Colaboran
Rodrigo Iglesias
Manuel de Cristobal
Paulina Casares Subia
Marcelo Campetella
Franco Vergara
Entrevista:
Humberto Carrasco Blanc
Secciones
Inés Tornabene
Jorge G. Obregón
Fabián Descalzo

Revista Digital
ElDerechoInformatico.com

El Derecho en tiempos de SELFIES

Modelo de Tapa
Valeria MENGO

Abril Nro 20

PRIMER ENCUENTRO ELDERECHOINFORMATICO.COM URUGUAY

Nuevas tecnologías
Nuevos paradigmas jurídicos

21 de mayo de 2015 - 8:30 hs.
Sala de Actos del Ministerio de Relaciones Exteriores
Colonia 1206 esq. Cuareim

Los nuevos paradigmas de la transparencia
Análisis del estado de situación del derecho y las telecomunicaciones
Impacto de las nuevas tecnologías en los datos de salud
Seguridad informática en los tiempos modernos

Conferencia de apertura: El derecho informático y sus desafíos en la actualidad
Charla: Desafíos procesales en el combate al cibercrimen
Conferencia de cierre: Democracia y gobernanza en clave de datos abiertos. Lecciones aprendidas y desafíos futuros

Taller: La actividad notarial en la era digital

Por más información visite http://corresponsales-uy.wix.com/jornadas2015

ORGANIZA: El Derecho Informático .com

AUSPICIAN: AALCC · MIGLIORISI abogados .com · microjuris.com · Suma Importadores · IJ Editores

APOYA: Asociación de Escribanos del Uruguay

Dirección

Abog. Guillermo M. Zamora

Secciiones - Responsables

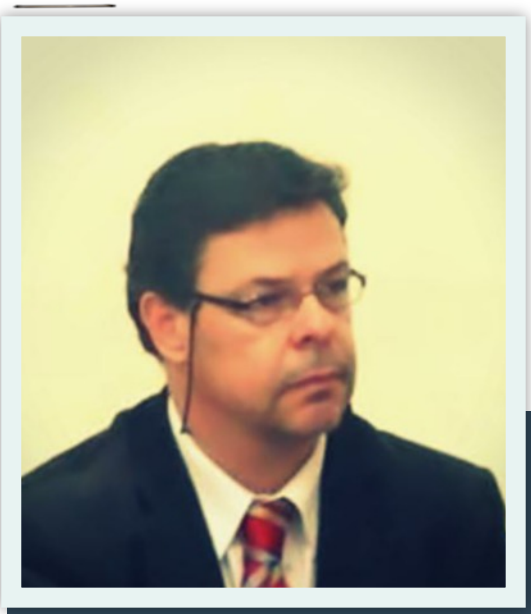
Emprendedores y StartUp - Abog. Jorge L Garcia Obregón
Privacidad y Datos Personales - Abog. Inés Rornabene
Governance y Compliance - Ing. Fabían Descalzo

Ilustración de Tapa

Modelo: Ana Valeria Mengo

Colaboran:

Entrevista



EDITORIAL

Como todo en la vida, cuando uno hace algo debe hacerlo por las razones correctas, escribir, hacer dieta, insultar, halagar, dar vida o incluso quitarla, todo tiene un sentido lógico si se hace por las razones correctas.

Así lo entendimos desde la Red hace ya unos 4 años y 20 números atrás, hacer una via de comunicación, un espacio donde todos pudieran decir o expresar lo que pensaban sobre determinados temas, no voy a negar que pudo haber artículos que no gustaron, pasa hasta en las mejores familias, pero lo importante fue que tuvieron su lugar, no me enorgullezco de que la Revista no tenga comité académico, pero si que cualquiera con ganas de decir algo lo pueda hacer, creanme que todos y cada uno de los autores han sido sus peores y más exigentes evaluadores. Ahora bien, que es hacer las cosas por las razones correctas, es una respuesta con bastantes sentidos, por un lado lo correcto será lo que uno considere, por el otro será lo que nos haga feliz, o nos ilumene en lo que querramos conseguir, no es una respuesta única ni indiscutible, es sólo una respuesta dentro de cada uno de nosotros.

En Mayo la Red capítulo Uruguay,organiza su primer evento fuera de Argentna, y eso es un fundamento y una razón correcta, dentro del evento haremos donaciones a dos entidades, vamos a conocernos cara a cara, desvirtualizar las charlas y las risas, y todas estas cosas son sin dudar razones correctas,

La Red llegó a su edición N° 20, ni es poco, ni es suficiente, es lo que tiene que ser, y estoy casi seguro que sea cual fuere la razón por la que se llegó a ese número es la correcta, porque estamos acá, escribiendo y leyendo, charlando y compartiendo, ¿no les parece?.-

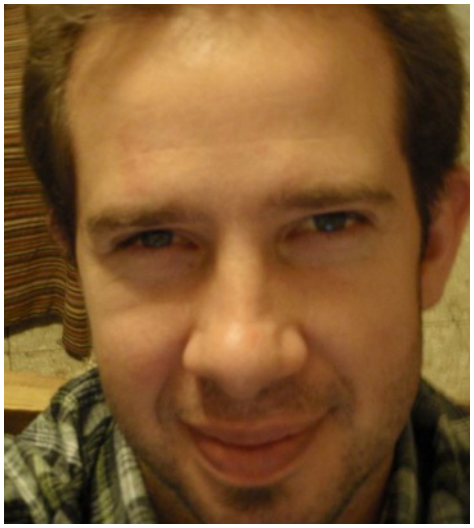
Telecomunicaciones y privacidad.

AUTOR: Rodrigo Sebastián Iglesias.

Abogado, Técnico en Electrónica.
Investigador UBACyT, miembro del HackLab Barracas.

Resumen.

El presente ensayo tiene como objetivo fundamental demostrar los problemas de seguridad en los cuales estamos sometidos desde tiempos previos a Snowden y que él nos informo de su existencia, como resulta mucho más procedente creer que no solo las personas pueden realizar una vigilancia, sino que son los Estados, Empresas y usuarios (en grupos) los que generan esta vigilancia. Para ello empleamos un método de "romper para reparar", en pocas palabras como violar nuestra privacidad, generar una forma de vigilancia, para luego incrementar nuestros niveles de seguridad, con el fin de intentar que esa vigilancia sea nula o mucho más complicada de realizar, este no es un enfoque técnico sino orientado a Abogados.



Introducción.

Corría el año 1955 y la empresa AT&T publica un artículo donde se explicaba como se trazan las comunicaciones telefónicas, sin publicar la frecuencia que utilizaban los tonos, esto fue develado en 1964, con estas dos indicaciones se dejo abierta la puerta a que cualquier persona con conocimientos de electrónica pudiera comenzar a utilizar el servicio de una forma "distinta".

Este es el comienzo de una nueva forma de pensar la forma de utilizar las cosas, y fue el inicio del pensamiento Hacker, gracias a Josef Carl Engressia (Joybubbles) y John Draper (Capitán Crunch) modificaron un silvato y lo hicieron sonar a 2600hz, con ello ingresaban en el sistema de telefonía y les permitía realizar cualquier llamada telefónica de forma gratuita. Con esto comenzó a darse forma la bluebox, y el pensamiento hacker que hoy conocemos como tal, es decir la utilización de una cosa con un fin distinto.

En los días en los que vivimos Internet nos lleva a pensar muchas veces de la misma forma en que lo hicieron estas personas, para usar el concepto de "romper para reparar".

¿Que podemos romper?.

En la actualidad, Internet es una herramienta que se basa en dos protocolos, que ya todos conocemos ellos son TCP/IP el principal problema es el protocolo TCP que tiene errores desde su creación y por ello nuestras comunicaciones son más delicadas en cuanto a la privacidad y la vigilancia que nos pueden producir, tanto Estados, Empresas o Usuarios. Es necesario entender "que" podemos (y como) romper en materia de seguridad en nuestras comunicaciones para luego incrementar los niveles de nuestra propia seguridad y con ello, nuestra privacidad.

Hoy con ver simples vídeos en Internet comprobamos que el conocimiento se encuentra a disposición de quien tenga la intensión de abrir cualquier sistema, conocer de programación[1], de realizar un test de penetración sobre su máquina (o su modem), y como incrementar los niveles de seguridad[2]. Claro que también puede ser utilizado en forma deshonesta y realizar dichos controles sobre objetivos no tan santos, y realizar delitos ya tipificados por el Código Penal desde el año 2008, es por esto que sostenemos que este trabajo es a nivel educativo y a los únicos fines de nuestra investigación, la propia seguridad

[1] https://rubymonk.com/ como aprender a programar Ruby, de forma autodidacta.

[2] http://www.jsitech.com/linux/tips-para-mejorar-la-seguridad-en-los-servidores-linux/ aunque es sobre servidores, esta información es igual de buena para un uso normal.

de nuestras comunicaciones a la hora de tener una conversación privada con nuestros clientes.

Vamos a intentar vulnerar TODO, si todo lo que se nos ocurra, con los fines de demostrar que la vigilancia es algo innecesario y contrario al concepto de seguridad, que esta seguridad debe ser el objetivo del Estado, y que la vigilancia trae consecuencias negativas.

¿Que vamos a utilizar?.

Software, simples programas de computadora, de código abierto, de distribución gratuita y desarrollados por la misma comunidad que todos integramos. Algunos de ellos son: Kali Linux, Wireshark, Backtrack, Kali, etc. Y para aumentar nuestra privacidad, y por tanto disminuir la vigilancia y así aumentar nuestra seguridad: Linux, Thunderbird, TOR, Ciboulette, Riseup, Enigmail, etc.

Comencemos!!!.

Parte 1.

Desde 1998, ingresamos al mundo de Internet con un acceso bastante precario y fue mejorando a lo largo de los años, pero la gran cantidad de usuarios lo hacían con Sistemas Operativos privativos y esos sistemas siempre fueron (y de forma creciente) inseguros, muchos recuerdan los virus como Miguel Ángel y más en nuestros tiempos LOVE. Esto es culpa del mismo SO que se encuentra diseñado de forma deficiente, y es necesario colocar un antivirus, para no correr estos riesgos (perder información, ese era el riesgo). Hoy muchos usuarios no aprendieron de estos problemas y continúan utilizando estos sistemas, dado que los SO seguros se demoraron mucho en generar un entorno gráfico “amigable” para el usuario doméstico y esto fue, es y será la mayor deuda del software libre.

Ya en el año 2001 los Estados entendieron que los Delitos Informáticos comenzaban a ser un problema y por ello se realizó el Tratado de Cibercrimen (o convenio de Budapest) donde se realizó un marco para que los Estados adecuen su normativa a este tipo de delitos.

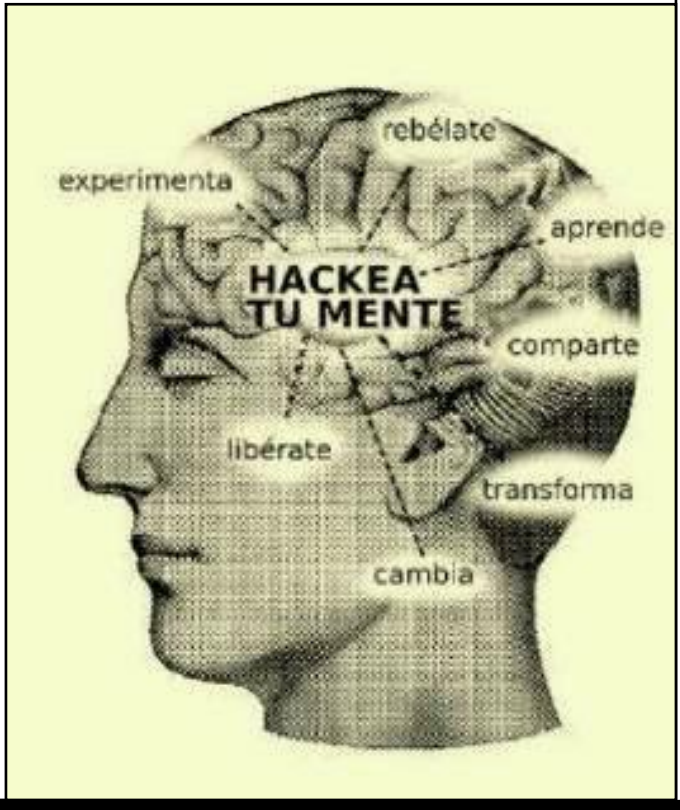
Argentina tuvo proyectos de ley en este sentido desde 1996, pero no fue hasta 2008 que entró en vigencia la ley de delitos informáticos, que aun continúa vigente, tipificando muchas de las conductas delictivas.

Es claro que la ley de protección de datos personales (Ley 25326), el artículo 43 de la Constitución Nacional, muchas de ellas con muy buenas intenciones y malos resultados, faltos de personal, presupuesto o simplemente sin un funcionamiento claro a la hora de investigar al propio Estado.

Con esto nos vemos obligados a investigar las telecomunicaciones y sabiendo que el Derecho (más precisamente las leyes y sus aplicaciones) vienen en desventaja en relación al tiempo en el cual se aplica. Entonces son los propios usuarios quienes deben incrementar su seguridad y su privacidad en términos de telecomunicaciones en la Internet.

Parte 2.

Como anteriormente señalamos, los SO libres son tardíos en cuanto a una interfaz gráfica amigable y por ello, en los inicios son mucho más complicados de utilizar por el usuario promedio, en cuanto ese entorno gráfico se volvió de uso sencillo, estos se encuentran en un crecimiento exponencial en cuanto a cantidad de usuarios y mucho tuvo que ver el uso de celulares con SO simples y si bien no son libres, estos utilizaron un entorno gráfico muy similar a distintas distribuciones de Linux, dando lugar a que



miles de usuarios pasen a la utilización de SO libres, incluso en países se está utilizando dicho software en el Estado (generando ahorro en grandes sumas por licencias y aumentando la seguridad de su país), pero ese es un análisis para otro trabajo. Comencemos a romper.

