Secciones

Inés Tornabene
Franco Vergara
Jorge G. Obregón
Fabián Descalzo

Colaboran

Nelvys Mendoza Gurdián.
Ana María Mesa Elneser
Francisco Calero

Revista Digital

ElDerechoInformatico.com

# 21 EDICIONES

## Ahora somos mayores de edad

### Esa cosa de la edad adulta... (o no)

Julio Nro 21

ElDerechoInformatico.com
Colombia

# II FORO EN DERECHO INFORMÁTICO

II Foro en Derecho Informático y Nuevas Tecnologías: "Derecho informático, informática forense, seguridad informática y protección de datos".

Medellín / Colombia

Del 10 al 12 de Septiembre

UNIVERSIDAD AUTÓNOMA LATINOAMERICANA-UNAULA

## 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**
**El Consultor en Seguridad Informática: Esp. Franco** Vergara

## Ilustración de Tapa

**El Número 21**
**Al cual estamos muy agradecido por su apareción**

## Contenido:

# EDITORIAL

Llegamos a las 21 ediciones, nos hicimos grandes y no se imaginan el esfuerzo que nos llevó.-

Por suerte los amigos nos siguieron acompañando con su material increíble, y no nos faltaron eventos que mostrar y material que brindar, solo que a veces la inspiración no llega y cuesta más que de costumbre. Poco a poco nos fuimos consolidando, y ya contamos con 4 secciones estables, nunca voy a terminar de agradecer a Inés Tornabene, Jorge Garcia Obregón, Fabián Descalzo y la última incorporación Franco Vergara, número a número nos dejan data increible y trabajos más que interesantes.-

Hay un agradecimiento especial a dos personas increíblemente generosas y maravillosos seres humanos **Gabriela Hormaizteguy y Elisabeth Bouvier**, nuestras Corresponsales en Uruguay, que organizaron un ENCUENTRO DE DERECHO INFORMÁTICO Y NUEVAS TECNOLOGÍAS impresionante!! (En días más sale un suplemento de esta edición con todas las ponencias y fotos por supuesto). El evento fue nuestra primer experiencia fuera de Argentina y no puedo estar más orgulloso, Paulina Casares Subia de Ecuador, Carlos Reusser y Lorena Donoso de Chile y brillantes colegas de Uruguay como Javier Wortman, Graciela Cami, Laura Nahabetian, Alejandrina Sande, Claudia Pereiro, Agustín Montemuiño, Veróica de Muro y el Maestro Marcelo Bauza fueron nuestros lujosos ponentes .-

Se viene nuevo diseño del sitio, II FORO EN COLOMBIA con nuestra corresponsal Ana Mesa Elneser como Anfitriona en Medellín, avances en el posgrado, en fin, todas esas cosas que nos van a hacer seguir creciendo, más todavía ahora que somos mayores de edición…

# Propiedad Intelectual en el ciberespacio: aciertos y desaciertos.[1*]

**LIC. NELVYS MENDOZA GURDIÁN.**
*Asesora Jurídica.*

***RESUMEN:*** *Los procesos contemporáneos de informatización y digitalización han revolucionado los medios tradicionales de transmisión del conocimiento, diversificando las posibilidades de creación, acceso e intercambio de contenidos con medios digitales. Estas facilidades han creado un estado de vulnerabilidad para los usuarios y creadores que convergen en la trama de las tecnologías y la información digital, especialmente en el caso de la gestión de la Propiedad Intelectual. La problemática radica en que las aplicaciones de las tecnologías han abierto brechas para la distribución indiscriminada de contenidos, la carencia de control en su utilización, la modificación arbitraria de las creaciones, la nulidad de los mecanismos de retribución y la vulneración de derechos morales y patrimoniales sobre las creaciones. Derecho, Propiedad Intelectual y tecnologías e información digital se encuentran en la disyuntiva entre el imperativo de acceso de la sociedad al conocimiento (Derecho de la Cultura) y el monopolio legal de los creadores sobre sus creaciones (Propiedad Intelectual). Es necesario examinar los mecanismos y alternativas de que disponen la sociedad y los creadores para entablar un marco legítimo de producción y utilización del conocimiento, aun cuando un entorno informatizado pueda dificultar ese fin.*

***PALABRAS CLAVES:*** *Derecho, Propiedad Intelectual, Derecho de autor, Tecnologías, Información Digital.*

***ABSTRACT:*** *The contemporary processes of computerization and digitization have revolutionized traditional means of transmission of knowledge and information, diversifying the possibilities of creation, access and exchange of digital media content. These facilities have created a state of vulnerability for users and developers converging on the plot of te ch*

*nologies and digital information, especially for the management of Intellectual Property. The problem is that the applications of technologies have opened up gaps for the indiscriminate distribution of content, lack of control in use, the arbitrary modification of the creations, the invalidity of compensation mechanisms and the violation of moral and economic rights on creations. Law, Intellectual Property and technologies and digital information are in the dilemma between the imperative of access to the knowledge society (Cultural Rights) and the legal monopoly of creators on their creations (Intellectual Property). It is necessary to examine the mechanisms and alternatives available to the society and creators to engage in legitimate framework of production and utilization of knowledge, even if a computerized environment can hinder this purpose.*

***KEYWORDS:*** *Laws, Intellectual Property, Copyright, Technologies, Digital Information.*

**SUMARIO: 1. El conflicto de la protección de la Propiedad Intelectual frente a las Tecnologías y la Información Digital. 2. Principales problemáticas. 3. A modo de epílogo.**

[1] *Este trabajo constituye un fragmento de la conferencia presentada por la autora en el VI SEMINARIO INTERNACIONAL SOBRE PROPIEDAD INTELECTUAL, efectuado del 15 al 17 de octubre del 2014 en La Habana, auspiciado por la Unión de Juristas de Cuba y la Organización Nacional de Bufetes Colectivos de Cuba.

## 1. El conflicto de la protección de la Propiedad Intelectual frente a las Tecnologías y la Información Digital

Los productos intelectuales relacionados con la educación, la cultura y la información se fundaron originalmente en soporte impreso, fonográfico, audiovisual, radiofónico y televisivo. En nuestros tiempos los periódicos, las revistas generales y especializadas, las publicaciones gubernamentales, las investigaciones y trabajos científicos, la información bursátil y cambiaria, las obras literarias, las emisiones de radio y televisión, la música, las imágenes de aplicación industrial o comercial, las obras plásticas, las obras pertenecientes a museos y colecciones privadas, las producciones cinematográficas y todos los demás productos del intelecto humano, se encuentran almacenados y accesibles en la gran urdimbre del ciberespacio.

