internet y de lo que se puede hacer en ella.



1 Abogado. Especialista en Docencia Investigativa. Experto en Derecho Informático. Coordinador del Grupo de Estudios Jurídicos de la Facultad de Derecho de la Universidad CES. Editor de Revista Facultad de Derecho de la Universidad CES.

2 Ingeniero Informático de la Escuela de Ingeniería de Antioquia.

3 Forma de interacción social definida como servicio en línea enfocado a comunidades de personas que comparten intereses y actividades, o que están interesados en explorar los intereses y las actividades de otros, y que requiere el uso de software.

4 WALLACE, Patricia. La Psicología de Internet. Barcelona. Ediciones Paidós Ibérica S.A. 2001.

Se puede pensar en la internet como un mundo dentro del mundo. En la red se puede llevar a cabo todas las acciones también realizables en el mundo real. Así entonces se puede proponer la existencia de dos mundos paralelos: un mundo real o físico, el tradicional, el que siempre ha vivido el ser humano; y un mundo virtual, el que en "The Matrix"⁵ se denominaría el mundo de "la realidad virtual".

Las redes sociales, una práctica herramienta de entretenimiento y contacto entre amigos y seres queridos, son un fenómeno en evidente expansión en todo el mundo. Lo anterior ha venido ligado a un creciente fenómeno de comportamientos inadecuados tales como spam⁶, scam⁷, suplantación de identidad y muchos otros, contemplados dentro de la legislación en muchos países y cometidos por usuarios que se aprovechan de la vulnerabilidad de dichas redes.

Pero, más allá de cuestionar los fraudes electrónicos o los delitos informáticos, es necesario desentrañar el comportamiento y la conducta de los individuos. Saber por qué es tan atractivo para una persona ingresar a las redes sociales. ¿Cuál es su motivación?, ¿qué busca?, ¿por qué lo hace?, ¿cómo actúa?, ¿cuál es su forma de pensar?, ¿cómo es su mundo?, etc.

Un individuo puede tener comportamientos diferentes en el "mundo real" y en el "mundo virtual", lo que motiva este escrito para generar una pequeña orientación en el uso responsable de las TIC y en especial de la información y la intimidad en las redes sociales.

La aparición de las redes sociales acortó las distancias entre personas e hizo que el contacto entre ellas se mantuviera. Dichas redes se han ido ampliando, ya no solamente son útiles para encontrar personas: es posible además compartir fotos, música, jugar y otra cantidad de actividades programadas por terceros, gracias a plataformas de desarrollo de aplicaciones para Facebook, Sonico, hi5, Twitter y muchas más.

5 The Matrix. Warner Bross. Estados Unidos, 1999.

6 Se define SPAM a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en forma masiva.

7 Una variación del anterior en el que en dichos correos se prometen premios y dinero a cambio de proporcionar datos bancarios.

Toda esa cantidad de ventajas cautivaron a la mayoría de usuarios frecuentes de la internet en el mundo y en Colombia. Su crecimiento en el país se ha dado de manera exponencial y las personas, sin advertir las posibles consecuencias, al suscribirse, proporcionan información personal delicada que puede ser usada por delincuentes informáticos.

Se identifican dos causas por las cuales se cometen los delitos: una subjetiva que va ligada a la cultura y es el descuido sobre la propia información, y otra es objetiva, que va unida al factor técnico de seguridad por no tener en cuenta las medidas de protección tecnológica, como el uso adecuado de programas, firewalls, antivirus, entre otros.

Las leyes de Habeas Data⁸ y la llamada de "Delitos informáticos"⁹ (Leyes 1266 del 2008 y 1273 de 2009, respectivamente), establecen los procedimientos para la recolección, conservación y actualización de la información en las centrales de información (bancos de datos) y contemplan infracciones como la suplantación de identidades, la violación al derecho a la intimidad y la recopilación de información para su posterior venta. Quienes vulneren dicha normatividad son sujetos de investigaciones por presunta vulneración a los derechos a la intimidad y a la información consagrados en el artículo 15 de la Constitución Nacional. Las redes sociales, debido a un incipiente control sobre sus usuarios y programadores, son hoy la nueva plataforma de acción para aquellos que pretenden vulnerar dichos derechos fundamentales.

Las leyes mencionadas procuran proteger la confidencialidad, integridad y disponibilidad de los datos, estableciendo procedimientos para el manejo de la información contenida en las bases de datos, por un lado, e imponiendo penas a quienes las infrinjan, por el otro. Las redes sociales son entonces un elemento sensible dentro de su cumplimiento.