En la actualidad, nos es impensable que una computadora no este conectada a Internet, el envío de mail, la conexión a redes sociales, transferencias bancarias, búsquedas de información, ver vídeos, etc. Pero, ¿esas cosas que habitualmente hacemos son seguras, privadas y confidenciales?.

¿Como pueden ingresar a un modem y conectarse a una red wifi con claves de seguridad?.

La respuesta es simple, depende de si la conexción es WEP, WPA o WPA2. Pero de todas formas todas son vulnerables (depende de la clave que ingreso el usuario y de la capacidad que tiene quien quiere ingresar).

Claves WEP: si bien este tipo de cifrado tiene una seguridad “igual a la de una red cableada” fue fácilmente vulnerada y ya no cuenta con el apoyo de la wifi alliance desde 2004, aun en Argentina se continúa con este sistema en todos los usuarios de empresas como Speedy.

Claves WPA: fue creado para reemplazar WEP, incluyendo una mayor seguridad en las comunicaciones de este tipo, utiliza un principio de autenticación mediante un servidor donde se guardan las credenciales y contraseñas, para que no se utilice el servidor se realiza mediante una clave precompartida, este sistema es vulnerable al realizar un ataque de recupero, reinyectando tráfico, esto es posible dado que diversos canales utilizan el modo QoS, pero también es posible utilizarlo por fuera del modo QoS. También se encuentra disponible en todos los ISP que ofrecen el servicio de Wifi en Argentina.

Claves WPA2: Claramente se utiliza este sistema para corregir los problemas de seguridad originados en sus antecesores. Tanto la versión 1 de WPA, como la denominada versión 2, se basan en la transmisión de las autenticaciones soportadas en el elemento de información correspondiente. En el caso de WPA 1, en el tag propietario de Microsoft, y en el caso de WPA2 en el tag estándar 802.11i RSN.

Durante el intercambio de información en el proceso de conexión RSN, si el cliente no soporta las autenticaciones que especifica el AP (access point, punto de acceso), será desconectado pudiendo sufrir de esta manera un ataque DoS específico a WPA.

Además, también existe la posibilidad de capturar el 4-way handshake que se intercambia durante el proceso de autenticación en una red con seguridad robusta. Las claves PSK (precompartidas) son vulnerables a ataques de diccionario (no así las empresariales, ya que el servidor RADIUS generará de manera aleatoria dichas claves), existen proyectos libres que utilizan GPU con lenguajes específicos como CUDA (NVIDIA) y Stream (AMD) para realizar ataques de fuerza bruta hasta cien veces más rápido que con computadoras ordinarias.

Uno puede pensar, que si se conectan a nuestra red Wifi, el único problema que puede existir es que nuestro servicio funcione de forma mas “lenta” que si bien no es un gran problema (para algunas personas) el principal inconveniente es sufrir un proceso legal por algún delito informático realizado desde el wifi en cuestión, pero salvando este inconveniente no existe un problema “significativo” para el propietario del servicio. No así para las empresas que ofrecen este servicio, dado que además de perder un potencial cliente, ven como un abonado tiene un consumo elevado de servicio y el mismo sufre una depreciación en cuanto a cantidad de clientes conectados a un mismo nodo, en definitiva complicaría mucho más la reducción de la cantidad de tráfico que nos va a “recortar” nuestro ISP, que un ataque real desde nuestro equipo.

Este es uno de los pocos casos en los cuales el SO no tiene ninguna incumbencia, dado que el ataque se realiza sobre el Modem o Router[1], pero si algunas Empresas tienen defectos de fabrica y los accesos son mucho más accesibles de distintas formas, claro que ningún ISP cambia

[1] Aunque puede utilizarse https://openwrt.org/ para cambiar el firmware de nuestro modem y con esto modificar algunos patrones.

librería | hammurabi

Talcahuano 440 - C1013AAI
CABA - Argentina
Tel.: (54-11) 4371-8179
info@libreriahammurabi.com.ar

en preparación

Colección «elderechoinformático.com»

11 volúmenes

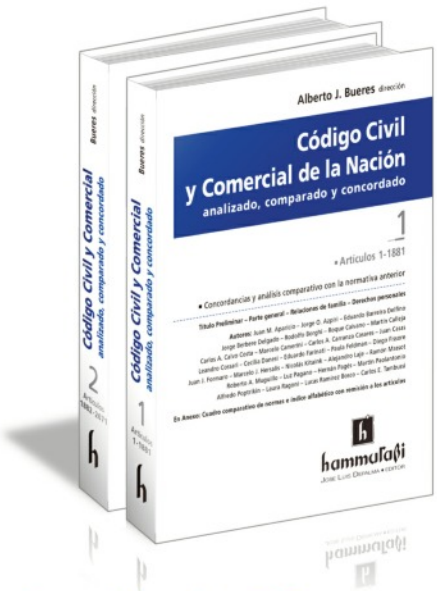
Guillermo M. Zamora dirección

1 — La prueba informática
2 — Negocios jurídicos en tiempos de Internet
3 — Delitos informáticos
4 — Propiedad intelectual en la era de la información
5 — Gobierno digital y gobierno abierto
6 — Datos personales, su protección
7 — ODR, Resolución de Disputas Online
8 — Firma digital
9 — Régimen jurídico de nombres de dominio
10 — Teletrabajo
11 — Aspectos jurídicos del *cloud computing*

Novedad

Código Civil y Comercial de la Nación

analizado, comparado y concordado



Alberto J. Bueres dirección

2 tomos | Artículos 1 - 2671

Análisis complementario de las principales normas que inciden en el «Derecho del trabajo» al cuidado de Juan J. Formaro

Contiene: Cuadro comparativo de normas. Indice alfabético de voces

• **Tomo 1. Arts. 1 a 1429.** **Autores:** Juan M. Aparicio – Jorge O. Azpiri – Eduardo Barreira Delfino – Jorge Berbere Delgado – Rodolfo Borghi – Martín Calleja – Marcelo Camerini – Carlos A. Carranza Casares – Rubén Compagnucci de Caso – Leandro Cossari – Cecilia Danesi – Paula Feldman – Diego Fissore – Juan J. Formaro – Marcelo J. Hersalis – Germán Hiralde Vega – Nicolás Kitainik – Alejandro Laje – Sabrina Luini – Ramón Massot – Luz Pagano – Hernán Pagés – Alfredo Popritkin – Laura Ragoni – Lucas Ramírez Bosco – Carlos E. Tambussi.

• **Tomo 2. Arts. 1430 a 2671.** **Autores:** Liliana Abreut de Begher – Beatriz Areán – Jorge O. Azpiri – Eduardo Barreira Delfino María I. Benavente – Gabriela Boquin – Roque Caivano – Carlos Calvo Costa – Marcelo Camerini – Juan Casas – Federico Causse Rubén Compagnucci de Caso – Leandro Cossari – Nelson Cossari – José Fajre – Eduardo N. Farinati – Juan J. Formaro – Andrés Fraga – Alberto Gabás Lidia Garrido Cordobera – Marcelo J. Hersalis – Gabriela Iturbide – Jorge Juliá – Alejandro Laje – Ricardo Nissen – Martín Paolantonio Christian R. Pettis – Lucas Ramírez Bosco – Javier Rosembrock Lambois – Luciana Scotti – Gabriel Ventura – Luis M. Vives.

un Modem o Router por estos inconvenientes. Pero de todas formas dichos equipos tienen un firmware que siempre se encuentra desactualizado, es decir hace que el inicio de tu conexión y poder realizar una libre VPN se torne imposible, con ello necesitamos openwrt y además de ser código abierto y utilizar licencias del tipo GPL, se encuentra muy actualizado.

Además, en estos ultimo días se descubrió que Estados Unidos logró descifrar el código de las tarjetas Sim Card de una empresa [1]y esta misma opera en Argentina con Telecom Personal[2]

Parte 3.

Navegando en privado.

Mucho se ha dicho sobre TOR[3], quitando prestigio o diciendo que los usan "hackers para hacer cosas malas", la verdad es que para muchos nuestra privacidad es dinero y con hacer una gran campaña contra nuestra privacidad es muy buenos números para Estados y Empresas, fundamental a la hora de que nuestro cliente nos muestre algunas cosas en Internet, o la mera búsqueda de esto.

The Onion Routers mucho más conocido como TOR, es un sistema de comunicaciones en Internet, el cual nos permite modificar nuestra dirección IP y con ello generar una conexión segura y privada, para que no puedan generar un rastreo de nuestra navegación, de quien la utiliza y desde donde. TOR propone un enrutamiento del tipo "cebolla" es decir por capas, con lo cual hace imposible descubrir la IP de quien se encuentra navegando, claramente hay que tener configurado de forma correcta (cancelar cookies, deshabilitar todos los plugins java, etc) el navegador dado que muchas personas creen tenerlo configurado de forma correcta y no es así.

Según declaraciones de Snowden la agencia de seguridad de Estados Unidos habría roto la seguridad de dicho sistema, consiguiendo mediante una inyección de paquetes detectar un %80 de los datos traficados por dicha red, en cuanto se informó de este inconveniente se cambio el sistema y se colocó una libre VPN haciendo imposible el rastreo de ningún paquete.

En este caso es el único que utilizamos el concepto inverso de lo que veníamos demostrando (romper para reparar) dado que en sus inicios TOR fue creado con el fin de proteger las comunicaciones de la armada naval de Estados Unidos y luego por falta de financiamiento recae en TOR Project desde 2005, en marzo de 2011 TOR fue premiado por la Free Software Foundation[4] y se encuentra utilizándose para aquellos países que vulneran la libertad de expresión y diversas cuestiones políticas en Internet, como vemos tiene finalidades muy distintas a la mala prensa que contiene el servicio que brinda.

Parte 4.

El correo electrónico.

Actualmente se cree (en el campo del derecho) que el correo electrónico es igual que una carta ordinaria, y no es cierto, más bien es como el envío de una postal sin sobre, es decir que el sobre protege de una forma la privacidad del correo y en el correo electrónico no existe un "sobre" sino que circula desprotegido de tal elemento.

Existen varias formar de vulnerar la seguridad de los correos, pero siempre es necesario instalar en la PC a atacar un Keylogger o una aplicación, para obtener la dirección y la contraseña, podemos instalar en la PC un software como keylogger Doublas 2,0 y aguardar a que cualquier persona ingrese desde esa PC (es claro que todo lo que escriba va a ser guardado en una carpeta oculta) se debe tener el antivirus (si utilizan SO privativos) deshabilitado.

Podemos realizar ataques con Kali Linux para obtener dichas contraseñas, con ingeniería social, es una forma de obtener cualquier tipo de contraseñas, desde un ataque remoto.

Pero existe un problema adicional a la privacidad y seguridad de los usuarios, y es

[1] La Emprea es Gemalto http://infomed66.blogspot.com.ar/2015/02/nsa-robo-millones-de-sim-card-claves-de.html

[2] http://tecnoportaleconomico.blogspot.com.ar/2011/10/gemalto-y-personal-argentina.html por ejemplo en el acceso a Facebook de sus clientes.

[3] https://www.torproject.org/

[4] https://www.fsf.org/

que el servicio de correo electrónico se encuentra en permanente vigilancia de los prestadores más comunes (como Gmail), para brindar publicidad o para (a pedido de la justicia en nuestro país) obtener todos los correos de determinado usuario.

Entonces ¿como nos protegemos?, recordemos que vamos a proteger la privacidad y la vigilancia, entonces existen varias formas.

Cifrar el contenido del mensaje[1], es decir utilizar un software de cifrado para ello necesitamos distintas claves (una publica y una privada), en el cual el mensaje (en este caso nuestro mail) no va a ser observado por la empresa que brinda el servicio, y de ningún otro usuario que no tenga dicha clave publica.

Otra forma es utilizar servicios de correo electrónico que garanticen la seguridad de nuestros mensajes y nuestra privacidad (como ser Riseup[2]) estos servicios no solo tienen cifrada la comunicación de nuestro mail (desde origen hasta destino) sino que los servidores utilizados se encuentran cifrados, con ello se protegen de ataques externos y de cualquier solicitud judicial que quiera obtener dicha información.

Lo ideal es tener un servicio de correo electrónico para usos generales, y un servicio que resguarde nuestras comunicaciones para obtener una privacidad de las cosas que queremos que sean privadas, por ejemplo la comunicación entre abogado y cliente.

Parte 5.

Redes sociales.

Como vimos en la Parte 4 cualquier ataque externo puede darnos la contraseña del usuario, es por esto que no se recomienda la utilización de casi ninguna red social (o mantener su uso conociendo las distintas vulnerabilidades que conlleva), si bien casi todas las personas utilizan redes sociales para distintos fines (recreativos, venta de productos, publicidad) muy pocos ven los riesgos que tienen frente a la vigilancia y privacidad de sus datos. No solo nunca se encuentra inscripta la base de datos, sino que todos los datos ingresados no son de pertenencia de quien los sube, sino de la red social (esto es un problema). Informar que nuestros datos (sean fotos, publicaciones o archivos) son de uso propietario por parte de las empresas es el modelo de negocio (dado que hasta borran los metadatos[3]) que es el de trasmitir publicidad directa en función a los gustos (o visitas) de quien usa dicha red social.