Ante esta realidad, en 1996 fueron aprobados los Tratados de la OMPI sobre *Internet* (WCT y WPPT), con lo que se sentó internacionalmente la necesidad de proteger la Propiedad Intelectual en el ámbito digital. En estos tratados se estableció el alcance de la protección a los titulares de los derechos dentro del entorno digital y los derechos exclusivos como el derecho de distribución, de alquiler, de comunicación al público de una obra y de puesta a disposición del público de una interpretación o ejecución sonora.Además, se estudió la aplicabilidad de los derechos de reproducción al nuevo entorno y sus posibles limitaciones. Igualmente, se garantizó el derecho exclusivo de autorizar la reproducción directa o indirecta de las interpretaciones o ejecuciones fijadas en fonogramas (o los fonogramas) por cualquier procedimiento o forma a los intérpretes o ejecutantes y productores de fonogramas. Sin embargo, no se estipuló la posibilidad de limitar estos derechos y permitir formas transitorias o accesorias de reproducciones provisionales. No obstante, se consintió la posibilidad de prever en las legislaciones nacionales, limitaciones o excepciones impuestas a los derechos concedidos a los autores de obras literarias o artísticas en casos especiales que no menoscabaran su explotación normal ni causaran un perjuicio a los intereses legítimos del autor y se contempló la probabilidad de permitir la aplicación, ampliación e introducción de estas limitaciones al entorno digital en las legislaciones nacionales.

En sentido general, estos tratados establecen un marco difuso sobre la adopción de nuevas limitaciones de los derechos o la adaptación de las limitaciones existentes al entorno digital en pos de un mejor acceso a la información. Las consecuencias internacionales de estas legislaciones pueden verse en el caso de Estados Unidos, donde fueron incorporados los Tratados de la OMPI sobre *Internet* mediante la aprobación del DMCA de 1998, aunque sin implicaciones de introducción de nuevas limitaciones sobre Derecho de Autor. Asimismo, Japón revisó la Ley sobre Derecho de Autor en 1999 para impedir acciones encaminadas a eludir las medidas tecnológicas de protección y la eliminación o alteración de la información para la gestión de los derechos. Un caso más ilustrativo es el de Australia donde el Parlamento aprobó el CADAA 2000. Esta enmienda, encaminada a aplicar los Tratados

de la OMPI sobre *Internet*, introdujo un derecho neutro de comunicar obras literarias, dramáticas y musicales al público en el entorno de las tecnologías. Este derecho, a diferencia del caso estadounidense y japonés, modificó diversas limitaciones del Derecho de Autor a fin de hacerlas aplicables al entorno digital y consagró la protección de la puesta a disposición de obras en línea.

## 2. Principales problemáticas

Esa situación de incertidumbre legislativa se ha reflejado en la práctica con múltiples ejemplos de la colisión entre la Propiedad Intelectual y las tecnologías. En primer lugar, se esboza el ejemplo de las bibliotecas como encargadas de suministrar información al público a través de catálogos, bases de datos y otras fuentes.En este plano, los medios digitales han resultado de provecho en la prestación de los servicios de las bibliotecas, lo que ha traído consigo dificultades para la Propiedad Intelectual.

La entrega electrónica de documentos, la realización de copias electrónicas del contenido y la digitalización del material protegido por la Propiedad Intelectual, han despertado suspicacias en los legisladores de la materia que consideran que las limitaciones a estos derechos pueden no ser aplicables en todos los casos. En este particular, es de considerar que la diferenciación debe atenderse con respecto al acceso al material y su comercialización en el entorno digital. Estas circunstancias han generado que los titulares de derechos recurran a cláusulas y condiciones contractuales para delimitar el alcance de las facultades de las bibliotecas y archivos sobre el material protegido o las licencias que obtienen.

Un paso de avance lo constituye el ya mencionado CADAA 2000, habida cuenta de que permite, a las bibliotecas y archivos, digitalizar y comunicar material protegido por el Derecho de Autor. Esta normativa extiende las limitaciones existentes y crea excepciones nuevas aplicables al entorno digital en favor de las bibliotecas. En sus preceptos establece que sin pago o autorización, las bibliotecas y archivos pueden: copiar o transmitir el 10% de

una obra o de un artículo de una publicación periódica para atender una petición con fines de investigación o de estudio; copiar o transmitir electrónicamente una obra a un usuario para atender una petición con fines de investigación o de estudio o a otra biblioteca, en la medida en que el material no sea accesible de otro modo dentro de un plazo razonable y a un precio comercial ordinario; copiar y transmitir electrónicamente material de sus colecciones a funcionarios de la organización con fines de preservación o de administración interna ycolocar un material adquirido de forma electrónica a disposición del público dentro del recinto de la institución o en un terminal de

librería | hammurabi

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

**en preparación**

# Colección «elderechoinformático.com»


11 volúmenes

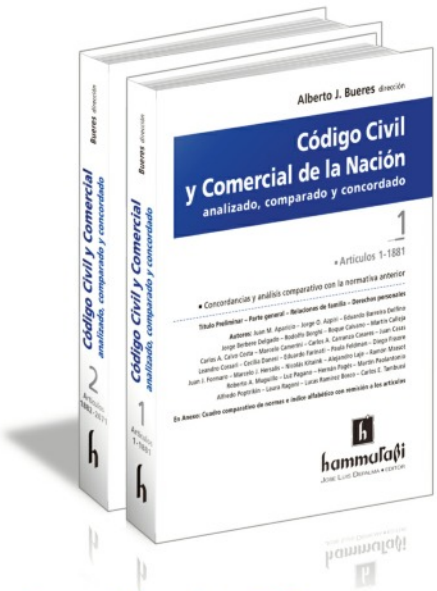
**Guillermo M. Zamora** dirección

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.

ordenador que no permita la reproducción electrónica o la comunicación electrónica.

