REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO (SEGUNDA ÉPOCA).
FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES DE DERECHO E INFORMÁTICA.
ISSN 2530-4496 – AÑO 1, N° 1, 2016, PÁGS. 91-96

Comentario al informe de Kaspersky Lab de 22 de abril de 2016

Comments on Kaspersky Lab Report of April 22, 2016

JUAN LUIS HERRERA GARCÍA

RESUMEN

El presente trabajo se basa en los resultados de un estudio realizado sobre los riesgos en el uso de las Nuevas Tecnologías de la Información, que evidencia el nivel de vulnerabilidad en que se encuentran los usuarios, situación que tiende a agravarse con el uso creciente de dispositivos en línea y el incremento de la interacción en el internet. La tecnología brinda muchos beneficios a las personas, pero también tiene un lado oscuro, lo que hace necesario su exposición ante la sociedad, fomentando el análisis y discusión de los peligros que conlleva la vida en línea que hoy disfrutamos.

Palabras clave: vulnerabilidad en línea, riesgo en internet, datos sensibles, ciberseguridad.

ABSTRACT

This work is based on the results of a study on the risks in the use of new information technologies. It shows the user´s vulnerability, a situation that tends to get worse because the growing use of online devices and internet interaction. The technology gives many benefits to people, but has a dark side too, making it necessary and useful expose the situation to society, promoting the analysis and discussion about the dangers that online life represents.

KEYWORDS

online vulnerability, internet risks, private data, cibersecurity.

I. ANTECEDENTE: EL INFORME DE KASPERSKY LAB

En 22 de abril de 2016 Kaspersky Lab[155] publicó una nota de prensa titulada "*Compartir datos online puede acabar con carreras profesionales*"[156], basada en los resultados de un estudio realizado en forma conjunta con la empresa B2B International[157], el cual fue denominado *"CONSUMER SECURITY RISK SURVEY, from scared to aware: digital lives in 2015"*[158].

La nota de prensa enfoca los resultados del estudio en la actividad profesional de los encuestados, afirmando que "*muchos usuarios continúan compartiendo información privada de manera imprudente a través de internet, a pesar de que esta información podría haberles costado el puesto de trabajo o afectado su relación de pareja"*.

Se basó en una encuesta en línea realizada a 12,355 personas mayores de 16 años, en 26 países de América, Europa, África y Asia. De los resultados puede resaltarse que los usuarios de internet interactúan con diversidad de dispositivos, los cuales se mantienen en línea y que contienen mucha información personal importante; la conexión inalámbrica es fundamental para estar en línea y la mayor actividad se da en redes sociales, correo electrónico, compras en línea, noticias, transacciones bancarias y entretenimiento.

El estudio concluye que el uso de dispositivos conectados a internet y las actividades en línea, se ha convertido en parte integral de la vida de los usuarios a nivel mundial, pero que existe una

[155] *Empresa especialista en antivirus y software de seguridad con presencia a nivel mundial.*

[156] *Sitio web: Sala de Prensa Kaspersky Lab España, "disponible en sitio web: http://newsroom.kaspersky.eu/es/noticias/detalle/article/compartir-datos-online-puede-acabar-con-carreras-profesionales (Fecha de consulta 20 de abril de 2016)"*

[157] *Empresa consultora especializada en estudios de mercado.*

[158] *Sitio web: Press Center Kaspersky Lab, "disponible en sitio web:https://press.kaspersky.com/files/2015/08/Kaspersky_Lab_Consumer_Security_Risks_Survey_2015_ENG.pdf (Fecha de consulta 20 de abril de 2016)"*

contradicción entre la conciencia de los riesgos que esto conlleva y la poca actividad encaminada a gestionarlos, subestimándose la vulnerabilidad en que se encuentran, por la falta de protección adecuada sobre los dispositivos y la información que contienen.

Kaspersky Lab sugiere que adicional a los mecanismos y herramientas de seguridad informática, como los que ellos comercializan, se debe proveer a los usuarios educación, soporte, información y advertencias, para que comprendan el valor que puede tener su información en línea para otros, incluyendo los criminales, resaltando la responsabilidad y riesgos que esto implica. Agrega que se debe empoderar a los usuarios, para que tomen decisiones informadas sobre su propia seguridad y la de otras personas que les preocupan.

Investigaciones como la realizada por Kaspersky Lab, revelan la dinámica imparable del uso de las Nuevas Tecnologías de la Información, que ha llevado la interacción social a escalas sin precedentes, donde la información transita a toda hora y en muchas direcciones, facilitando el acceso a muchos servicios, sin embargo, han surgido también nuevos problemas, situaciones imprevistas, que requieren abordajes diferentes, auxiliándose en muchos casos de otras disciplinas.

Las nuevas vías de comunicación, los dispositivos informáticos y la información misma, están al alcance de cualquier persona, lo que implica que también la criminalidad se sirve de la tecnología, como herramienta muy eficiente para ladrones, estafadores, acosadores, terroristas y una extensa lista de nuevas modalidades delincuenciales.

II. EL DERECHO Y EL DELITO INFORMÁTICO

Las acciones delictivas con el uso de las Nuevas Tecnologías de la Información, han sido objeto de un tratamiento jurídico, generando en el Derecho, una nueva visión del crimen, que en la actualidad se encuentra en discusión y revisión constante. No es objeto del presente comentario, abordar en profundidad el Delito Informático, pero si es oportuno señalar que una dificultad importante es la tipificación, ya que la creación de tipos penales informáticos afronta retos difíciles, de los cuales se pueden resaltar la velocidad con que surgen nuevas conductas criminales y la superación de la territorialidad en el alcance de la norma.