Además las empresas se encuentran en permanente observación por distintos organismo, que pueden ser muy buenos en materia de delitos, pero algunos no son de este tipo y brindan un espionaje muy real a sus usuarios.

Existe una red social en base a TOR realizada en Buenos Aires y su nombre es Ciboulette[4] dado que opera con la misma lógica que TOR es 100% privada si realizamos la configuración correcta y manejamos los proxys de forma correcta. Esta es la única red social completamente segura para el usuario.

Parte 6.

Protección de nuestra PC.

Como anteriormente dijimos, utilizar software libre es una de las opciones más seguras en relación a virus y malware debemos aumentar el nivel de nuestra

[1] https://enigmail.net/home/index.php es un servicio adicional al Thunderbird y cifra nuestros correos antes de ser enviados a cualquier servidor.

[2] https://help.riseup.net/es una buena aclaración es que para obtener una cuenta hay dos formas, una es solicitar la cuenta indicando el motivo por el cual se requiere este tipo de correo (casi nunca responden), la otra es soliicitar dos códigos (una a cada usuario diferente) y poder abrir nuestra cuenta nueva.

[3] Para saber que es un metadato y que redes sociales las eliminan recomiendo http://netting.wordpress.com/2013/09/02/imagenes-a-por-los-metadato/

[4] http://wiki.hackcoop.com.ar/Ciboulette

seguridad, dado que los dispositivos que utilizamos son de muy buena utilidad para vulnerar la privacidad y generar un nivel de vigilancia óptimo. Casi todas las Notebook, Netbook poseen cámaras de video o webcam y casi ninguna de ellas tiene su lente cerrada, y este es un objetivo más habitual de lo que pensamos tanto por delincuentes como por parte de investigaciones que pueda utilizar cualquier servicio del Estado (el nuestro o cualquier otro) para poder observar quien se encuentra frente a estos dispositivos (un ejemplo básico es utilizando Cammy, pero existen otras formas). La única forma se estar seguros es tapando el objetivo de la cámara.

Si nuestros datos pueden ser vulnerados, ingresando a nuestra PC, como me protejo?.

Entonces podemos cifrar nuestro Disco Rígido, esto se puede realizar al instalar el Sistema Operativo (un Ubuntu, por ejemplo), pero si no le realizamos en ese momento podemos utilizar Truecrypt (pero desde hace unos meses presenta problemas de seguridad), recomendamos utilizar LUKS[1] (en caso de utilizar Sistemas Operativos Libres) o AxCrypt (en Sistemas Operativos Privativos). LUKS es posible su utilización en dispositivos de almacenamiento externos. Si interesa saber como es el funcionamiento de GPG, solo hay que visitar su web https://www.gnupg.org/ donde explican de forma muy completa su desarrollo.

Si tenemos archivos cifrados y deseamos enviarlo a cualquier servicio de “nube”, entonces ciframos nuestros archivos y los subimos, destacamos que algunos servicios de “nube” se encuentran brindando información a distintos Estados, por ello en caso de necesitar este tipo de servicios recomendamos utilizar Owncloud[2]

Si bien existen muchas otras formas de vulnerar la privacidad de las personas, sean por el Estado o por delincuentes, existen formas de protegernos y esta es la finalidad de este trabajo, el mismo presenta las ventajas de utilizar software libre. Lo importante de nuestra privacidad (además de ser nuestra), es mantener la confidencialidad entre Abogado y cliente.

Autor: Rodrigo Iglesias.

1 https://code.google.com/p/cryptsetup/

2 http://owncloud.org/

Dra. Paulina Casares Subia

- Corresponsal en Ecuador de la Red ElDerechoInformatico.com

Maestrante en la Maestría en Ciencias Forenses (Especialidad Criminología)– Universidad Marista de Guadalajara – Guadalajara –México (2013 – 2015)

Máster en Informática y Derecho (Derecho Informático) – Universidad Complutense de Madrid – Madrid – España (2002/2003) – Registro SENESCYT No. 4244R- 12 -2615

Ciencia Ficción vs Realidad

¿Estamos acaso viviendo una novela de ciencia ficción? La verdad es que ya no sabemos si lo que estamos viviendo en estos días es real o se trata de una novela de ficción. Los avances que la ciencia y la tecnología están desarrollando especialmente en el campo médico son cada día más grandes y no sé si decirlo de cierta forma hasta tenebrosos y macabros.

El pasado mes de marzo me encontré con una noticia que me puso los pelos de punta, el titular decía: ***"Monstruos híbridos humano-animal están siendo creados por científicos"***, inmediatamente se me vino a la mente la novela de ciencia ficción **"La Isla del Dr. Moreau"** de George Wells de 1896, novela en la que su autor ya plantea la vivisección de animales con el fin de transformarlos en humanos y es así que mientras leía el artículo mi asombro era cada vez más grande en especial cuando dicen que:

"Es sólo cuestión de tiempo antes de que los seres humanos comiencen a permitirse a sí mismos modificarse genéticamente con el fin de "luchar contra las enfermedades" o "mejorar" sus capacidades. La tentación de insertar los genes de animales o plantas en las personas con el fin de crear "súper soldados" o una "raza superior" sin duda llega a ser demasiado tentador. A menos que se haga algo para contener toda esto, al parecer será casi seguro que el infierno genético se desatara sobre la raza humana. Una vez que los seres humanos modificados genéticamente comiencen a criar a los seres humanos normales no podremos meter al genio nuevamente en la botella. Con el tiempo, podríamos llegar al punto donde hay muy pocos "100%" seres humanos".[1]

Es así que la aparición de lo que hoy conocemos como bioderecho tiene su razón de ser, en especial cuando hablamos de la manipulación de las conocidas como células madre que son aquellas que están en todos los organismos multicelulares y tienen la particular capacidad de dividirse y diferenciarse en distintos tipos de células especializadas y de auto renovarse para poder producir más células madres; es debido a esto que han surgido muchos términos para nombrarlas, ya sea por su origen o procedencia; por su capacidad reproductiva funcional, lo que va dando lugar a las células hijas de diversos linajes y distintos tipos de especialización.

Dos son las características fundamentales de las células madre:

1 http://www.masqforo.com/post/Curiosidades/2836/Monstruos-hibridos-humanoanimal-estan-siendo-creados-por-cientificos.html

- Capacidad de generar otra célula con sus mismas características (autorenovación); y,
- Capacidad de generar células diferenciadas de tejidos específicos (diferenciación)

Dados los antecedentes expuestos es que existen múltiples instrumentos internacionales en materia de derechos humanos y bioética, que buscan la regulación de estas investigaciones científicas, esto en atención a que el Bioderecho Internacional no sólo ha sido un gran apoyo para el desarrollo del Bioderecho Interno sino que, ha sido un aporte esencial en la conceptualización actual de la bioética en su relación directa con la dignidad y los derechos humanos, generando su vinculación estrecha con la ética de las ciencias y de las tecnologías, así como en la comprensión de sus elementos sociales.

El bioderecho como lo conocemos nace de la unión de la bioética y el derecho como una necesidad para dar solución a los distintos interrogantes que surgen del orden biológico y jurídico, con el fin de instaurar ciertos límites lícitos en la intervención artificial del ser humano/científico en la vida.
El objetivo central del bioderecho se enfoca a los temas relacionados con la vida y la muerte, así como de los límites respecto de la libertad de investigación y experimentación, pero sobre todo en la intervención y manipulación de los procesos naturales.

La bioética se caracteriza por ser una ciencia multidisciplinar que tiene como punto de partida los valores, los criterios y principios éticos que permiten analizar la conducta humana y que va de la mano del avance científico y tecnológico, en especial en su aplicación con la vida humana; es de esta forma que términos como biojurídica o bioderecho se utilizan para referirnos a los límites que se impone a la actividad científica y que tienen como base a la bioética, aunque muchas veces esos límites sobrepasen o se contrapongan a un sentir social o religioso, como sería el caso del artículo referido líneas anteriores.

Algunos de los principales problemas que enfrenta el bioderecho son: el aborto, la reproducción asistida, la crioconservación de embriones, la clonación, la maternidad subrogada, el consentimiento informado, la manipulación genética, la eutanasia y el suicidio asistido.

Si bien el derecho busca normar las conductas humanas, no podemos dejar a un lado religiones y sistemas éticos, donde la polémica se desata al tratar de establecer si la vida humana comienza en la fecundación, pues de acuerdo con sus argumentos, cualquier medida intencional para detener el desarrollo después de la concepción se considera como la destrucción de una vida humana. Sin embargo, científicos y críticos no tienen un problema moral con la investigación con células madre humanas, pero tienen miedo de un precedente para la experimentación humana.

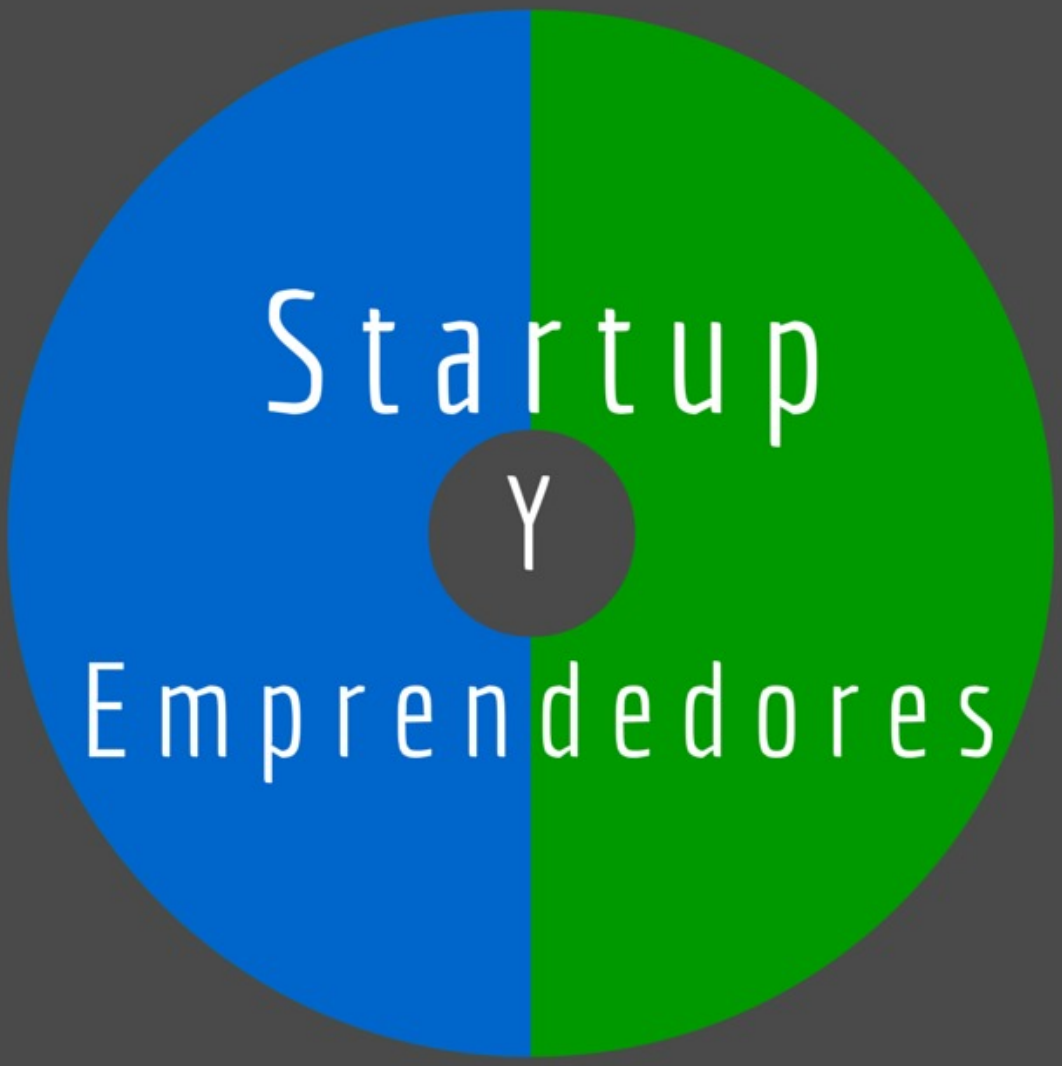
Algunos críticos apoyan la idea de la investigación, pero quieren que se impongan estrictas normas legales que impidan la experimentación genética con humanos, como la clonación y que garanticen que los embriones humanos sólo se obtengan a través de fuentes apropiadas. Prevenir que la investigación con células madre humanas se convierta en una plataforma directa hacia experimentos genéticos humanos es lo que genera la gran controversia alrededor del tema; sin embargo el desarrollo que el ser humano ha traído consigo, existen acontecimientos muy importantes especialmente en el campo de la ciencia que han desencadenado en nuevas técnicas tanto de obtención, preservación y tratamientos médicos que van de la mano de las células madre.

Y es de esta forma que para Flores Trejo (2004)[1], el Bioderecho gira en torno a ciertos principios fundamentales:

1. Libertad de investigación limitada,
2. Libre experimentación condicionada,
3. Intimidad individual,
4. Confidencialidad individual,
5. Supremacía de la dignidad humana,
6. Exclusividad de la especie humana y, por último,
7. Indiscriminación genética

Finalmente y contestando a la pregunta con que iniciamos, podemos decir que la ciencia ficción se convirtió en una realidad latente, sin embargo nos deja abierta una interrogante aún más fuerte… ¿Estamos en la cúspide del renacimiento biológico, o estamos sembrando las semillas de nuestra propia destrucción?.