Otro panorama se advierte en Estados Unidos, donde las actividades de préstamos entre bibliotecas están estrictamente reglamentadas y se rechaza la posibilidad de la transmisión digital de documentos. A este respecto, el DMCA sostiene la misma posición del artículo 108 de la Ley sobre Derecho de Autor de Estados Unidos, que condiciona los préstamos entre bibliotecas y la entrega de documentos a los siguientes requisitos: que la biblioteca o el archivo determinen previamente, sobre la base de una investigación razonable, la imposibilidad de adquirir por un precio racional la copia o grabación sonora de la obra protegida por el Derecho de Autor; que la copia o grabación sonora pase a ser propiedad del usuario y la biblioteca o el archivo no hayan tenido conocimiento de que la copia o grabación sonora se utilice para cualquier propósito que no sea el estudio privado, los conocimientos académicos o la investigación y que la biblioteca o el archivo coloquen una advertencia notable de Derecho de Autor en el lugar donde se reciben las solicitudes y la incluyan en el formulario de solicitud.

Un escenario similar se proyecta en el caso de los educadores y los investigadores, para quienes la tecnología digital juega un rol fundamental en sus labores. En este punto, los legisladores se acogen a una posición reservada con respecto a la extensión de las limitaciones vigentes del Derecho de Autor al ámbito digital, aunque con ello se beneficiarían actividades docentes e investigativas. Las principales causas de esta situación radican en el temor de los autores a que la libre utilización de las obras en el entorno digital perjudique su comercialización en línea.

Esto deriva en la posibilidad de que el amparo de las limitaciones facilite el plagio de contenidos y su comercialización ilícita sin incurrir en infracción legal y menoscabando el mercado de creaciones. Se sostiene la ya afirmada posición de encontrar un equilibrio entre los intereses de los autores, las industrias de la información y las instituciones educativas y de investigación. Esta pretensión ha afianzado la utilización de condiciones contractuales para buscar ese punto medio, aunque debería pensarse en incluir limitaciones justificadas para instituciones que utilicen la tecnología digital sin ser nocivas a la explotación normal de las obras protegidas o los legítimos intereses de los autores. Se impone relacionar algunas aristas de este punto con la protección de la Propiedad Intelectual. En esta dirección de estudio se señala que los programas de computación o ***Software*** son un conjunto de instrucciones expresadas mediante palabras, códigos o en cualquier otra forma que, al ser incorporadas en un dispositivo de lectura automatizada y traducidas en impulsos electrónicos, demandan la ejecución de una tarea o resultado por parte del ordenador, por lo que constituyen aportes de especialización, novedad y soluciones técnicas de creciente valor en el mercado intelectual y tecnológico. Las precitadas potencialidades del *software* lo han convertido en objeto recurrente de la piratería, la copia y la modificación ilícita por parte de un significativo número de usuarios que manipulan disímiles medios tecnológicos.

En este entorno se entabla el debate sobre la protección del *software* por la patente de invención o por la vía autoral. El resguardo por la vía de la *Patente* ofrece una protección sólida y exclusiva sobre la idea inventiva. Sin embargo, no todos los programas de computación cumplen suficientemente con los requisitos de novedad y de calidad inventiva exigidos por el patentamiento como vía de la Propiedad Industrial. Además, el derecho de patentes es territorial y se obtiene dentro de los límites de un país, por lo que para extenderlo a otros países se debe gestionar directamente en cada uno de ellos.

Por otra parte, la protección por el *Derecho de Autor* implica que la creación se encuentra protegida de forma universal desde su nacimiento, en virtud de lo que instituye el Convenio de Berna. La protección por vía autoral no requiere la revelación del programa fuente, aunqueadolece de la limitación de proteger únicamente la forma en que se expresa la idea y no la idea en sí. En conclusión, la protección debe extenderse a la expresión del programa, su estructura y la organización interna abarcando la forma y las ideas, ya que esta concepción inclusiva tiende a contrarrestar la ingeniería inversa (escribir un programa nuevo con instrucciones propias, en forma distinta del original, luego de haber descompilado el programa que se desea copiar).

Entre las herramientas de la informática y las telecomunicaciones se encuentran las ***Bases de Datos***, entendidas como un sistema de almacenamientoestructurado de datos conformado por un conjunto de registros donde se alojala información que debe manejar un programa de computación con el fin de recopilar, organizar y proteger el contenido. Las bases de datos pueden almacenar datos e imágenes factuales (informaciones puntuales y breves sobre aspectos de la realidad), datos e imágenes personales (información vinculada a personas físicas), obras (con la problemática de si las obras se encuentran en el dominio público o si aún se encuentra reservada su explotación al ámbito de su autor o sus derechohabientes), imágenes en movimiento no personales ni factuales y fragmentos sonoros. Estas facilidades la han convertido en una producción imprescindible en la gestión, análisis y procesamiento de información, utilizada frecuentemente con fines comerciales altamente lucrativos.

*Ab initio* el aspecto de la autoría de las bases de datos debe analizarse desde su fabricante, reconocido en la persona o personas naturales o jurídicas que realizan una inversión en la recopilación, ensamblaje, verificación, organización o presentación de las bases de datos. No obstante, se establece

una doble categoría de titulares que contempla de un lado los autores de las bases de datos que, por la selección o disposición desu contenido, constituyan una creación intelectual y los fabricantes de las bases de datos cuando la obtención, verificación o presentación de dicho contenido, representen una inversión sustancialdesde el punto de vista cuantitativo o cualitativo. En este acápite, se considera que el autor de la base de datos es la persona física o el grupo de personas físicas que haya creado dicha base o, cuando la legislación lo permita, la persona jurídica que dicha legislación designe como titular del derecho. En cambio, se

considera fabricante a quien ha realizado una inversión sustancial en laobtención, recopilación, ensamblaje, verificación y presentación del contenido desde el punto de vista cuantitativo o cualitativo.

El cúmulo de derechos que ostenta el fabricante sobre el contenido de la base de datos se integra porlas facultades de realizar, autorizar o prohibir actos de extracción y utilización o reutilización de la totalidad de las bases de datos o de una parte sustancial de su contenido. Mientras, el autor de la base de datos ostenta el derecho exclusivo a realizar o autorizar la reproducción temporal o permanente, sea total o parcial, por cualquier medio o forma; la traducción, adaptación, reordenación y modificación; la comunicación, exhibición o representación y toda reproducción, distribución, comunicación, exhibición o representación al público de los resultados. En estos casos algunas normativas contemplan la duración de la protección con un plazo máximo de 15 años, mientras que en otras legislaciones oscila hasta un plazo mínimo de 25 años, ambos a contarse a partir de la fecha de terminación de la fabricación o de publicación de la base de datos.