8 Ley 1266 de 2008, promulgada el 31 de diciembre de 2008.

9 Ley 1273 de 2009, promulgada el 5 de enero de 2009.

LA SEGURIDAD DE LA INFORMACIÓN

El concepto “seguridad de la información” envuelve dos términos fundamentales dentro de su definición: riesgos y vulnerabilidades, ambos muy estrechamente ligados. La explotación de la vulnerabilidad dentro de un sistema informático trae riesgos de toda índole, los cuales deben ser minimizados hasta llegar a un riesgo residual fácilmente detectable y controlable gracias a un adecuado plan de contingencia.

Al contener delicada información personal de sus usuarios, las redes sociales representan un escenario perfecto para los delincuentes informáticos gracias a las muchas vulnerabilidades, debidas principalmente a la ignorancia de quienes las utilizan. En la gran mayoría de los casos, los usuarios, sin medir consecuencias, ofrecen en sus perfiles datos tan importantes como su historia laboral, cargo actual, teléfonos, correos electrónicos y hasta dirección de residencia. Esos datos pueden ser obtenidos por terceros con malas intenciones mediante el desarrollo de aplicaciones sencillas o suplantando identidades. De igual forma, las cifras de spam, identidades suplantadas y otros fraudes electrónicos, han alcanzado niveles alarmantes en las redes sociales.



Las redes sociales

Las redes sociales suelen posibilitar que pluralidad y comunidad se conjuguen y allí quizás esté gran parte de toda la energía que le da vida a los grupos humanos que conforman esas redes. Las redes sociales dan al anónimo popularidad, al discriminado integración, al diferente igualdad, al malhumorado educación y así muchas cosas más. La fuerza del grupo permite sobre el individuo cambios que de otra manera podrían ser difíciles y genera nuevos vínculos afectivos y de negocios.

Básicamente, su funcionamiento comienza cuando una vez montado el soporte técnico, un grupo de iniciadores invitan a amigos y conocidos a formar parte de la red social, cada miembro nuevo puede traer consigo muchos nuevos miembros y el crecimiento de esa red social puede ser exponencial.

Las redes sociales han sido partícipes de un interesante fenómeno de masificación entre usuarios de internet, lo que ha hecho que el crecimiento de personas registradas sea inmenso y se haga prácticamente imposible para sus administradores, ejercer un control eficiente sobre la exposición de los datos de muchos de ellos.

Términos y condiciones en las redes sociales

Es un acuerdo de privacidad que debe ser aceptado por un usuario en cualquier red social al momento de hacer su registro, y contiene los derechos y deberes e incluye aspectos como: privacidad, información y contenido a compartir, seguridad, registro y seguridad de las cuentas, y responsabilidad en el manejo de la información. Aunque existen muchos otros aspectos que deberían ser tenidos en cuenta, pero a los que normalmente no se les presta atención.

Opciones de privacidad

Se trata de ciertas configuraciones que la red social permite llevar a cabo buscando la protección de los datos de todos los usuarios, e incluyen la visibilidad de la información y otros aspectos fundamentales para alguien preocupado por su confidencialidad.

Riesgos y vulnerabilidades de las redes sociales

Las vulnerabilidades son debilidades de un sistema informático, sea cual fuere, que representan un riesgo para sus usuarios y que permiten al atacante violar la confidencialidad, integridad y disponibilidad de la información almacenada. La mayoría de las veces dichos riesgos son medibles y mitigables llevándolos hasta un riesgo residual más fácil de controlar. Se afirma además que es imposible eliminar un riesgo, por eso se crean procedimientos para darlos a conocer y evitar al máximo su materialización.

Las vulnerabilidades pueden tener origen en alguno de los siguientes aspectos:

Espacios o elementos físicos: áreas de trabajo de los usuarios, ubicación de servidores, cableado, etc.

Los usuarios: las personas podrán revelar información importante muchas veces sin saberlo, incluso después de ser advertidas.

Claves de acceso: la complejidad de dichas combinaciones es esencial, si hay obviedad y poco cambio este elemento de seguridad se convertirá en una vulnerabilidad.

Mala programación: en algunos casos los desarrolladores no se enfocan en equipar su software de buena seguridad, esto crea huecos fácilmente aprovechables por personas malintencionadas.

Mala infraestructura: algunas redes no cuentan con equipos adecuados para evitar posibles ataques.

Integridad de datos: falta de copia o redundancia que puede causar pérdidas.