[1] http://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CCIQFjAB&url=http%3A%2F%2Fwww.anaipes.udg.mx%2Fdoc%2Fmem_XIX%2FPonencia%2520Dr.%2520Flores%2520Trejo.doc&ei=5m4dVb_CKoqfNuLwg_AC&usg=AFQjCNGUZHOUxzwWeePA7VXjVYIB_AhM9w&bvm=bv.89744112,d.aWw



Responsable: Dr. Jorge Luis Garcia Obregón

Empresas digitales.

Hace un tiempo atrás escribí sobre las empresas digitales, desde mí blog personal, pero la verdad el tema requiere mayor atención con énfasis en los modelos de negocios actuales que tenemos. Veamos:

¿Qué es una empresa digital?

Podríamos decir que es una unidad de negocios, en las que su estructura interna, su estrategia de marketing, su relación de proveedores, clientes y directivos interactúan por medios digitales. Este tipo de empresas están tomando mayor auge en el mercado, van creciendo a pasos de gigantes, tomando el control de las actividades económicas de manera voraz. Ya no hay espacio para la estructura clásica de empresa, con jefes y empleados dispuestos a cumplir horarios como albañiles donde desean únicamente terminar la jornada y esperar fin de mes para cobrar su cheque…

La tercerización de servicios ha crecido de manera constante a nivel mundial, pues tiene increíbles ventajas; mayor rapidez y eficiencia, menos riesgos y costos, fluidez operacional, mejor trato contable, etc.

Hace un par de años las empresas digitales estaban germinando en modelos de negocios ya hoy en día clásicos como diseños de páginas webs, alguna que otra publicidad ó el boom del diseño gráfico, pero ese tiempo ya paso! Ahora, podemos ver como el espectro digital se ha expandido a otros modelos de negocios; tales como la venta retail, exportación de bienes y servicios, delivery y cuantas actividades económicas deseemos imaginar, ya están en la web…

Una empresa digital como tal, puede crecer en una cochera, en una sala de estar de un apartamento, no requiere mayor estructura que una laptop y una conexión de alta velocidad en internet. Los conocimientos en páginas web y similares puede ahorrarte mucho dinero, también puedes instruirte online sobre ellos a un menor coste, así mismo como cualquier otro tipo de conocimientos adicionales que sean interesantes a tu modelo de negocio, te agradaría conocer la cantidad de recursos útiles y gratuitos que hay en la web, entre ellos te puedo mencionar como instrucciones para desarrollar un plan de negocios, una estrategia de mercado, un modelo de organización y maxificación de recursos, estrategias de marketing, entre otros…

Las empresas digitales como tales, han sido identificadas en su estructura y funcionamiento por ciertas características, que han señalado su esencia marcaria. Entre estas características puedo mencionar las siguientes:

1) Una empresa digital no puede funcionar su esquema de negocios sin Internet. Sí fuera una empresa tradicional, como las de comercio con establecimiento fijo, la falta de internet podría considerarse como una limitante, pero jamás sería una parálisis de operaciones detendría de operar a falta de éste. Por ende, podemos deducir que sí una empresa depende 100% de una conexión a internet, es una empresa digital.

2) Su forma de trabajo se define por sus creadores. Su misión, visión y cultura es definida por sus fundadores, quienes son muy exigentes en cuanto a la satisfacción inmediata de los clientes. Saben que el cliente es vital. Así también algunas veces podemos ver que la forma de trabajo se aleja un poco de la concepción convencional que existe, en cuanto a horarios, vestimentas y otras convenciones propias de las empresas tradicionales.

3) Trabajan en equipos pequeños, sus ciclos de planificación son cortos, son rápidos y crean sus productos muy rápidos, pues prefieren cambiarlos en el camino y no perder el tiempo en un diseño que perdure en el tiempo, por ello se tiende a algo similar a

prueba y error. Sino sirve se desecha y si requiere se mejora.

4) Trabajan de manera horizontal, pues lo vertical evita el aporte de creatividad de este modelo de negocios. La colaboración es parte de su esencia. Sí bien es cierto que hay un líder en ellas, no siempre este líder trabaja como director de orquesta o mando militar, sino más bien es alguien que está ahí y trata de aprender de su equipo de trabajo a la misma vez que colabora fuertemente con ellos.

5) La burocracia es su enemiga. Las ideas son el motor y la comunicación su combustible, pues todo fluye ajeno a las tensiones de las empresas tradicionales. Por ello, es normal ver que los procesos se eliminan y se crean más bien puentes especiales de producción y maxificación de tiempos.

6) Sus colaboradores son escogidos más por su personalidad que por su CV. En estas empresas se requiere más el deseo de innovar y cambiar que un Cv de Harvard ó un PHD.

En algunos países de LATAM, estos modelos de negocios, han comenzado a surgir ampliamente. Pues, representan un modelo de vida más que una unidad económica. Por ello, es que países como Colombia han logrado en estos días ser íconos de referencia en este tema, al igual que Chile. Así poco a poco, podemos ver como en el ecosistema emprendedor van creciendo estas economías de negocios escalables.

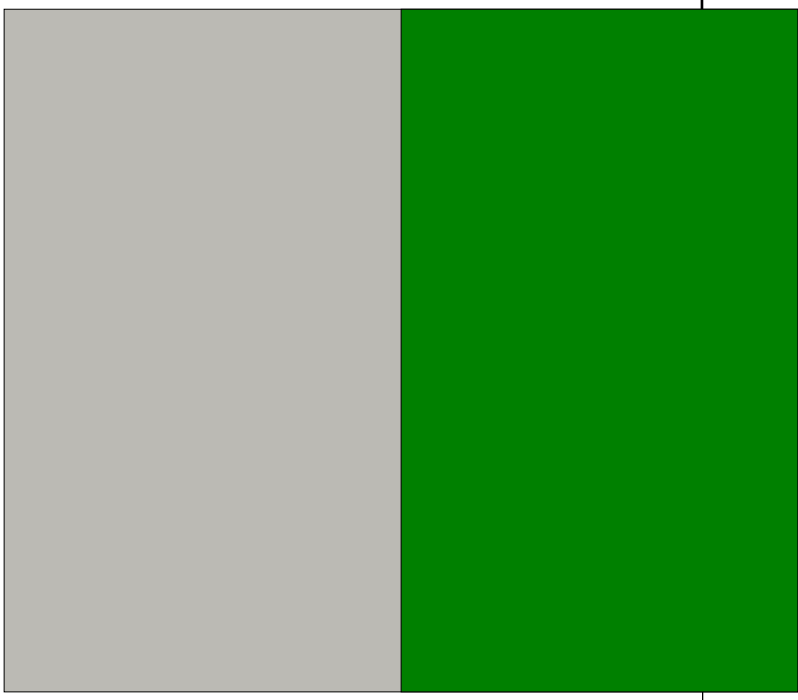
Para este tipo de empresas sin embargo no es ajeno que tienen que cumplir ciertos parámetros y requisitos legales para poder afianzar de manera firme y exponencial su negocio.

Para ello, es primordial siempre tener en el radar que es imperante escoger un vehículo legal apropiado para la formalización empresarial. Bien sea, que empecemos por una sociedad anónima que permita la entrada de financiamiento por varias vías, entre las que podemos señalar; prestamos, inversionistas, venta de acciones… Entre otros…. Debes diseñar tu negocio con un vehículo legal que prevea el crecimiento exponencial que vislumbras, previendo elementos importantes como la internacionalización, la financiación, entrada de nuevos socios e incluso la salida de aquellos que deben salir.

Luego, está la protección de la idea donde debes ver que esto es lo más importante de tu empresa, pero también representa el mayor activo de la misma. No debes jugar a esconderla, sino más bien a protegerla.

Así mismo, debes valorar el elemento fiscal. Este punto es trascendental verlo en la fase germinadora de negocios. Pues, si no lo estudias con el tiempo que se merece verás que luego te puede comer parte de tu empresa.

En números anteriores y próximos a ésta edición podes ver temas relacionados a los que te hablo, por ello te invito a que los leas y que así mismo, visites mi blog www.itaxlegal.com



www.itaxlegal.com

TAXLEGAL

Derechos de Negocios/ Planificación Fiscal/ Derecho deTICs

El Blog de Jorge García

LMSTREINAMENTOS.COM.BR

ELDERECHOINFORMATICO.COM - BRASIL

CAFÉ

INFORMÁTICO

INVITAN

TODOS LOS MESES VIA STREAMING

Coordina: Dra. Laine Souza

Modera: Guillermo M. Zamora

Inscripción Gratuita - Certificados: 10U$S

Un proyecto de la Red Iberoamericana
ElDerechoInformatico.com

Tu wifi muestra donde vivís, trabajás y viajás

Autor: Franco Vergara

Licenciado en Informática
Especialista en Seguridad Informática
mail@francovergara.com

Tenía un artículo casi terminado, casi listo para enviar hasta que se me cruzó esto que les voy a presentar..

En la era en donde todo el mundo busca un motivo para compartir lo que hace o deja de hacer en su red social favorita cada vez hay más dispositivos electrónicos con acceso a internet por una interfaz wifi; Laptop, celulares, tablet, cámaras de fotos y una larga lista de etcéteras de equipos que generalmente son portátiles y digo generalmente porque, por ejemplo, Samsung tiene el modelo RF4289, una heladera con que viene conectividad wifi.. algo que nunca me imaginé de chico. En fin de la larga lista de dispositivos vamos a centrarnos en el que se lleva el primer puesto en lo que a movilidad respecta: El teléfono celular.

Seguramente más de un usuario de este tipo de tecnología escuchó alguna vez que su teléfono podría ser rastreado fácilmente usando tanto la red telefonía móvil como el GPS (rastreo satelital) pero, ¿Usando el wifi del equipo? y ¿Sin tener ni un App instalado? No creo. Tanto los teléfonos celulares como la mayoría de dispositivos con conectividad wifi suelen almacenar las redes a las que algunas vez estuvieron conectadas y cuando el aparato se encuentra nuevamente dentro del rango de una red almacenada el teléfono utiliza las credenciales que tiene en su poder para conectarse automáticamente, siempre y cuando los datos de acceso no hayan sido modificados. Y lo que puntualmente almacena un teléfono para volver a conectarse es: su nombre de red (SSID) “Casa”, por ejemplo, la dirección o identificador único del equipo que provee la conección (MAC) El modem, por ejemplo, y la contraseña de acceso si la red la tuviese.

En general los nombres de estas redes suelen mantener una nomenclatura:

· Las Redes hogareñas: Suelen llamarse "Casa" o tener el nombre del proveedor de Internet asociado a algún número.

· Las Redes Laborales: Suelen tener el nombre de la empresa.

· Las Redes de Hoteles: Suelen tener el nombre del hotel o una combinación del nombre.

· Los Cafés, Fast foods: Suelen tener el nombre del lugar en cuestión.

¿ Y todo de los nombres de redes, SSID, MAC que tienen que ver con la localización de un teléfono celular?

WiGLE, https://wigle.net/ , es una web que prácticamente cumple con la premisa de su slogan “*Todas las redes que se encontraron en el mundo*”. Si bien es casi imposible que un sitio tenga registradas todas las redes wifi del globo esta web tiene una base de datos muy, muy extensa y que además está vinculada con los mapas de google por lo que una red se podria ubicar tanto por su nombre (SSID) como por las coordenadas del GPS y entre nos, yo no me aguante las ganas y tuve que verificar si **WiGLE**

realmente funcionaba así que usando mi celular obtuve las latitud y longitud de mi ubicación, la cargue en el sistema y la respuestas, para mi agrado, fue positiva.

Ahora, una persona que tenga acceso a un teléfono celular ajeno ya sea físicamente porque de alguna manera llegó a sus manos o virtualmente, capturando los datos con algún software tipo "Aircrack", podría utilizar el registro de todas las redes que tiene almacenadas el teléfono y con la ayuda de **WiGLE** conocer todos los lugares por donde estuvo el aparato y así, basándose en los patrones normales de los nombres que suelen tener las redes inalámbricas, conocer el perfil del dueño del dispositivo; Donde trabaja, Donde estudia, Donde vive, Donde fue de vacaciones, etc.

Pero seguramente más de uno estará diciendo: "Hay un montón de redes con el mismo nombre en el mundo. McDonalsFree, por ejemplo." Y tienen razón pero en el caso alguien intente hacer una búsqueda o rastrillaje y se cruce con 100 redes
"McDonalsFree" seguramente utilice los filtros de búsqueda que ofrece el sitio además de el sentido común para darse cuenta que un teléfono encontrado en Ecuador no podría acceder una red llamada "McDonalsFree" un día en Alemania y al otro en Brasil.

Vamos con un ejemplo Práctico:

Luego de cargar una serie de datos en el sistema llegamos a la siguiente conclusión: Los marcadores verdes son redes encriptadas, los rojos son redes abiertas y si bien en este caso no aparecieron, los marcadores azules corresponderían a redes desconocidas. Cada uno de los puntos hace referencia a un solo y único lugar que en este caso y por el zoom no se aprecia. La persona en análisis trabajaría en Buenos Aires, por el nombre y tipo de la red, viajaría a Mendoza también por trabajo y pasó una estadía de vacaciones en Uruguay también por el SSID de la red: "HotelXX"

Que quede claro que este es un ejemplo muy específico y concreto y que en el seguimiento pueden haber muchas fallas/errores como por ejemplo la caída de una red por un fallo técnico o simplemente el cambio de nombre de la misma

¿Cómo nos defendemos de esto?

En Android, que es el sistema operativo que hace años vengo eligiendo, hay una serie de programas que van a ayudarnos a mantenernos seguros de esto: WiFi Advanced Config Editor, Wi-Fi Privacy Police, Wi-Fi Matic -Auto WiFi On Off.Ahora encontrar los programas que logren este cometido en otras plataformas (IOS, Windows Phone) queda como tarea para el hogar para mí y para ustedes.