## 3. A modo de epílogo

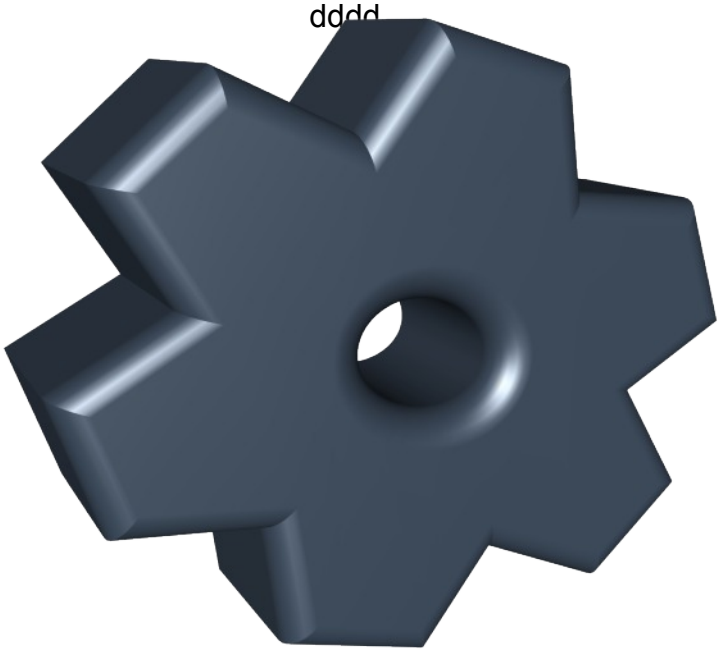
La proyección jurídica de estas circunstancias se evidencia en varios hechos. En un primer punto, los acontecimientos que ocurren en el ciberespacio desconocen los límites geográficos y carecen de vínculos que permitan su limitación en espacios físicos determinados, lo que dificulta la ubicación del lugar en el que los hechos suceden y el derecho aplicable. En un segundo punto, la red posibilita la realización de transacciones virtuales que pueden ser efectuadas simultáneamente por varios consumidores en diferentes lugares, con el riesgo que entraña la prescindencia de un

intercambio personal o del conocimiento de datos generales de la contraparte para la seguridad jurídica. Estas afirmaciones se han traducido en la latente posibilidad de un conflicto de leyes, el cuestionamiento de la efectividad de la protección y la complejidad de la localización de las infracciones a los derechos de propiedad intelectual. A ello se contrapone una serie de iniciativas para lasolución de conflictos en línea, la armonización de las legislaciones y la asimilación de la propiedad intelectual al entorno digital. Sin embargo, aún no se dispone de la infraestructura tecnológica necesaria para abordar en línea los litigios. Se puede concluir este análisis con la idea de que el goce de los derechos exclusivos, con cierta amplitud, por parte de los autores debe ser un presupuesto para la validez de limitaciones al ejercicio de esos derechos, fundado en el precepto cardinal de proteger, en circunstancias justas y equilibradas, el derecho de la sociedad a acceder y utilizar los contenidos.

**BIBLIOGRAFÍA**


4. **ÁLVAREZ NAVARRETE, LILLIAN**; *"Derecho de ¿Autor? El debate de hoy"*; Editorial de Ciencias Sociales, La Habana, 2008.
5. **BORGUES, CLARISA Y JULIO DÍAZ**; *"Derecho de cita en el ámbito de las humanidades y las ciencias sociales"*; Boletín Electrónico ABGRA (Asociación de Bibliotecarios Graduados de la República de Argentina), Año 3, No. 3, Septiembre, 2011.
6. **CÁCERES PRADO, JOSÉ ANTONIO**; *"Virus Informáticos ¿Cómo protegerse?"*; Editorial Científico-Técnica, La Habana, 2012.
7. **COLECTIVO DE AUTORES**; *"Selección de lecturas de Derecho de Autor"*; Editorial Félix Varela, Ciencias Jurídicas, La Habana, 2007.
8. **DÍAZ CABALLERO, JOSÉ RICARDO Y SANDRA ISAAC BORRERO**; *"¿Hacia dónde va la tecnología?"*; Editorial Científico-Técnica, La Habana, 2011.
9. **GENTA, MARIELA**; *"Etapas hacia las Sociedades del Conocimiento"*; Editorial UNESCO, Montevideo, 2008.
10. **FULLERTON, ANNE Y DAVID REINKING**; *"Equilibrar la titularidad y la utilización de las obras digitales: enfoque de una asociación profesional sin fines de lucro"*; Doctrina y opiniones, Boletín de Derecho de Autor, OMPI, enero-marzo, 2003.
11. **LIPSZYC, DELIA**; *"Derecho de Autor y Derechos Conexos"*; UNESCO CERLALC ZAVALIA, La Habana, Editorial Félix Varela, 1998.


dddd



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

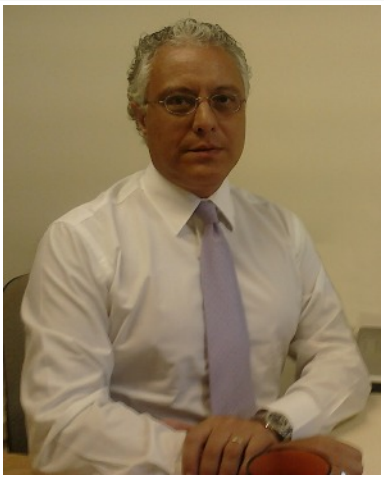
# GOBIERNO

# &

# CUMPLIMIENTO

RESPONSABLE

ING FABIÁN DESCALZO



# Fusiones y adquisiciones

***Cultura, gobierno y cumplimiento: Las necesidades del negocio y el riesgo de resistencia a los cambios organizacionales***

Si lo que la organización busca es beneficiarse con una fusión de empresas para disminuir los gastos de operación y/o producción y aumentar la rentabilidad ¿Porque no tener en cuenta el análisis previo de plataformas, aplicaciones y procesos tecnológicos que dan soporte al negocio, evitando así mayores costos en su remediación posterior por cuestiones regulatorias o generar nuevos expuestos de seguridad a sus procesos internos y a la información?

Hay dos condiciones que generan profundos cambios en la operación funcional y tecnológica de las empresas que hacen peligrar el gobierno de sus procesos internos: La adopción de nuevos estándares o regulaciones de negocios, y la adquisición o fusión de empresas. Ambas problemáticas responden a una acción decidida y planificada por la alta dirección y representada en el plan de negocios de la organización, pero los cortos tiempos de implementación resultantes de una baja coordinación desde el negocio con las diferentes áreas de servicio y soporte de la organización hace que los riesgos sobre el gobierno de las tecnologías y la falta de cumplimiento aumente.