Existen en la actualidad, esfuerzos importantes en legislación sobre delitos informáticos, sobre todo luego del Convenio sobre la Ciberdelincuencia[159], celebrado en Budapest en el año 2001, primer tratado internacional que establece delitos cometidos a través de medios informáticos, el que ha servido de base para la inclusión de normativa especializada en muchos países, incluyendo varios de América Latina.

La tipificación del delito informático[160], es un proceso en trámite, algo que aún está en discusión y probablemente dure un buen tiempo, situación que haría pensar que no puede abordarse el problema, que la ausencia de acciones tipificadas, impide aplicar acciones correctivas, sin embargo, el control puede aplicarse de forma preventiva, enfocando las baterías en una idea atípica del fenómeno, entendiéndolo como una conducta criminógena en la que intervienen las Nuevas Tecnologías de la Información.

---

[159] Sitio web: Consejo de Europa, Convenio sobre cibercrimen, "disponible en el sitio web: http:// http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (Fecha de consulta 20 de abril de 2016)"

[160] Capítulo de libro: TELLEZ VALDEZ, J. "Derecho Informático", México: UNAM, 1987.

III. ALCANCE PREVENTIVO DEL DERECHO INFORMATICO

La prevención del delito informático es deseable, sin embargo, es mi intención en el presente escrito, señalar la posibilidad de un efecto adverso para las propias Tecnologías de la Información, causado por la poca comprensión de aspectos muy peculiares de su dinámica y naturaleza, sin los que no hubiese sido posible su auge y que sean hoy, parte integral de nuestra vida.

La sugerencia de Kaspersky Lab, en un análisis superficial, puede calificarse como un mero ejercicio de mercadeo, donde resaltan sus productos y servicios de seguridad informática para el mundo en línea que hoy vivimos, sin embargo, puede y debe hacerse una lectura más profunda, donde es posible encontrar elementos valiosos, que ayudaran a garantizar un entendimiento apropiado desde lo jurídico hacia lo informático, requisito fundamental para un proceso de tipificación correcto en materia de delitos informáticos.

La creación de soluciones tecnológicas, muy difícilmente, se acompaña de la idea de prevención. Es la toma de caminos diferentes, el abandono de los paradigmas, el arriesgarse a lo desconocido, lo que ha proveído a la humanidad de muchos avances, donde la apertura, entendida como un panorama sin límites, ha permitido que surjan las más diversas propuestas, las que una vez concebidas y probadas sus bondades, no tendría sentido, ni sería factible, pretender limitarlas con la intención de evitar que los usuarios se causen daños, sean estos con o sin intención.

Relacionado a lo anterior, está la libertad que existe en las carreteras de la información, tanto de tránsito como de expresión, donde los permisos y las autorizaciones -que si existen-, poco o nada tienen que ver con entes administrativos estatales o de tipo jurisdiccional, aspecto que también ha sido fundamental para el crecimiento de lo que hoy está conectado a internet y que abarca personas y cosas.

El inventar dispositivos de todo tipo con conexión a internet, crear redes sociales, portales y servicios en línea abiertos a cualquier persona y de cualquier tema, y la intercomunicación que existente entre todos estos productos, surgió y sigue desarrollándose en una mal llamada “tierra de nadie”, lo cual no es del todo cierto, pero que no ha requerido de normativa o regulación específica para ser lo que hoy es.

La velocidad de los cambios tecnológicos y sus efectos sociales, superan por mucho, la adaptación que el Derecho puede lograr ante dicha realidad, situación que puede generar una especie de “ansiedad” por la falta de una efectiva tutela jurídica, lo que puede derivar en el desarrollo de normativa excesivamente preventiva, demasiado cautelosa y desconfiada ante los riesgos y peligros que representan las Nuevas Tecnologías de la Información para los usuarios, situación que ya se ha dado en otras ramas del Derecho, tal es el caso del principio precautorio en el Derecho Ambiental, el que adopta una postura protectora ante sospechas fundadas, de que ciertos productos o tecnologías crean un riesgo grave, sin que sea necesaria una prueba científica, concepto que, al relacionarlo con lo expuesto por Kaspersky Lab, parece encuadrar perfectamente.

La regulación sobre delitos informáticos, tiene una relación importante con los riesgos, peligros y daños derivados de la interacción en línea, pero no abarcan todo el fenómeno, hay una proporción de responsabilidad individual por parte de los usuarios, más cercana con la educación y alejada de la facultad sancionadora del Estado. El delito informático representa muchos retos, la utilización de tipos penales parece no ser suficiente, pero teniendo presente que hace referencia a una conducta, la cual realizan las personas, es posible evitar orientar la normativa en las Tecnologías de la Información con un enfoque restrictivo, que podría fácilmente limitar su dinámica.

Las Nuevas Tecnologías de la Información, son cosas, no debe olvidarse que la tipificación, sea correctiva o preventiva se enfoca en las acciones realizadas por individuos. El alcance efectivo de un

bien jurídico, requiere del Derecho un entendimiento y respeto por la naturaleza del fenómeno que pretende abordar, una correcta lectura desde lo jurídico hacia la informática, de lo contrario, y como suele suceder, el exceso de protección puede generar, irónicamente, daños importantes y en muchas ocasiones irreparables.

SOBRE EL AUTOR

JUAN LUIS HERRERA GARCÍA es Licenciado en Sistemas de Información y en Ciencias Jurídicas y Sociales por la Universidad Francisco Marroquín, Guatemala.

Se desempeña como docente de las Universidades Francisco Marroquín y de la Universidad Galileo, ambas en ciudad de Guatemala, Guatemala.

Su correo electrónico es: jluishg@gmail.com

Este trabajo fue recibido el 19 de junio y aprobado el 15 de julio de 2016.