La Violencia y la Informática

Autor: Marcelo Campetella - Abogado - Especialista en Derecho Informático
abogado
http://www.campetella.com.ar/

Con esta afirmación comienza la ley 4241 de la provincia de Río Negro (Argentina), que en el año 2007, modificó en forma integral a la famosísima ley 3040. Es más, "tiene una 3040" significa ya no solo en la jerga legal, sino que es "vox populi", que ha habido una denuncia por violencia en la mayoría de los casos de una mujer contra un hombre, esposo, novio, concubino o cualquiera de estos que sea un "ex".

Y en menor medida de hombres contra mujeres.

Y si es por citar normas vigentes aplicables a los casos de violencia, de manera subsidiaria y complementaria encontramos a la Convención de Eliminación de toda forma de Discriminación contra la mujer, la Convención Internacional de los Derechos del Niño, Niña y Adolescentes o la ley 26.485 de Protección Integral para prevenir, sancionar y erradicar la violencia contra las mujeres en los ámbitos en que se desarrollen sus relaciones interpersonales.

Hecha esta introducción, nada nuevo bajo el sol, nada que los jueces de familia, defensores oficiales y los abogados no sepamos. Muy bien, realizada la denuncia, en un juzgado de paz o en la comisaría más cercana es precisamente el Juez de Paz quién dicta las primeras medidas cautelares atendiendo las características de la denuncia y las razones de urgencia para luego enviar el expediente a un Juzgado de Familia para que confirme esas medidas.

En tal sentido las medidas que la ley menciona son la exclusión del denunciado de la vivienda en donde habita el grupo familiar; restituir a la víctima al hogar si fue ella quién tuvo que escapar para salvar su vida; la prohibición de acceso al denunciado tanto al domicilio de la víctima como a su lugar de trabajo, estudio o esparcimiento; fijarle un perímetro de exclusión para permanecer o circular, conocida como "restricción o prohibición de acercamiento" todas medidas justamente para prevenir nuevos hechos de violencia o la muerte de mujeres y hasta de hijos o parientes inocentes. Claro que esta enumeración de medidas cautelares es enunciativa y el abanico es amplio, ya que según la ley, se podrá ordenar cualquier medida necesaria y oportuna para garantizar la seguridad de los integrantes de la familia o hacer cesar la situación de violencia y evitar la repetición de todo acto de agresión, perturbación o intimidación por parte del agresor.

Y que tiene que ver la informática con todo esto? Tiene mucho que ver, ya que el agresor, el violento con prohibición de acercamiento a todos lados, excluído del hogar, continúa acechando, acosando, amenazando, torturando psíquica o emocionalmente a través de la comunicación electrónica, a través de los mensajitos de textos al celular o por WhatsApp, por mensaje privado en Facebook ya sea a través de un face falso o el del propio agresor o en los audios de los mensajes que quedan grabados en un celular o en un contestador automático. La violencia entre el cobarde y violento y la víctima continúa y no cesa, pese a todas las medidas cautelares que se dictan inicialmente en un juzgado de paz. Lo novedoso y particular, es que toda comunicación electrónica

receptado en el Código Penal de nuestro país. Lo novedoso es comenzar a establecer enl as resoluciones judiciales la prohibición de comunicación electrónica del den unciado hacia la víctima.

Luego de dispuesta la prohibición de comunicación electrónica, el denunciado podrá continuar comunicado a través de un tercero, una abuela, una amiga pero no en forma directa con la denunciante, porque el circulo vicioso de la violencia no cesa y muy por el contrario aumenta con finales trágicos. Si se prestara atención a la comunicación electrónica existente y previa a los sucesos de lesiones gravísimas o la muerte de las víctimas, es muy probable que se encuentre suficiente y sobrada prueba que anticipaba que iba a suceder lo que luego ocurrió. Es decir, hoy no alcanzan las medidas cautelares preventivas dictadas luego de recibida la denuncia, las que deben completarse con esta prohibición de comunicación electrónica. Todos los operadores del sistema de justicia los jueces, defensores, jueces de paz y abogados pueden recurrir a esta medida cautelar y preventiva identificando los medios por los cuales no podrá comunicarse si fuera necesario. Y por supuesto que la víctima es la primer persona que lo puede solicitar. Y en caso de que se viole la prohibición de comunicación electrónica realizando una amenaza un nuevo delito habrá cometido el violento: el de desobediencia judicial.

No existen vacíos legales en la fría ley escrita

aunque sí víctimas, hijos y familias.

Contents

EL DECLIVE DE GOOGLE

Autor: Manuel de Cristóbal López

Abogado - Madrid

manuel@asesoria-legal-ya.com

http://www.legaltoday.com/colaboradores/de-cristobal

es.linkedin.com/pub/manuel-de-cristobal/6b/a23/206/

https://www.asesoria-legal-ya.com/content/opinio/colaboradores/mcl

Al principio Internet era un escaparate de información a través de páginas "web" pero rápidamente creció y surgieron páginas comerciales, catálogos de ventas, opiniones personales, noticias, "blogs" íntimos, etc. Estructuralmente, no existe forma de catalogar o diferenciar cada uno de esos elementos.

Al éxito de los buscadores como GOOGLE es consecuencia de la prestación de un servicio gratuito que todo el mundo reclama y utiliza, y que ha sido posible por su novedad, ausencia de legislación y desconocimiento de posibles efectos. Pero recientemente, se empezó a tener conciencia de esos efectos adversos, en ocasiones, muy negativos; y, de forma unánime, en todos los países, se reclama judicialmente la protección del derecho a la intimidad, a la privacidad, surgiendo normas sobre tales aspectos.

Actualmente, a este gravísimo problema se le conoce coloquialmente como **"DERECHO AL OLVIDO".** Realmente es algo más complicado que tres simples palabras. La solución judicial ha sido reconocer, en abstracto, este derecho pero con la ausencia de una legislación completa sobre la materia se carece, incluso, de definiciones legales que fijen con exactitud muchos de esos criterios citados en las resoluciones judiciales. Se desconocen los límites de las ideas o conceptos que se utilizan definidos eb normas jurídicas y resoluciones judiciales.

No está definido qué es un particular o un personaje público (así se podría considerar como persona pública a quien sale en una, dos o tres revistas, o una o cinco veces al mes, pero también a quien tiene quinientos o más contactos en "FACEBOOK").

Tampoco se sabe qué pertenece al ámbito del conocimiento público o a la esfera de la publicidad temporal de cuestiones privadas (por ejemplo, una lista de boda o una esquela; el nombre del cónyuge o la identidad de la amante del presidente de la compañía "X"). Las amantes son muy interesantes, en Derecho. A primera vista, pertenecen al ámbito más privado de la persona, salvo que le pidamos opinión a cierto expresidente de E.E.U.U. (o a varios) y, por otro lado, la normativa prevista en la Ley 10/2010, de 28 de abril, de Prevención del Blanqueo de Capitales

puede llegar a exigir conocer quien es la amante del presidente de la república “XXX”, a los efectos de cumplimentar la correspondiente comunicación por parte de dicho presidente, en cuanto sujeto obligado (art. 2), y esto significa que alguna empresa debe informarme (y venderme) una base de datos con los nombres de los presidentes del gobierno de todo el mundo, de sus cónyuges, exmaridos, exesposas, hijos, amantes, etc., algo impensable e inestimable para el común de las personas.

multa de tráfico por exceso de velocidad o una simple multa de aparcamiento. Cada tipo de información debería tener un tiempo preciso para tener que “olvidarse”.

La jurisprudencia española más reciente utiliza todos estos conceptos pero sin definirlos y, al tiempo, ha cargado su manejo sobre la espalda de GOOGLE, pero no le ha concedido la capacidad legislativa para delimitarlos, que sólo corresponde al Congreso de los Diputados. GOOGLE tiene la obligación pero

No se ha cuantificado la duración en el tiempo del “derecho al recuerdo” o del “derecho al olvido”.

Tampoco existe una clasificación de los diferentes tipos de información y el tiempo qué ha de transcurrir respecto de cada uno de esos tipos de información para esgrimir el “derecho al olvido”. No es lo mismo ser condenado por pederastia, por estafar 400.000 Euros o cometer un atraco a mano armada, que una

no tiene la capacidad jurídica para definir estos elementos. En el resto de los países, la situación no es muy distinta.

Por si fuera poco, GOOGLE es su propio enemigo pues quiere fijar un criterio único o universal, cuando la normativa sobre estos temas en E.E.U.U., Latinoamérica, Europa o Japón es muy diferente. La información, el lenguaje y el tiempo, también son enemigos de las pretensiones de

uniformidad del modo de trabajar de GOOGLE. La interpretación o valoración que se da hoy al contenido de una noticia, puede no ser la misma que tenía en el momento de su efectiva publicación hace cinco o diez años. No ha de olvidarse que se está pidiendo que se borre información, bajo los criterios interpretativos actuales, de noticias redactadas en un lenguaje de hace diez o veinte años o, en otros casos, como las Hemerotecas de algunos periódicos (en España, por ejemplo, ABC), la reproducción de periódicos de hace más de cien años.

Los elementos que se esgrimen en el actual "derecho al olvido" son conceptos que se irán definiendo con cuentagotas, en sucesivas sentencias dictadas por todo el mundo pero, como es lógico, con criterios muy dispares que, en ocasiones, serán incluso discrepantes.

En este escenario, GOOGLE es, de nuevo, su propio enemigo. Según las últimas sentencias existe una matriz de GOOGLE en E.E.U.U. (GOOGLE INC.) que es quien gestiona todos los buscadores y unas empresas, controladas por esa matriz, en las diferentes partes del mundo como, por ejemplo, GOOGLE SPAIN, que se dedican, básicamente, a gestionar publicidad. Esta estructura es económicamente funcional pero le resultará muy difícil la recepción y gestión de los cambiantes conceptos jurídicos de un país como España. A un Abogado en E.E.U.U., con formación jurídica anglosajona, le va a costar mucho entender conceptos de Derecho español basados en el Derecho Romano; conceptos para los que, además, en ocasiones, no existirá traducción directa o exacta al inglés, y si su filial en España no tiene abogados españoles, nunca recibirá un informe útil para poder adoptar cambios a la interpretación española de la ley local.

Si el problema jurídico tiene difícil solución, el problema técnico es aún peor. Resulta totalmente imposible que ese abogado de E.E.U.U. le explique a un programador informático los elementos que debe tener o contener el algoritmo de búsqueda para respetar la legislación de España, aplicando criterios de lingüística computacional a una noticia redactada en España, tratada a través de un traductor por un ingeniero en E.E.U.U. Y es de suponer que situación similar encontraremos respecto a la legislación mexicana, brasileña, japonesa o australiana. Con independencia de que se pueda explicar al programador todo lo anterior, estos elementos se van a acabar definiendo por vía judicial con un contenido, extensión y cuantificación diferentes en cada país. Un goteo de sentencias irá definiendo:

a.- Los elementos que deben usarse:

-Extensión, y

-Límites

b.- Qué es un famoso

c.- Qué es un particular

d.- Qué tiempo puede permanecer el "link" de una noticia que trate sobre un famoso o cuál es el tiempo de permanencia del "link" de una noticia sobre un particular, o sobre un político

e.- Cuáles serán los conceptos y tiempos aplicables a los diferentes supuestos

f.- Cuánto tiempo puede permanecer la crónica de sociedad de una boda o la referencia a la imputación de un delito, cuya pena privativa de libertad sea de veinte años, o una condena por pederastia o violación.

Hasta que el Tribunal Supremo dicte una sentencia que aclare y defina cada concepto, se irán acumulando nuevos procedimientos judiciales y se producirán **eventuales condenas** con indemnización y costas, que **lastrarán la cuenta de resultados de GOOGLE.**

Si GOOGLE NEWS ha cerrado en España por la aprobación de la nueva Ley de Propiedad Intelectual, no es de extrañar que, en los países más "conflictivos", es decir, aquellos que reconocen unas indemnizaciones más altas, o allí donde se tiene mayor conciencia de los derechos y/o mayor facilidad para litigar, la opción de GOOGLE será también el cierre. **Pasará como con las piezas de dominó: la gente descubrirá que puede ganar dinero demandando a GOOGLE, éste responderá cerrando las Sucursales** en cada país y podría ser que, en poco tiempo, se proceda a su cierre y liquidación definitiva.

En España el pasado mes de julio de 2014, la Audiencia Provincial de Barcelona resolvió un recurso de apelación formulado contra una sentencia desestimada en primera instancia, interpuesta por un ciudadano contra varios buscadores, entre ellos, GOOGLE SPAIN, S.L. **Es la primera sentencia referente al "derecho al olvido" contra GOOGLE, dictada en España, en la jurisdicción civil.** El actor solicitaba el "olvido" de un indulto de pena privativa de libertad a la que había sido condenado por un delito contra la salud pública cometido en 1981 (en España, es obligatoria la inserción de los reales decretos de indulto en el Boletín Oficial del Estado -BOE-), ya que cuando introducía su nombre y apellidos en GOOGLE, salía la página del citado boletín oficial informando del indulto de 1999. La Audiencia resuelve el recurso condenando a GOOGLE SPAIN, S.L. a pagar al actor la cantidad de 8.000 Euros, por vulneración de su derecho a la protección de datos personales. El fundamento de dicha condena es que **el indulto** a favor del actor -por unos hechos de 1981- data de 27 de agosto de 1999-, **fue publicado en el BOE de 18 de septiembre de 1999**, por tanto, **su aparición, en 2010, en la lista de resultados de un buscador de Internet** no se ajusta en absoluto a los principios de tratamiento de datos personales pues los **antecedentes penales son un dato sensible**. Es importante destacar que la sentencia también **rechaza la falta de legitimación pasiva alegada por GOOGLE SPAIN** sobre la base de que es la estadounidense Google Inc., la sociedad que gestiona o controla el motor de búsqueda de Google que indexó la página del BOE donde se publicó el indulto del demandante. Pero **esta sentencia no es firme** pues contra la misma caben recursos ante el Tribunal Supremo y, a fecha de hoy, no se ha podido constatar sí se ha formulado algún recurso.