Esta exposición que impacta negativamente sobre la gestión y seguridad de los procesos de negocio puede verse representada en fusiones o adquisiciones mal administradas que provocan, entre otros, los siguientes riesgos a los negocios:

Estratégico

- Incapacidad para manejar las expectativas de los inversionistas
- Fallas del gobierno corporativo y control interno
- Rechazo interno al marco regulatorio
- Acciones legales o punitivas por falta de cumplimiento al marco regulatorio
- Incapacidad para atraer y retener conocimientos y competencias durante la transición
- Bajo control de costos

Operativo y Cumplimiento

- Administración ineficiente o fallas en la prestación de servicios internos y externos
- Inversión ineficaz en la infraestructura con impacto negativo que la convierte en obsoleta o inadecuada
- Débil seguridad de los datos y riesgos de privacidad
- Riesgos en los procesos de servicio de TI y seguridad de la información
- Incapacidad de explotar y proteger activos (piratería y derechos de propiedad intelectual)

- Sistemas y procesos inadecuados para sustentar el negocio
- Aumento en las presiones regulatorias

Esta problemática abarca tanto a procesos funcionales como tecnológicos, partiendo de la base que hace a la cultura interna de toda organización y que establece las pautas para la gestión del negocio: las políticas y su entorno documental, y los usos y costumbres de las personas. Por ello cada vez que nos ha tocado el desafío de ayudar en una organización para adecuar sus procesos y procedimientos internos, ya sea de negocio o de servicios de tecnología y seguridad, nos hemos encontrado con las limitaciones propias del nivel de madurez de las mismas empresas que pretenden alinear sus procesos ante fusiones o adquisiciones poniendo en riesgo la calidad de sus servicios, la gobernabilidad de sus operaciones y la seguridad de la información que procesan.

Por ello, los riesgos mencionados no solo están relacionados con la **Confidencialidad**... Compatibilizar creencias, cultura, sistemas y mecanismos de transferencia puede afectar seriamente la **disponibilidad e integridad de la información** y por consecuencia afectar a la **CALIDAD** de los servicios o productos que ofrecemos, y por ende impactar negativamente en la **IMAGEN** de nuestra Compañía.

En respuesta a esta problemática debemos analizar cómo es que se ha desarrollado la cultura de cada una de las empresas involucradas en el proceso de fusión, y esto involucra el analizar como tratan y cumplen las personas con cada una de las políticas, normas y procedimientos, su entendimiento de las regulaciones y su nivel de compromiso en el cumplimiento, y cuál es su enfoque de acuerdo al grupo de interés que ocupe en la organización determinado por niveles de Dirección, Gerencial o Usuarios.

De esa forma podremos construir un modelo de comunicación para poder obtener el apoyo desde la Dirección y Alta Gerencia, la colaboración de los Usuarios y su compromiso con el proyecto, responsabilidad con la información brindada y eficiencia en su efectiva implementación. De por sí, ya sabemos que dentro de esos grandes grupos definidos como Dirección, Gerencias y Usuarios, los intereses de cada uno frente a una fusión son diferentes, por lo que establecer una forma de conectar cada área de interés es INDISPENSABLE en estas situaciones para la salud y sobrevivencia de una Organización.

Sabemos también que desde el negocio se deben tomar acciones coordinadas en cuanto a la preparación de nuestra organización para que responda en forma adecuada a los nuevos requerimientos planteados desde sus objetivos actuales. Para comunicar en forma clara estos objetivos debe entenderse que:

- **El Negocio** debe comunicar cuáles son sus futuros objetivos, para conseguir el

soporte necesario por parte de la Organización, ya sea desde sus áreas administrativas como de sus áreas tecnológicas.

- **La organización**, desde las diferentes áreas brindará el soporte necesario acorde a los requerimientos del Negocio.

¿Que tener en cuenta entonces? Primordialmente, reconocer y conocer cuáles son los requisitos normativos y regulatorios que impactan en el proyecto de fusión como consecuencia de la unión de ambas empresas, y a partir de allí establecer equipos interdisciplinarios que nos permitan analizar en forma integral todos los aspectos que hacen que nuestro negocio sea exitoso a partir del tratamiento y procesamiento de la información. Áreas comerciales, legales, administrativas, tecnológicas y de seguridad de la información pueden ser los principales actores para definir en forma adecuada para el esclarecer el nuevo entorno del negocio.


Ante una fusión o asociación de empresas debemos pensar que para asegurar cada uno de los procesos de negocio resultantes, sobre todo aquellos que surjan nuevos o adecuados a la nueva organización, deben ser alineados siguiendo los siguientes conceptos:

1. Entender que la buena comunicación interna aporta un valor positivo (más que agregado) para cumplir objetivos regulatorios del negocio, claridad en los requerimientos operativos del Negocio y sus procesos manuales y tecnológicos y facilitar la coordinación de los diferentes equipos al establecer roles específicos ante proyectos de respuesta al Negocio.

2. Promover con el apoyo de la Alta Gerencia esta comunicación, para que desde cualquier área de la organización puedan establecerse ambientes colaborativos con pautas claras y roles definidos que aporten a la concreción de los objetivos establecido por el Negocio durante todo el proceso de fusión.

3. Analizar cada uno de los procesos de uno y otro lado, para poder identificar posibilidades de integración o riesgos de posibles conflictos. Esto nos permitirá obtener las herramientas necesarias para conseguir una mejora de nuestro Negocio desde la integración, y las respuestas correctivas para resolver inconsistencias

4. Al iniciar el proyecto identifique una fase de capacitación para el entendimiento de la operación, identificación de intervinientes, alcances y roles dentro del

proyecto, necesidades de cumplimiento legal y de negocio, y fundamentalmente las necesidades de servicio por parte de las áreas tecnológicas (IT, redes, comunicaciones) y de seguridad (seguridad de la información, o bien seguridad física y seguridad informática).

5. Si bien integrar la cultura de distintas organizaciones siempre es un desafío que afecta en forma directa al negocio, recordar y no perder de vista nuestras políticas debe servir para repasar la documentación asociada a cada uno de los procesos, identificar aquellos “puntos a cubrir” que surgen de los cambios, y establecer la actualización adecuada para la capacitación de cada uno de los integrantes de la organización basados en el entendimiento y la comunicación para reforzar nuestra cultura interna en su nuevo entorno.