Las redes sociales, al ser un sistema informático como cualquier otro, cuentan con peligrosas vulnerabilidades debidas principalmente a sus mismos usuarios. Son ellos quienes están expuestos a diferentes amenazas y su falta de conocimiento muchas veces puede llevarlos a revelar información

personal, probablemente recolectada por quienes con seguridad no tienen las mejores intenciones.

Las redes sociales son, por lo tanto, un escenario propicio para quienes pretendan atentar contra la seguridad de la información de muchísimas personas; adicionalmente los usuarios, en la mayoría de casos, no son conscientes del riesgo incurrido al divulgar abiertamente información de amplio interés para los delincuentes, situación que ha ayudado a proliferar dichas prácticas.



La ética en redes sociales

Probablemente una discusión filosófica planteada desde hace tantos años pueda salirse del alcance de una investigación informática, así tenga un especial enfoque en las leyes relacionadas con dichos temas. Sin embargo, es necesario tener en cuenta algunas consideraciones pertinentes para quienes cuenten con conocimientos diferentes a los del común.

Son precisamente las habilidades de muchos desarrolladores de software -tema que la mayoría de las personas no domina-, aquellas a las que es necesario prestar especial atención debido a los muchos comportamientos legalmente válidos, pero desde un punto de vista ético bastante reprochables. El desarrollo de aplicaciones para las más populares redes sociales es un aspecto que no escapa de esa discusión donde se plantea el cumplimiento de la ley así la actitud sea éticamente incorrecta.

Es necesario considerar el desconocimiento de muchos aspectos de estas herramientas en la gran mayoría de usuarios de las redes sociales. Muchos de ellos, llevados por su curiosidad y deseo de estar en contacto con las personas a su alrededor, se registrarán en una de esas redes aceptando ciegamente los términos y condiciones relativos a dicho sitio web; a partir de ese momento comenzará una cadena de actitudes desafortunadas, tanto por parte del nuevo usuario, como de quienes quieran aprovecharse de su falta de conocimiento.

Las redes sociales cuentan con un perfil público donde el usuario podrá configurar su nivel de privacidad, de esa manera estará en sus manos la cantidad de información que éste quiera publicar a quienes puedan no tener ninguna relación directa con él. Su desconocimiento por parte de muchos usuarios de esas políticas es un aspecto común, no es raro buscar alguna persona en el directorio de la red y encontrar todos sus datos sin siquiera enviar una petición de amistad y sin que ésta sepa que sus datos están expuestos a todo el público.

Mucho se ha argumentado acerca de los límites de la ley y la aplicación de la ética en su cumplimiento. Cuando un programador saca provecho de las ventajas que tiene sobre todos aquellos sin conocimientos informáticos avanzados, no está violando ninguna ley, más aun cuando esa persona ha aceptado poner sus datos a disposición de un tercero, así sea de manera involuntaria; sin embargo surge la pregunta ¿está siendo ese programador ético? La cuestión se sale de los alcances de la legislación y depende única y exclusivamente de la concepción del bien y el mal de cada persona.



Un ejemplo práctico es el del peatón cruzando una peligrosa avenida sin usar el puente peatonal ubicado a escasos metros del lugar. La ley podrá proteger a aquel que lo atropelle bajo el argumento de la irresponsabilidad del peatón al no cruzar por el puente. Hipotéticamente, podría aparecer quien quiera sacar provecho de la situación arrollando a su enemigo cuando se encuentre en una situación como la descrita. En teoría esa persona estará protegida por la ley pero ciertamente su actuar no fue ético teniendo en cuenta la intencionalidad a la hora de asesinar a su enemigo.

Es necesario recalcar que no es el instrumento, en este caso representado por las redes sociales, la amenaza para la seguridad o confidencialidad de las personas y sus datos. Son los usuarios quienes pueden matizar dicho instrumento convirtiéndolo en una herramienta útil y de entretenimiento o en una amenaza para la mayoría de la población sin mucho interés en temas informáticos. Por eso la aplicación de la ética y en general la educación sobre buenas costumbres se convierte en un elemento trascendental a la hora de poner al alcance de la población algo tan poderoso y universal como las redes sociales.

No son las redes sociales una herramienta creada para violar la ley y cometer toda clase de delitos, al contrario, son una útil y poderosa interfaz de interacción y entretenimiento que lamentablemente algunos de sus usuarios han ido convirtiendo en un espacio donde es necesario ser cauteloso con datos personales. El actuar de los usuarios se sale del alcance de los administradores de una red social, pues se hace prácticamente imposible controlar a cada una de las millones de personas con cuentas activas.