Y, finalmente, señalar que en la jurisdicción contencioso

ODILA

Observatorio de Delitos Informáticos de Latinoamérica

administrativa, la Audiencia Nacional ha dictado recientemente (el día 29-12-2014) dieciocho sentencias sobre el "derecho al olvido". En catorce de ellas, desestima los recursos de GOOGLE contra las resoluciones de la Agencia Española de Protección de Datos, mientras que en las otras cuatro resoluciones, el tribunal estima los recursos del buscador frente a las pretensiones de los particulares, en algún caso por estimar que GOOGLE SPAIN no tiene legitimación y en otros porque los particulares no especificaron en su denuncia, ante la Agencia Española de Protección de Datos, que la búsqueda se realizó a partir de la introducción de su nombre como persona física en ese buscador, indicando los resultados o enlaces obtenido a través de dicho buscador, así como el contenido de esa información que le afecta y que constituye tratamiento de sus datos personales a los que se accede a través de dichos enlace, cuales eran esas páginas, características y antigüedad de las mismas, fines que pudieron justificarlas pues, según el tribunal, en estos casos, no es posible realizar el juicio de ponderación de los intereses en juego, como exige la sentencia del Tribunal de Luxemburgo de 13 de mayo de 2014 (asunto C-131/12) que responde precisamente a una cuestión prejudicial planteada por la Audiencia Nacional, en procedimiento sobre protección de datos personales entre "Google Spain" y "Google Inc.", por un lado, y la Agencia Española de Protección de Datos y un ciudadano español por cuanto al introducir su nombre, en el buscador aparecía información ligada a su identidad personal referida a un anuncio de subasta de inmuebles derivado de un embargo por deudas a la Seguridad Social, que estaba solucionado y cerrado desde hacía años. Sólo cabe añadir que las sentencias de la Audiencia Nacional también son recurribles ante el Tribunal Supremo en casación por lo que, todavía no está todo dicho en esta materia.

Por último señalar que cualquier ciudadano extranjero podría pleitear en España, invocando tal "derecho al olvido" siempre que la "web" que publique la noticia, y a la cual apunte GOOGLE, tenga algún vínculo, legalmente significativo, con España.

INTIMIDAD

SECCIÓN

PRIVACIDAD

Responsable

INÉS
TORNABENE

Protección de Datos Personales: repasando un poco de Historia, del Tercer Reich a Facebook

Durante casi 40 años, la gente estuvo bajo monitoreo y es obvio que esto pone a las personas muy nerviosas cuando se trata de la privacidad"
Carsten Casper, Gartner

El concepto de protección de datos está vinculado a la aparición del derecho a la privacidad en las postrimerías de la Segunda Guerra Mundial. Un enfoque en los derechos humanos básicos y las libertades fundamentales llevó a una serie de cartas y declaraciones internacionales, por ejemplo. la Declaración Universal de los Derechos Humanos (DUDH).

Poco después de que el régimen nazi de Hitler llegó al poder en 1933, el gobierno alemán comenzó a recopilar los catálogos de tarjetas de identificación de enemigos políticos y raciales del Reich alemán. En el siglo XX en Alemania, los personas que profesaban la religión judía se encontraban plenamente integrados en la sociedad alemana y ejercían diversas profesiones y ocupaciones. Sin embargo, una vez que Hitler llegó al poder, el pueblo judío se convirtió en un objetivo de exterminio. Una de las obsesiones de Hitler fue la purificación de la raza alemana basada en considerar que la raza aria era el ideal de perfección y que era una raza superior. Otro de los objetivos a perseguir por el régimen nazi fueron las personas con discapacidades. Y los gitanos. Así, se estima que entre cinco mil niños y ochenta mil adultos con discapacidad han sido asesinados en los hospitales estatales y las instituciones mentales bajo el régimen de Hitler. Seis millones de judíos y quinientos mil gitanos se calcula que han muerto en Europa como consecuencia de la Segunda Guerra Mundial, muchos de ellos asesinados en campos de concentración por los nazis.

Cuando pensamos en ese contexto histórico surgen algunas preguntas:

1.Cómo pudo el régimen nazi llevar a cabo un holocausto de tal magnitud?

2.Cómo sabían las autoridades nazis exactamente quién era judío?

3.Cómo eran capturados los judíos?

4.Cómo hizo el Tercer Reich para identificar áreas donde la mayoría de la población eran judíos?

Los nazis usaron los DATOS PERSONALES para crear sofisticados sistemas de identificación de la población. Entre estos sistemas hay dos que podemos destacar:

5.EL CENSO: Una de las principales herramientas fue el Censo Nacional de Población de 1939. En este censo se le pidió a los ciudadanos que informaran su origen étnico y su religión. Pero no sólo eso: también debían informar la religión de sus cuatro abuelos, de forma tal de poder rastrear el origen judío de cualquier persona. En tres años se terminó de completar el registro de judíos y judías, de raza pura y de raza mixta. El objetivo era proporcionar la base para la confección de las listas de deportación.

6.LAS TARJETAS DE IDENTIDAD: Mediante la combinación de datos obtenidos por distintas fuentes gubernamentales, se procedió a la distribución de tarjetas de identidad con fotos, de uso obligatorio para todos los habitantes del Reich, basados en un ley del 10 de septiembre de 1939. Un reglamento especial del 27 de septiembre del mismo año dio lugar a la distribución de las “tarjetas para judíos”

En una nota publicada por The Washington Post por Michael Dobbs, se afirma lo siguiente:

“Thomas J. Watson, el fundador de IBM, aceptó en junio de 1937 una distinción que se volvería en su contra: una medalla que Adolf Hitler creó para extranjeros “que demostraron ser dignos del Reich alemán”. Rebosante de svásticas y águilas, la medalla confirmaba la contribución de IBM a la automatización de la Alemania nazi.

En aquel momento, Alemania era el segundo cliente de IBM después de EE.UU. Los historiadores ya documentaron cómo la tarjeta perforada de IBM, precursora de las computadoras, desempeñó un papel importante en áreas que iban desde la puntualidad de los trenes alemanes hasta el programa de rearme de Hitler, pasando por los datos de censos, que constituían un elemento clave para la política racista nazi.

Pero un nuevo libro supone un paso más contra Watson e IBM y sostiene que la tecnología de esa empresa contribuyó a facilitar el Holocausto al permitir que Hitler automatizara la persecución a los judíos mediante la creación de listas de grupos destinados a la deportación a campos de exterminio.

El libro cuenta cómo, después de que IBM perdiera el control sobre las operaciones en Alemania en 1941 y Watson devolviera su medalla, la misma tecnología se siguió usando en Auschwitz y otros campos nazis a los efectos de registrar los ingresos y hacer un seguimiento de los trabajos forzados.

“La tecnología de IBM contribuyó a que las cifras del Holocausto alcanzaron niveles verdaderamente fantásticos”, argumenta Edwin Black, ex periodista e hijo de sobrevivientes del Holocausto. Black pasó tres años analizando la participación de IBM en la Alemania nazi para escribir su libro, “IBM y el Holocausto”. “El Holocausto habría tenido lugar con o sin IBM, pero el Holocausto tal como lo conocemos, el Holocausto de las cifras impresionantes, es el Holocausto de la tecnología IBM. Permitió a los nazis trabajar en otra escala, con más velocidad y eficiencia”.

Las conclusiones de Black dieron lugar a un acalorado debate entre especialistas en el Holocausto. Algunos historiadores avalan la tesis de Black de que IBM y su subsidiaria alemana desempeñaron un papel importante en la persecución nazi. Otros, en cambio, insisten en que la tecnología IBM no tuvo mucho que ver con el Holocausto.

Carol Makovic, portavoz de IBM, señaló que a la empresa le resulta difícil hacer declaraciones respecto del libro de Black ya que no tuvo acceso al mismo antes de su publicación. Agregó que IBM está dispuesta a colaborar con investigadores independientes y que depositó archivos importantes en la Universidad de Nueva York y la Universidad Hohemheim de Stuttgart, Alemania. Señala que la documentación sobre las actividades de la compañía en la Alemania nazi es “incompleta y de ninguna manera concluyente”. “Claro que

IBM considera que el régimen nazi fue algo lamentable", afirmó.

Según un mensaje interno de la compañía informática, la IBM alertó a sus empleados sobre la aparición del libro y dijo que si la obra "muestra nueva y verificable información que permita avanzar en el conocimiento de esa trágica era, IBM lo examinará y pedirá a reconocidos eruditos e historiadores que hagan lo mismo".

Una demanda contra la empresa fue presentada en Nueva York por sobrevivientes del Holocausto. Le reclaman compensaciones económicas.

La afirmación más controvertida del libro de Black es que la tecnología de tarjeta perforada de IBM se usó para generar listas de judíos y otras víctimas a las que luego se deportaba. Si bien no hay duda de que IBM de Nueva York permitió la utilización de su tecnología en operaciones de censo nazis, entre ellas los de 1933 y 1939, lo que se debate es la utilidad que tuvieron en la localización de personas.

La tecnología de tarjeta perforada se remonta a 1884. Herman Hollerith, un ingeniero germano-norteamericano de 20 años, creó un dispositivo para almacenar datos en tarjetas por medio de una serie de perforaciones, cada una de las cuales representaba un dato distinto, tales como edad, educación, domicilio y religión. Las tarjetas se ingresaban luego a una máquina, que cruzaba toda la información.

Las máquinas de Hollerith fueron la tecnología de información más sofisticada antes del advenimiento de la era de la computación. A partir de mediados de la década de 1920, las tarjetas perforadas fueron el principal vehículo de la expansión de IBM en todo el mundo. IBM patentó la tecnología, con lo que la empresa podía alquilar máquinas a sus clientes y al mismo tiempo ejercer un estricto control sobre la provisión de tarjetas perforadas.

La tecnología de Hollerith brindó a los nazis una poderosa herramienta de control social. Pocas semanas después del ascenso de Hitler al poder, en 1933, el director de la subsidiaria alemana de IBM, Willy Heidinger, proclamó que las máquinas ayudarían al Fuhrer a mantener la "pureza" y la "salud" de la política alemana.

Cuando estalló la Segunda Guerra Mundial, en 1939, IBM ya entregaba a la Alemania nazi más de mil millones de tarjetas perforadas por año, según el libro de Black. Las relaciones amistosas entre IBM y la Alemania nazi se deterioraron desde junio de 1940, cuando Watson le devolvió a Hitler su medalla con la explicación de que ya no podía seguir apoyando "la política de su gobierno". Al año siguiente, Watson perdió el control de la subsidiaria alemana de IBM, la Dehomag, que pasó a manos de Heidinger, del partido nazi.

Si bien no hay pruebas de que IBM supiera que las máquinas de Hollerith se utilizaban en lugares como Auschwitz, Black sostiene que la empresa lucró con las actividades de su subsidiaria Dehomag."

En el otro lado del Atlántico, los investigadores han demostrado recientemente, cómo la Oficina del Censo de Estados Unidos proporcionó información a las agencias de vigilancia estadounidenses durante la Segunda Guerra Mundial. Los datos del censo se utilizaron para identificar a las personas de ascendencia japonesa. O sea, que cualquiera sea el gobierno que la utilice, la información personal es una herramienta de poder que exige los rangos más elevados de protección jurídica.

La gente está empezando a entender el poder destructivo que la información podría tener en las manos de un mal gobierno y cómo la información recopilada para un propósito podría reutilizarse para una amplia gama de propósitos siniestros. Estos ejemplos extremos de sistemas de abuso de censos e identificación de la población para realizar un seguimiento de las minorías con el propósito de procurar su exterminio pesaron fuertemente en la mente de aquellos a los que le tocó a reconstruir Europa y se tuvo en cuenta al redactar las declaraciones de derechos humanos.

Este trasfondo histórico nos ayuda a entender por qué la confidencialidad es hoy en día reconocida específicamente como un derecho humano – la lección de la posguerra de proteger a los ciudadanos de la interferencia externa está consagrado en el artículo 12 de la Declaración Universal de Derechos Humanos (1948) y en el artículo 8 del Convenio Europeo de Derechos Humanos, (1950).

Los rápidos avances tecnológicos han dado lugar a un creciente interés en el tratamiento de datos personales en grandes volúmenes; cada vez hay mejor tecnología, más posibilidades de almacenamiento a gran escala y herramientas de análisis de la información más perfeccionadas y precisas. La protección de datos se concentra en las garantías necesarias que deben estar en su lugar en el tratamiento de datos de carácter personal a través de una variedad de medios de comunicación. Hoy en día, la protección de datos se compone de un marco establecido de leyes a nivel internacional y nacional que encarnan principios fundamentales basados en la protección de la privacidad, dentro de un marco internacional que tiende paulatinamente a reconocer la necesidad cada vez mayor de garantizar la protección de las personas en forma integral.

Esta toma de conciencia a nivel internacional ha hecho que muchos países hayan reconocido en su legislación el derecho a la protección de los datos personales y se hayan creado autoridades específicas en la materia a fin de llevar adelante las tareas de control.