6. Todas las aplicaciones deben ser previamente analizadas, teniendo en cuenta su administración, operación y control, entradas y salidas de información, posibilidades de importación y exportación de datos, compatibilidad de software de base y posibilidades de upgrade, interfaces existentes y la posibilidad de crear nuevas, haciendo que se mantenga la DISPONIBILIDAD e INTEGRIDAD de la información y CONTINUIDAD de procesamiento.
7. Todo el equipamiento debe ser previamente analizado para revisar su dimensionamiento respecto a las nuevas necesidades del Negocio, establecidos sus estándares de configuración de acuerdo a lo indicado por los requisitos regulatorios y normativos e identificar en forma correcta estos componentes dentro de cada uno de los procesos para asegurar protección al Negocio desde la infraestructura de los servicios de IT.

Cada uno de estos aspectos deben ser analizados por un equipo interdisciplinario desde el principio de las negociaciones; esto permitirá que podamos establecer los alcances de impacto en nuestra organización, medir los esfuerzos y establecer la disponibilidad de los recursos financieros, económicos y operativos, establecer las medidas necesarias para mitigar los riesgos de seguridad e integridad de la información, planificar en forma adecuada las futuras implementaciones estableciendo fechas y prioridades acorde a los resultados esperados

por el Negocio.

El resultado de esta “sinergia” generada desde la Alta Dirección al propiciar la participación efectiva de los referentes de cada área permitirá que su plan de negocio sea más sólido en su estrategia, recordando que las áreas de **seguridad y tecnología** son parte de ese **plan** en el marco empresario actual, brindando a través de ellas **calidad y gobernabilidad** sobre todos los servicios de IT.

¿A que debemos estar atentos en la transición?

1 Establecer auditorias para la verificación de cumplimiento con el compromiso de seguridad y tratamiento de la información, acorde a la Política de Seguridad de nuestra organización, así como la aceptación de la política mencionada por parte del nuevo personal.

1. Informar sobre todos los cambios de personal que afecten al negocio, así como especificar roles y responsabilidades en el tratamiento de la información, la que deberá ser previamente clasificada y analizar los riesgos y medidas de protección durante todo el proceso.
2. Disponer de procedimientos definidos y aceptados por nuestro socio, para la detección y respuesta de alertas de intrusión por ejemplo, previendo la notificación por medio de alertas o intrusiones de alto riesgo.
3. Todo sistema, red o conexión externa no operado por nosotros y que interactúe con nuestros sistemas o redes deben estar documentadas y contar con instalaciones y equipamiento previamente analizados y aprobados por nuestra organización.

Estableciendo una relación entre los aspectos legales y de seguridad de nuestro negocio, a veces es conveniente reforzar los contratos comerciales con **convenios de confidencialidad** aunque tengan una cláusula de confidencialidad incluida, ya que contienen otros aspectos más amplios a los de una simple

***¿Invitarías a tu casa a alguien que no conoces?***

***¿Compartirías tus sueños y proyectos con alguien que no comparte tus "ideas y creencias"?***

cláusula contractual y en él se transcribe la política de acceso a la información involucrada, por ejemplo, por nuestra organización.

Como conclusión, y cuando desde cualquier Unidad de Negocio se planteen estrategias comerciales que resulten en fusiones o convenios de acciones comerciales conjuntas lo primero que debemos preguntarnos es:

***Fabián Descalzo***

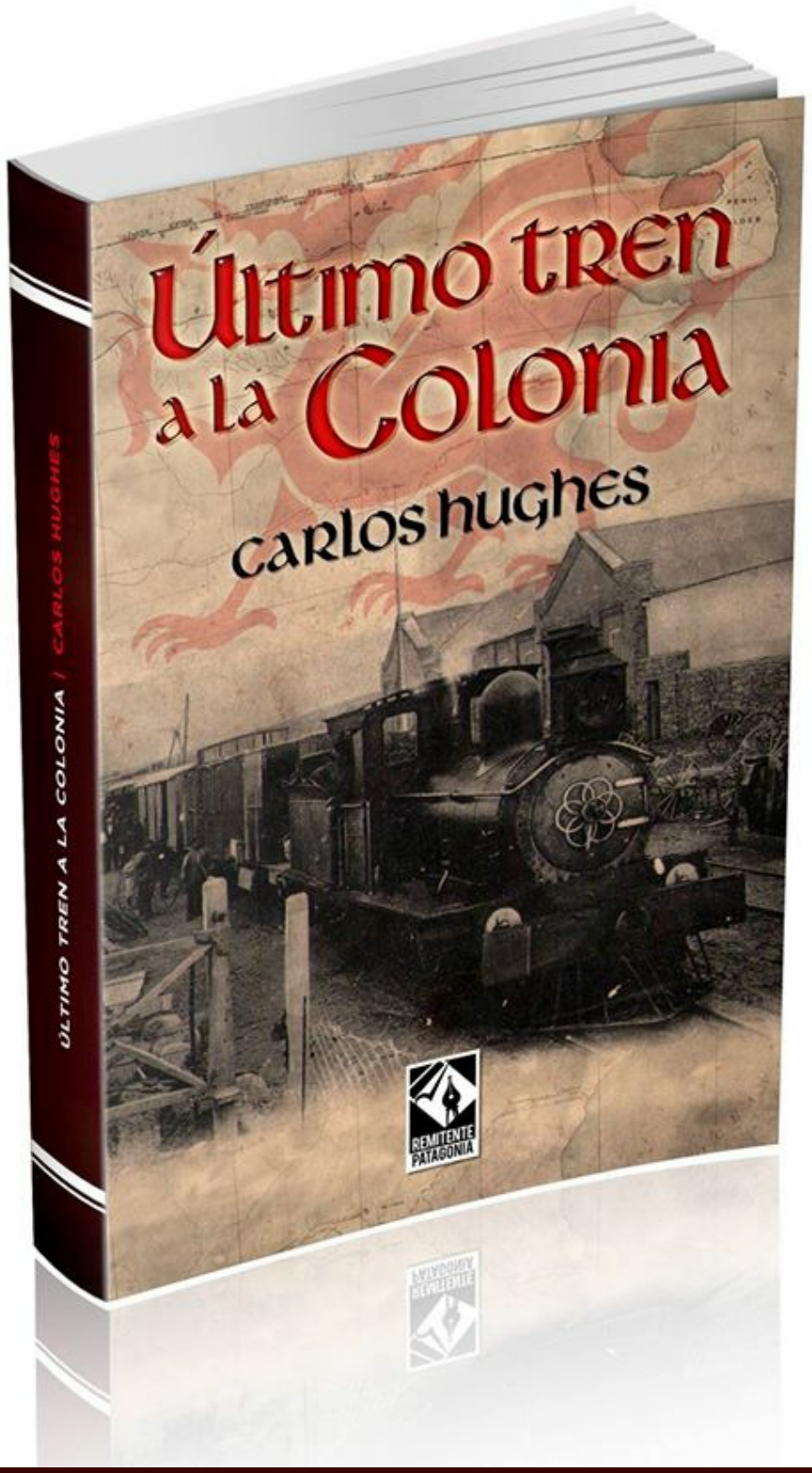
*Gerente de Governance, Risk & Compliance*