El desconocimiento entre los usuarios colombianos de los riesgos relacionados con las redes sociales, así como de todas las oportunidades que éstas brindan para proteger su privacidad, es un aspecto preocupante que debe ser atacado para evitar el incremento de hechos ilegales de los que ellos mismos son víctimas.

Se hace estrictamente necesario un mayor enfoque de la ética en la educación del país, las personas no deben seguir pensando que las limitaciones de la ley son un elemento idóneo para aprovecharse de ella y tranquilamente declarar su inocencia pese a haber tenido intenciones negativas.

Bibliografía

-BORGHELLO, CRISTIAN, *Seguridad de la información. SPAM*, (n.d./Año), Fuente electrónica [en línea], Segu Info, <http://www.segu-info.com.ar/malware/spam.htm>, (Visitado 15 de septiembre de 2009)

- BORGHELLO, CRISTIAN, *Seguridad de la información. PHISHING*, (n.d./Año), Fuente electrónica [en línea], Segu Info, <http://www.segu-info.com.ar/malware/phishing.htm>, (Visitado 15 de septiembre de 2009)

- PARODY, GINA. *Ley de Habeas Data*, (n.d./Año), Fuente electrónica [en línea], <http://www.ginaparody.com/leyes/ley-habeas-data>, (Visitado 13 de septiembre de 2009)

Ley 1266 de 2008 promulgada por el gobierno nacional del día 31 de diciembre de 2008

Ley 1273 de 2009 promulgada por el gobierno nacional el día 5 de enero de 2009

- ZAMORA, MARCELO. *Redes Sociales en Internet*, (2006, 11, 14), Fuente electrónica [en línea], Maestros del Web, <http://www.maestrosdelweb.com/editorial/redessociales/>, (Visitado 20 de septiembre de 2009)

- CAVELIER, ANDRÉS, *Se dispara el uso de redes sociales en Brasil y América latina*, (2008, 11, 24), Fuente electrónica [en línea], Andrés Cavelier, <http://andrescavelier.com/2008/11/24/noviembre-24-se-dispara-uso-de-redes-sociales-en-brasil-y-america-latina/> (Visitado 17 de septiembre de 2009)

- CATTIVONE. Aumentan los casos de robo de identidad en redes sociales, (2009, 07, 05, GMT 18:26), Fuente electrónica [en línea], Globedia, <http://co.globedia.com/aumentan-casos-robo-identidad-redes-sociales> (Visitado 15 de septiembre de 2009)

- THORBORG, MARTIN. El SPAM se adueña de las redes sociales (2009, 02), Fuente electrónica [en línea], Tecnonews, <http://www.noticias.com/opinion/spam-se-aduena-redes-sociales-d08.html> (Visitado 15 de septiembre de 2009)

- WALLACE, Patricia. *La Psicología de Internet*. Barcelona. Ediciones Paidós Ibérica S.A. 2001

Envíe sus comentarios y sugerencias a través de las siguientes direcciones:

dbuitrago@ces.edu.co

loperaja@gmail.com

fochoa@ces.edu.co

jwosorio@ces.edu.co

jtaborda@ces.edu.co

Integrantes del Grupo de Investigación ETICES:

Francisco Luis Ochoa J. Médico. Magíster en Epidemiología.

José María Maya Mejía. Médico. Magíster en Salud pública.

Jhon Mauricio Taborda A. Filósofo. Magíster en Filosofía con énfasis en Ética.

Jhon Wilson Osorio. Historiador. Especialista en Educación.

Santiago Henao. Médico Veterinario. Candidato a Doctor en Bioética.

Jorge Humberto Molina O. Historiador. Magíster en Hermenéutica Literaria.

Mario Fernando Arenas S. Filósofo. Magíster en Hermenéutica Literaria.

Luis Fernando Toro P. Médico. Magíster en Epidemiología.

Stella Navarro. Médica. Intensivista. Magíster en Bioética.

Imágenes tomadas de:

www.ingimage.com

ETICES

Boletín de Bioética

Ética en las redes sociales



Boletín trimestral de Bioética
Facultad de Medicina y Departamento de Humanidades
Grupo de Investigación ETICES
Volumen 2, número 4
Octubre – Diciembre de 2010

Rede
EDITORIAL
CES



UNIVERSIDAD CES

Un Compromiso con la Excelencia

Resolución del Ministerio de Educación Nacional No. 1371 del 22 de marzo de 2007

ISSN: 2145 - 3373