El derecho a la privacidad nace en el derecho a estar sólo, a ser dejado sólo y a vivir la propia vida con un mínimo de interferencia, ya sea de otras personas o del propio Estado. Pero, ha sido el ver cómo los datos personales pueden ser utilizados de manera diabólica lo que permitió el reconocimiento de el derecho a la intimidad, a la privacidad y a la protección de los datos personales.

Alemania es uno de los países pioneros en la lucha por la protección de los datos personales.

En agosto del año 2011, el Centro Independiente para la Protección de la Privacidad (ULD) en Schleswig-Holstein, prohibió a todas las organizaciones del estado tener páginas de fans en Facebook y poner botones de “me gusta” en sus sitios en internet. La razón era simple: el Centro sostenía que los ciudadanos estaban siendo monitoreados sin que se dieran cuenta. Faltaba bastante para que se conocieran las revelaciones del ex agente Edward Snowden que reveló la forma de espionaje masivo llevado adelante por la NSA en Estados Unidos y otras agencias de seguridad del resto del mundo.

La lucha de Alemania contra los programadas de Google Street View también son de larga data. En el 2010 las autoridades en materia de protección de datos impusieron a Google la obligación de pixelar las imágenes de las personas y propiedades que aparecían en las fotografías tomadas desde los vehículos. Hubo incluso ciudades que no permitieron la circulación de los autos de GSV. En abril de 2011 Google dejó de tomar fotos en Alemania. Había recibido hasta ese momento al menos 250.000 peticiones de ciudadanos alemanes que pedían que sus imágenes o las de sus casas fueran retiradas del sistema.

Parece que Alemania no puede, ni debe, olvidar los archivos Stasi

Carsten Casper, analista de privacidad de la firma de investigación tecnológica Gartner, coincide en que la sombra de la Stasi, el órgano de inteligencia de la República Democrática Alemana, es un factor primordial en la lucha de Alemania por defender los datos personales.

“Durante casi 40 años, la gente estuvo bajo vigilancia y es obvio que esto pone a las personas muy nerviosas cuando se trata de la privacidad”, señaló a la BBC en el año 2011. “Esto no hace diferencia entre la privacidad física o de los datos. Todos estos temas están mezclados en la mente del público”.

La primera ley de protección de datos del mundo fue aprobada en el estado alemán de

Hessen en 1970 y la ley federal de protección de datos del país, la Bundesdatenschutzgesetz, está entre las más estrictas del mundo.

Facebook firmó un código de conducta alemán para firmas comerciales en internet con clientes jóvenes ya en el año 2011, sin perjuicio de lo cual criticaron duramente la posición de dicho país respecto al botón “me gusta” y sostuvieron en diversos medios que siempre respetaron la privacidad de los usuarios de internet alemanes.

Tanto Alemania como otros países de Europa y la Comisión Europea, han sido muy críticos con la forma en que el gobierno de los Estados Unidos accede a los datos de cualquier ciudadano del mundo, desde que Edward Snowden reveló la existencia de los programas de vigilancia masivos, en especial a partir de que se conoció que el espionaje llevado a cabo por la NSA incluyó las comunicaciones telefónicas de Angela Merkel. La canciller no se quedó atrás: propuso en febrero del 2014 la creación de una red de datos europea que evite el paso de las informaciones digitales por servidores norteamericanos. En un mensaje grabado y distribuido por internet sostuvo que empresas como Google y Facebook “almacenan informaciones allí donde la protección de datos está peor garantizada”.

Cuando se conoció la adquisición de WhatsApp por parte de Facebook, hace un año atrás, el responsable de la oficina de regulación de privacidad en las comunicaciones emitió un comunicado en el que desaconsejaba a los alemanes utilizar WhatsApp. La combinación en un mismo dispositivo del sistema de mensajería y de Facebook genera un altísimo nivel de desprotección para los datos contenidos en los teléfonos celulares actuales, por lo que las autoridades alemanas no dudaron en instar a la población a que no utilizara más los servicios de WhatsApp.

Hoy, 26 de febrero de 2015, sabemos que Tim Cook, CEO de Apple, se reunió con Angela Merkel hace unas horas. ¿Cuál fue el tema principal del encuentro? Seguridad de la información, privacidad y protección de los datos personales de los ciudadanos. Hace poco tiempo, en una cumbre de seguridad de la Casa Blanca, Cook destacó que “la historia nos ha demostrado que sacrificar nuestro derecho a la intimidad puede tener graves consecuencias”.

Las graves consecuencias ya las hemos visto a lo largo de la historia. Poner los ojos en el pasado a veces no es una pérdida de tiempo, nos sirve para entender la esencia humana, comprender los hechos e intentar que algunas historias y dolores no se repitan más.

Inés Tornabene

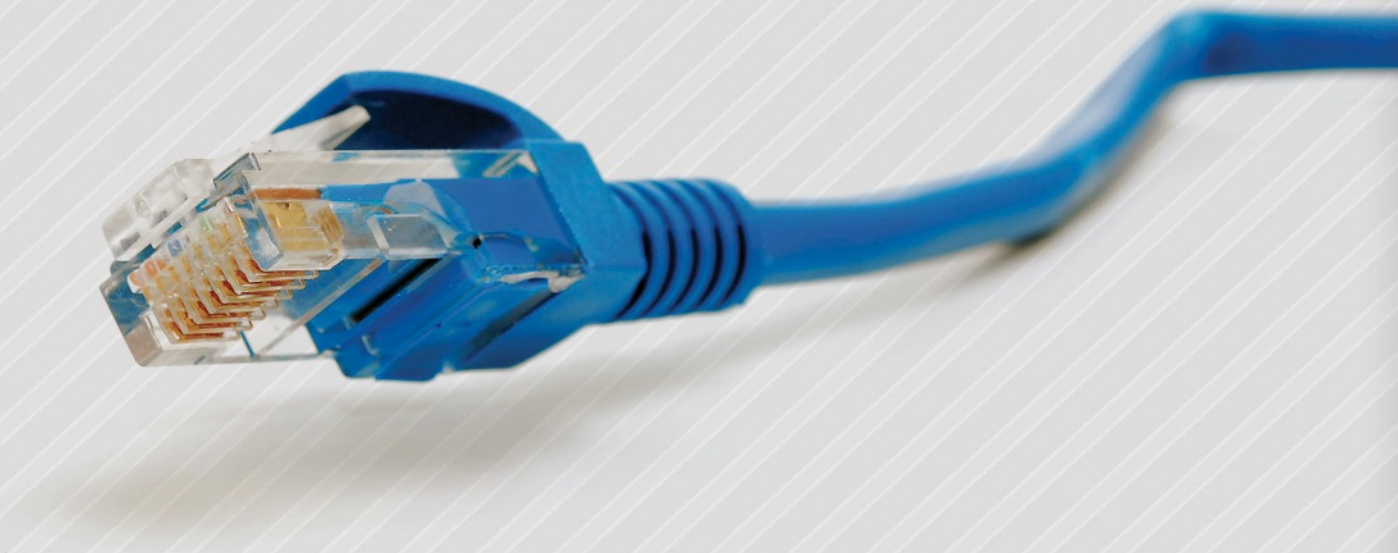
Fuentes consultadas:

The Washington Post, vía Clarín, publicado el 13.02.2001,http://edant.clarin.com/diario/2001/02/13/i-02101.htm

BBC, De la experiencia nazi a Facebook: por qué Alemania cuida su privacidad, publicado el 10.09.2011,http://www.bbc.co.uk/mundo/noticias/2011/09/110910_facebook_alemania_privacidad_sao

EuropaPress, Google Street View “abandona” Alemania tras los problemas de privacidad, publicado el 11.04.2011, http://www.europapress.es/portaltic/internet/noticia-google-street-view-abandona-alemania-problemas-privacidad-2011041111 4948.ht ml

http://www.adiar.org



ADIAr

Asociación de Derecho
Informático de Argentina

Una Asociación en todo el país

creciendo junto al derecho
informático desde el 2007

GOBIERNO

&

CUMPLIMIENTO

RESPONSABLE

ING FABIÁN DESCALZO

La gestión como apoyo al cumplimiento

Cada vez es más notoria la necesidad en empresas de diferentes sectores el contar con una gestión para el gobierno de la seguridad y la tecnología que acompañe a sus objetivos de negocio, ya que para alcanzar resultados no solo dependen de lo comercial sino también del cumplimiento regulatorio y normativo.

Habitualmente, y en cada caso en el que se debe dar respuesta a condiciones de cumplimiento por parte del negocio, uno de los principales puntos de control se refiere a los recursos tecnológicos y sus procesos asociados con los que se le brinda servicio a las diferentes áreas organizativas.

Debido a ello, lo que debe analizarse primero es nuestro modelo de negocio y conocer las regulaciones y normas internas para determinar si la gestión actual está alineada con los estándares del negocio, lo que nos dará como resultado el nivel de madurez en el gobierno aplicado a los procesos tecnológicos y si los mismos cubren los requerimientos de cumplimiento de las regulaciones que le aplican a la organización. Recordemos que un buen gobierno de las tecnologías y su aseguramiento permiten a las organizaciones brindar servicios de calidad y evitar el impacto negativo interno y externo proveniente de la falta de cumplimiento de leyes, regulaciones o certificaciones adquiridas por el negocio.

Este ejercicio inicial, normalmente llamado “Assessment”, nos permite identificar la brecha a remediar para alcanzar el nivel de cumplimiento requerido y es una herramienta fundamental en la mejora de los sistemas de gestión permitiéndonos ajustar las definiciones de base que nos aseguren la condición de "Compliance" con el marco regulatorio, legislativo y las políticas internas de la organización incluyendo las condiciones contractuales de seguridad, control y auditoría con terceras partes.

Para completar un plan orientado a desarrollar un entorno estratégico de gestión, debemos considerar una serie de acciones orientadas a la identificación de riesgos teniendo en cuenta los recursos tecnológicos utilizados en los procesos de negocio y el tratamiento variado sobre los distintos tipos de información que hace que su sensibilidad pueda variar significativamente. De esta forma y ya conocidas las condiciones de riesgo y cumplimiento, podremos establecer procesos funcionales y de servicio tecnológico protegidos y pensados a la medida de nuestra empresa mitigando los riesgos potenciales que, en caso de materializarse, impacten negativamente en la organización si no remedio la brecha de cumplimiento detectada.

Todo sistema de gestión debe estar documentado, y los documentos que registran definiciones normativas, procedimientos operativos y estandarizan los aspectos técnicos relacionados con los parámetros de configuración también deben ser verificados, para garantizar que desde las normativas compiladas en una biblioteca de documentos que conforman el marco normativo de la organización se da respuesta al marco regulatorio en forma adecuada según el tipo de industria, acorde a la dimensión de la empresa y basado en la operación de los procesos soportados por servicios tecnológicos.

El implementar un sistema de gestión es una decisión de negocio, pero lo que debe entenderse es que el compromiso a asumir por el negocio puede tener dos visiones diferentes:

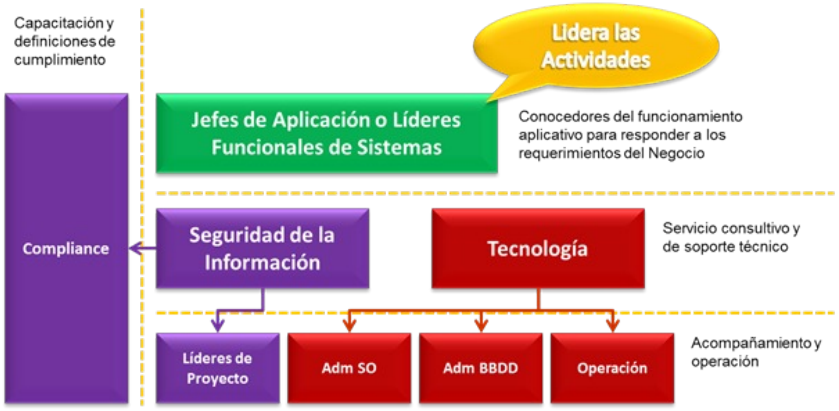
1. **Compromiso y delegación**, cuando se toma la decisión pero todas las responsabilidades son derivadas en áreas de Organización y Métodos,

Sistemas o Seguridad de la Información poniendo en cabeza de estas áreas responsabilidades de peso y comunicación que le son propias de la Dirección.

2. **Compromiso y acompañamiento**, obviamente cuando la Dirección asume su compromiso por completo a través de sus comunicados y apoya las acciones de las áreas implementadoras.

Normalmente los hechos se inclinan por la primera visión, y se podrá ver claramente cuando aquellas tareas que hayamos planificado para cada una de las actividades empiezan a dilatarse en el tiempo debido a falta de colaboración interna, demoras en la aprobación de presupuestos o en la toma de decisiones, etc. El no contar con el acompañamiento adecuado de la Dirección impacta directamente sobre el ánimo de colaboración del principal recurso de cualquier sistema de gestión, el humano.

Pensémoslo de esta forma, año a año la Dirección define objetivos estratégicos relacionados con una mejora en la rentabilidad de las operaciones empresariales como respuesta a sus accionistas, y en muchas oportunidades la concreción exitosa de estos objetivos está relacionada con una decisión propia de adoptar un estándar (como puede ser el certificar ISO 9001) o bien establecer políticas orientadas a reforzar el cumplimiento regulatorio asociado a su negocio (como pueden ser las normativas del BCRA, el estándar PCI, o leyes como SOx o HIPAA). Entonces ¿Porque no apoyar nuestras propias decisiones?