***Cybsec S.A. – Security Systems***

Gerente de Servicios y Soluciones en el área de Gobierno, Riesgo y Cumplimiento (GRC) en Cybsec Security Systems S.A., certificado en Dirección de Seguridad de la Información (Universidad CAECE), instructor certificado ITIL Fundation v3-2011 (EXIN) y auditor ISO 20000 (LSQA-Latu).

Columnista especializado en áreas de Gobierno, Seguridad y Auditoría, Informática en Salud y Compliance en las revistas CISALUD, PERCEPCIONES (ISACA Montevideo Chapter), El Derecho Informático, CXO-Community y MAGAZCITUM; y disertante para CXO-COMMUNITY, Consejo Profesional de Ciencias Informáticas, ISACA Buenos Aires Chapter, ISACA Montevideo Chapter.

Profesor del módulo 27001 del curso de IT Governance, Uso eficiente de Frameworks y la Diplomatura en Gobierno y Gestión de Servicios de IT del Instituto Tecnológico Buenos Aires (ITBA)




Autor: Carlos Hughes
EDITORIAL REMITENTE PATAGONIA
Pedidos: remitentepatagonia@gmail.com
web: remitentepatagonia.com.ar

# LA PROTECCIÓN DEL DATO PERSONAL EN RELACIÓN CON LA EVIDENCIA DIGITAL

Por

Ana María Mesa Elneser[1]

RESUMEN

La Protección al Dato Personal en Colombia es un Derecho Constitucional Fundamental regulado con la expedición de la Ley 1581 de 2012 y los Decretos Reglamentarios 1377 de 2013 y 886 de 2014, eje articulador para enmarcar los límites entre la disponibilidad de la información y los datos, con la protección la intimidad y la privacidad en la gestión empresarial. Sin embargo este universo de derechos y obligaciones no interactúa solo, a su vez se relaciona, de forma directa, con la disciplina técnico-científica denominada Forense Digital, la cual se ocupa de la extracción y obtención de la evidencia digital, con el fin de probar la ocurrencia de un incidente informático o hecho delictivo.

PALABRAS CLAVES: dato personal, evidencia digital, forense digital, intimidad y privacidad

## EL DATO PERSONAL Y SU PROTECCIÓN

El Dato Personal, tiene sus orígenes a nivel global que evidencia la interrelación con la Privacidad, sin que puedan considerarse en el mismo contexto. Se debe tener en cuenta que existe mayor relación entre el derecho a la intimidad y la privacidad, que entre el derecho al dato personal y la privacidad, sin que ello no sea presupuesto para establecer como función y finalidad de la privacidad, la protección del dato personal.

Por lo anterior se puede afirmar que la protección de datos personales es un derecho que va a surgir en función, fundamentalmente de determinados acontecimientos históricos que ocurrieron, que mostraron a la sociedad que la recolección y acumulación de datos personales por parte de los Estados puede dar lugar a un abuso de poder y a la utilización indebida o ilegal en razón al uso con fines totalmente distintos

[1] Doctoranda en Derecho Procesal Contemporáneo. Abogada y Magíster en Derecho Procesal U. de M.. Especializanda en Derecho Informático y Nuevas Tecnologías Univ. Patagonia en Argentina. La Autora participa en representación de la Universidad de pertenencia: Universidad Autónoma Latinoamericana Ubicada en la Ciudad de Medellín Carrera 55A N° 49-51. Medellín-Colombia-Suramérica, Teléfono: 5112199 ext. 401. Dirección de correo electrónico: ana.mesael@unaula.edu.co

para los cuales se pretendían en el momento de su recolección.

### 1. Alemania Nazi

Si nos remontamos a la época de la Alemania Nazi cuando llega Hitler al poder empieza a realizar un proceso de búsqueda en determinadas herramientas que le permitieran poder identificar todas aquellas razas que él consideraba en contra de la concepción de la raza perfecta o "Raza Aria" entre los cuales, sin limitarse a ellos, estaban: los Judíos, de los Gitanos, Delincuentes, Homosexuales, Religiosos y de los Discapacitados.

Una de las herramientas que utilizo para compilar esta información respecto de toda la gente existente en el territorio alemán en muy poco tiempo, además que fuera un diseño absolutamente planificado y que permitiera hacer un estudio de cómo estaba compuesta la población Alemana fue el Censo Nacional, contemplando preguntas de tipo de carácter violatorio de derechos fundamentales o personalísimos, y que tendrían directa confrontación con la mayorías de las leyes vigentes en materia de protección de datos personales.

Toda esta información fue recolectada, fue procesada y analizada, permitiendo al Tercer Reich hacer el exterminio masivo que hizo a posteriores, esta es la fuente más directa de donde surge la necesidad de legislar en materia de datos personales.

### 2. Jurisprudencia Norteamericana

Desde otro escenario es importante manifestar lo que paso en EEUU en cuestiones decantadas por diversos autores respecto a "el derecho de estar solo", por ejemplo dice : "todo intento por delimitar el significado de <<intimidad>> parte con una dificultad previa: no existe –dice- un acuerdo generalizado sobre el término concreto a utilizar ni en la vida cotidiana ni entre los que estudian la cuestión", "Se emplean por igual las expresiones «intimidad », «vida privada», o «esfera privada», «ámbito íntimo» o «privado», y la cada vez más común «privacidad», un neologismo que como los anteriores sirve para referirse a ese deseo de disfrutar lo personal y la pretensión consiguiente de exigir a los demás su respeto y, en su caso, su protección legal".