Para asegurar el adecuado funcionamiento de un sistema de gestión que cubra las necesidades de cumplimiento de nuestra organización, necesitamos que toda la organización entienda por qué y para qué interviene en el proceso. Tengamos en cuenta que el entendimiento es algo progresivo y que fluye desde la aceptación como propio de cada etapa del sistema de gestión. Si no se crea un ambiente colaborativo es muy difícil de hacer que se entienda y para que ello suceda necesitamos el acompañamiento de aquellos que tomaron una decisión estratégica para el negocio.

Esto denota que entre otra de las claves para asegurar el cumplimiento, es el contar con recursos humanos capacitados no solo técnicamente sino también en el entorno de la organización y sus procesos, para lo cual debemos establecer condiciones estándar de concientización y trabajo en equipo interdisciplinario, estableciendo actividades que acompañen cada etapa del sistema de gestión adoptado.

A todo esto debemos tener en cuenta que el organizarse a través de estándares siempre trae acarreado algún tipo de conflicto interdepartamental ya que cuando tenemos por objetivo adecuar y normalizar procesos, esto implica redefinir roles y responsabilidades, crear nuevas áreas, fusionar otras, cambio de personal, modificar permisos y accesos, etc. Por ello es muy importante la comunicación y la motivación, ya que se requiere trabajar con el miedo y los sitios de confort utilizados por los empleados hasta este momento; cambiar su realidad y modificar sus costumbres no es tarea fácil.

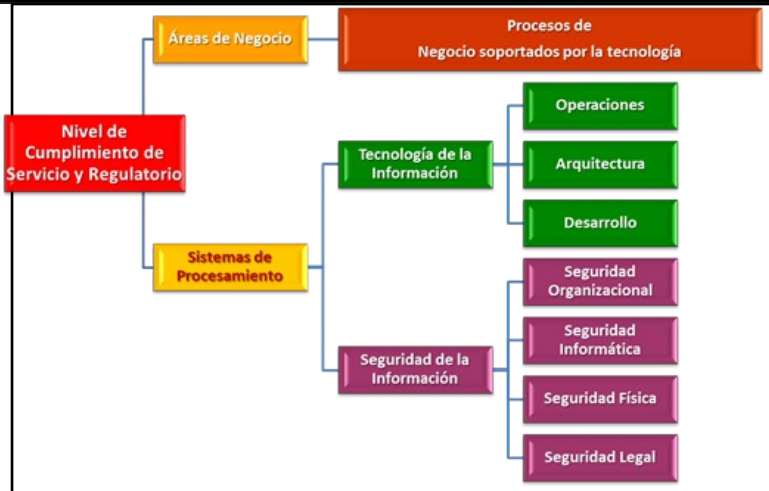
Como podrán haber visto, en lo planteado hay un estricto sentido de dirección en integrar diferentes actividades enfocándolas hacia la concreción de un sistema de gestión desde el aspecto del cumplimiento, ya que a partir de ello conseguiremos encausar cada necesidad de implementación tecnológica no como un proyecto individual para resolver una situación puntual de un área de negocio sino como una herramienta de solución a procesos de tratamiento de información y alcance exitoso de objetivos de negocio.

EL POSGRADO

ORGANIZA RED IBEROAMERICANA
ELDRECHOINFORMATICO.COM

DOCENTES:
LAINE SOUZA - JOEL GOMEZ TREVIÑO - CARLOS D. AGUIRRE - HORACIO FERNANDEZ DELPECH - ALVARO A. SOTO - MARTÍN BARRANDEGUY - ELISABETH BOUVIER - INÉS TORNABENE - CARLOS REUSSER MONSALVEZ - IVAN MARRUGO JIMENEZ

aula.elderechoinformatico.com



Bajo este contexto, la premisa más importante es la de establecer un gobierno que permita administrar los diferentes procesos tecnológicos y de seguridad de la información para garantizar que el uso de las tecnologías cumple con los objetivos éticos y legales requeridos por la organización. Esto nos llevará a primeramente a interpretar cada una de las leyes de aplicación para de esta manera adecuar nuestros sistemas a las necesidades de cumplimiento.

Otra de las actividades fundamentales corresponde al proceso de gestión de la auditoría interna para obtener información sobre el funcionamiento del sistema de gestión implementado y su nivel de madurez. Para ello, se debe planificar, establecer, implementar y mantener un programa de auditoría, incluyendo la frecuencia de las mismas, los métodos a utilizar, responsabilidades, requisitos de planificación e informes. De este proceso es esencial asegurar que los resultados se reportan a la dirección para su revisión.

¿Por qué darle importancia a un sistema de gestión como respuesta a las necesidades de cumplimiento? Porque es la única forma de:

- Establecer pautas documentadas, estandarizadas y medibles de la operación de los diferentes servicios tecnológicos que brindan el soporte al negocio necesario para alcanzar sus objetivos estratégicos.
- Garantizar transparencia en el tratamiento de la información y su comunicación cuando los datos confidenciales y sensibles a las personas y las organizaciones se sometan al tratamiento de forma automatizada, implementando medidas técnicas y organizativas que garanticen un nivel de seguridad adecuado en relación con los riesgos en el tratamiento y la naturaleza de los datos.
- Permitir una evaluación de los riesgos para adoptar medidas de protección de los datos contra su destrucción accidental o ilícita, o su pérdida accidental, y de impedir cualquier forma de tratamiento ilícito, en particular la comunicación, la difusión o el acceso no autorizados o la alteración de estos datos.
- Especificar conformidad en los criterios y condiciones aplicables a las medidas técnicas y organizativas para sectores específicos y en situaciones de tratamiento de datos específicas, habida cuenta en particular de la evolución de la tecnología y de las soluciones de privacidad desde el diseño y la protección de datos.

Fabián Descalzo
Gerente de Governance, Risk & Compliance
Cybsec S.A. – Security Systems

Es Gerente de Governance, Risk & Compliance (GRC) en Cybsec S.A., Certificado como Director en Seguridad de la Información (U-CAECE), instructor certificado ITIL Fundation v3-2011 (EXIN) y auditor interno ISO 20000 (LSQA-Latu).

Especialidades: Desarrollo e implementación de Políticas, Normas y Procedimientos; Estándares de seguridad física, electrónica y lógica; Auditoria de Seguridad de la Información; BCRA A4609 y A5374, SBIF (Chile), SBS (Perú), PCI-DSS, COBIT, Habeas Data Regional, SOX (Sarbanes-Oxley), Especialista en procesos de gestión de seguridad (ISO27000), procesos de gestión de IT (ISO20000), gestión de análisis de riesgos y Continuidad de Negocio (BCM/DRP/BCP). Dirección y coordinación de proyectos con personal propio y de terceros.

ENTREVISTA

H.C.B

Pág. 42

HUMBERTO CARRASCO BLANC

ABOGADO - 41 AÑOS - CHILENO - CO FUNDADOR DE ADI CHILE - SECRETARIO LACRALO

“A mi juicio, el abogado que sea experto en temas de video juegos tiene un futuro prometedor… “

1 - Ud. es un Abogado chileno, capacitándote en Europa, que diferencias encuentra entre la visión del derecho informático entre Latinoamérica y Europa?

La verdad es que la pregunta es un poco amplia y de alguna forma contestarla implica asumir un conocimiento casi acabado de lo que constituye derecho informático en Latinoamericano y en Europa. No es este mi caso y lejos podría declararme experto en el derecho informático de ambos continentes. Sin embargo, si he tenido la suerte de poder investigar en temas de derecho informático respecto de varios países de Latinoamérica y Europa, lo que me permitiría al menos esbozar una opinión sobre lo que se me pregunta.

La gran diferencia deriva del Tratado de Funcionamiento de la Unión (TFUE) y las directivas europeas que hacen que de alguna forma el tratamiento de temas relacionados con tecnologías sea más uniforme que lo ocurre en latinoamericana. Un buen ejemplo lo constituye el tratamiento de la protección de datos personales, donde en general la normativa y los reguladores europeos tienden a tener mayor homogeneidad. No ocurre lo mismo en Latinoamérica. Es posible encontrar diferencias notables en su tratamiento en los distintos países. Esta sería la situación de Argentina y Chile. El modelo chileno no tiene un regulador en materia de protección de datos a diferencia del modelo argentino.

Me gustaría hacer una acotación final en este punto. Hay que tener claro que no es universalmente aceptado el término derecho informático. En la lengua anglosajona se llama Information Technology Law, o Internet Law, entre otras denominaciones. En español también se conoce como derecho de las tecnologías de la información o derecho de Internet. Sin embargo, en forma pragmática todas estas expresiones pueden ser usadas como sinónimos.

2 - Cuales le parecen que son los temas que más desarrollo van a tener en materia jurídico/tecnológica a futuro? Porque?

A mi juicio, el abogado que sea experto en temas de video juegos tiene un futuro prometedor. Todas las aplicaciones que se hacen para Apple App Store o Google Play

deben ser revisadas por un abogado. Sin miles los programadores que quieren publicar sus aplicaciones aquí. Aquí se encontrarán con problemas de derechos de autor, software, marcas, temas laborales, tercerizaciones, privacidad de datos, redacción de condiciones generales de contratación, etc. A mi juicio, es una de las labores más interesantes actualmente y en el futuro para los abogados interesados en temas de derecho informático.

3 - Actualmente se desempeña como Secretario de Lacralo. Podría explicar brevemente que es Lacralo y que función cumple?

LACRALO es una organización regional que está formada por estructuras de alcance (ALSs) de América Latina y el Caribe, acreditadas por ALAC (que es el Comité Asesor At-Large). Tiene por objeto asegurar y promover la participación de los usuarios de la región en los procesos de desarrollo de políticas de ICANN.
En términos más simples LACRALO busca representar los intereses de los usuarios finales de nuestra región en ICANN y tratar de lograr que estos intereses sean reflejados en las políticas de ICANN.

4 - Considera que internet debe estar regulado? porque?

Esta es una pregunta de mucha complejidad. Primero que todo yo tengo una visión positiva de la regulación. Segundo, hay que distinguir que es lo que hay que regular de Internet. Sus actividades están reguladas por las leyes nacionales de cada estado. Otra cosa es la efectividad de su regulación o su cumplimiento. Siempre hay conductas que merecen de regulación especial, en particular en el ámbito de la ciberdelincuencia. Ahora, otra cosa dice relación con la gobernanza de Internet que es un tema aparte. La gobernanza de Internet en términos generales es el desarrollo y aplicación por los gobiernos, el sector privado y la sociedad civil, en las funciones que les competen respectivamente, de políticas públicas que configuran la evolución y utilización de Internet. Lo que caracteriza la gobernanza de internet es la interrelación de diversos grupos de interesados como iguales. Todo lo anterior es regulación.
¿Necesita Internet ser regulado? Mi respuesta final es Si.

5 - Que visión tiene de las políticas que tienen grandes empresas como google o facebook en materia de privacidad?

Honestamente, no las he revisado en detalle como para poder emitir un juicio sobre ellas. Sin embargo, he leído algunas tesis y artículos que señalan que sus políticas violan legislación de datos personales en varios países. Incluso, en la actualidad existe una demanda colectiva en Europa en contra de Facebook por violaciones a la privacidad que se presentó el

mes de marzo del 2015 y que tendrá su primera audiencia el día 9 de abril. Esta es la demanda colectiva más grande de Europa que agrupa a 25mil usuarios y que podría costarle a Facebook 14 millones de dólares en pago de daños causados a los usuarios, por violación del llamado acuerdo de puerto seguro que protege la privacidad de los ciudadanos de la UE. Yo creo que el respeto de la legislación de privacidad de datos se hace mediante el ejercicio de acciones en los respectivos países donde se vulnera la privacidad.

6 - Cuando descubrió al derecho informático, y como fue ese descubrimiento?

Es una pregunta muy buena. Cuando estaba pensado en que escribir mi tesis de pre-grado, me dije "voy a escribir sobre algo que no hay escrito mucha gente y que me permita hacer algo que pueda publicar como libro". Así fue como llegue al derecho informático y publique mi tesis titulada "Contratación electrónica y Contratos Informáticos" como libro en el año 2000. Debo confesar que le debo mucho al derecho informático, no sólo desde el punto de vista intelectual, sino que me abrió la puerta para conocer una gran cantidad de colegas interesados en los mismos temas, muchos de los cuales terminaron siendo grandes amigos hasta el día de hoy.

7 - Que se extraña más de Chile?

De Chile, extraño la familia, los amigos, el mar, la cordillera y la patagonia. También extraño mi casa porque es un lugar donde me podía reunir con amigos a compartir buenos momentos y conversaciones, vino y asados.

8 - Considera que es necesario un replanteo sobre las regulaciones en materia de propiedad intelectual y tratamiento de datos personales?

En términos generales, considero que es necesario preparar regulaciones en estas materias que sean capaz de adecuarse a los cambios de la tecnología, de forma que no sea necesario modificar permanentemente estas normas. Por ejemplo, en materia de derechos de autor, tengo la convicción que el modelo de negocios tradicional que existía antes de la digitalización no tiene sostenibilidad en la práctica hoy en día. Esto por la facilidad de copia de la música o libros. No solo se debe cambiar las normas, también se deben adaptar los modelos de negocios a las nuevas realidades.

9 - Que consejos les daría a colegas que comienzan a incursionar en la temática?

Que si comienzan a interesarse y les gusta la materia, no duden en persistir en el estudio. Con ello, no solamente me refiero al estudio personal, sino que traten de hacer cursos de post-grado en la materia con el objeto de estar mejor preparados para defender a sus clientes. No hay que parar nunca de estudiar. Esto es una premisa para todo el estudio del derecho, pero en el derecho informático con mayor razón aun, debido a la velocidad en las innovaciones tecnológicas.

GRACIAS HUMBERTO!!!