### 3. Perspectiva Colombiana

El artículo 15 de la Constitución Política Colombiana de 1991, definió sin limitaciones el derecho a la protección de datos personales en asocio con el derecho a la intimidad personal como un derecho Constitucional, general, absoluto, patrimonial, inalienable, imprescriptible y que se puede hacer valer por cualquier ciudadano *erga omnes* frente al Estado y a cualquier particular.

Es a partir de la Sentencia C-748 de 2011, por medio de la cual la Corte Constitucional declara la constitucional del proyecto de ley estatutaria que da vida a la Ley 1581 de 2012, en la cual, dijo la corte que, toda persona por el hecho de serlo, es titular innato y exclusivo del derecho a

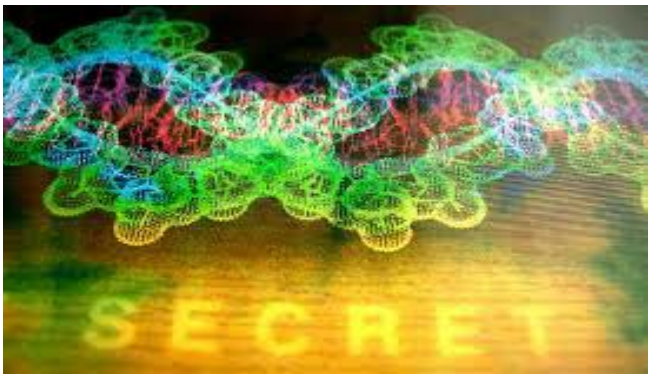
la Protección al Dato Personal, siendo el único legitimado a permitir la divulgación de sus datos personales concernientes a su vida privada, teniendo como finalidad, el aseguramiento de la protección de su Derecho Constitucional a que se le respete su intimidad, su buen nombre, su honra, en todo caso, los derechos morales de toda persona física en Colombia.

La Protección al Dato Personal y la Intimidad, consagrada en el art. 15 C. Pol., también se vincula al derecho a la Autodeterminación Informática "esta se enmarca en principios orientadores, que opera como parámetro para la validez de las actuaciones que adelantan las fuentes, operadores y usuarios del dato personal, así como fundamento para la exigibilidad jurídica de las facultades que se confieren al titular del dato", que tiene todo ciudadano respecto del tratamiento de sus datos en bases de datos, archivos, y bancos de datos, dando respuesta a la necesidad de establecer límites como lo indica el artículo 15 C. Pol. "la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución".

La ley 1581 de 2012 se expide para la protección de todos los Datos Personales a nivel general, salvo los que se someten a regímenes especiales como se identifican en el artículo 2 de dicha ley en atención a que su protección por un régimen especial sea coherente, claro, seguro y favorable de acuerdo a su naturaleza o su especial justificación legal de conservar o preservar otro tipo de protección, aun siendo un dato personal.

### 3.1. Principio de Responsabilidad Demostrada

La ley 1581 de 2012 y su decreto reglamentario 1377 de 2013 en su art. 26, desarrolla el principio de responsabilidad demostrada, que plantea para toda persona que recolecte datos personales la adopción de programas integrales en esa actividad que permitan dar cumplimiento a la protección constitucional y legal que se le ha reconocido al dato personal a partir de la Constitución Política de 1991.




El programa integral de protección de datos personales, no pueden responder a estándares generalizados por sectores empresariales, en contrario, deben responder a un análisis e implementación del programa de protección de datos personales, hecho a la medida de la empresa, teniendo como consecuencia el desarrollo de un instrumento protector del cliente o proveedor, haciendo uso de su papel de titular del dato personal.

La protección del dato personal a nivel mundial está diseñado para que la industria y el comercio, primero estén obligados a generar estrategias de recolección, tratamiento y

circulación de datos, bajo una previa autorización "el permiso del titular", antes de proceder a su uso y conservación, pero no así es generalizado para las empresas el diseño de sus estrategias de mercado, muchas de estas respondiendo a metodologías que no evidencian ni piensan en el permiso previo por parte del titular para la obtención de su dato personal, sobre las políticas de tratamiento, ni las medidas de seguridad y protección de sus datos, que navegan comercialmente en un escenario oculto sobre el tratamiento de sus datos, es un escenario de incertidumbre y desconfianza del cliente frente al comerciante e industria.

## EVIDENCIA DIGITAL

### 4. Breve Análisis Internacional

Es un campo que determina el escenario que rodea la Evidencia Digital, a partir de protocolos forenses certificados por instituciones reconocidas[1], además de los estándares aplicables a laboratorios forenses y el perito forense, permiten dar respuesta a las necesidades investigativas en las nuevas formas delictuales o cibercriminales, cumpliendo requisitos de legalidad y legitimidad tanto de la evidencia como de la prueba, por la utilización de protocolos certificados y de reconocimiento internacional, aunque de gran costo en su adopción al caso concreto.

Lo anterior tiene como efecto principal, que los actos investigativos se direccionan para extraer una evidencia digital, al momento de la investigación del delito informático, como es el caso Colombiano o de países latinoamericanos, el aval a la evidencia realizada a partir de la certificación del instituto como fuente de respaldo en el cumplimiento de autenticidad, integridad, originalidad, confiabilidad y no repudio.

### 5. Breve Análisis Colombia

Inicialmente hay que delimitar la exigencia en Colombia respecto de los principios orientadores de la actividad forense[2], pero el término jurídico de *la evidencia digital* en Colombia no se encuentra expresa en el ordenamiento jurídico, a su vez en el art. 275 de la Ley 906 de 2004, solo se tienen las categorías correspondientes a medios cognitivos, las denominadas Evidencias Físicas y Elemento Material Probatorio, permitiendo concluir que la podemos entender como éste tipo de evidencias la construida por campos magnéticos y cursos electrónicos, que puede ser reportados, almacenados y realizados con herramientas técnicas específicas, entiéndanse protocolos, software y hardware vinculado, que no se han desarrollado para el Estado Colombiano a la medida, por consiguiente, se han acogido las internacionales del NIST y del SANS principalmente.

### *6.* Evidencia digital en relación con intimidad, privacidad y datos personales en *log*

Cuando se habla de un tratamiento del incidente informático se tiene que establecer el alcance de

[1] SANS, NIST, INTERPOL, ISO.

[2] autenticidad, integridad, originalidad, confiabilidad y no repudio

la intimidad y la privacidad desde dos miradas, o mejor desde dos disciplinas científicas que son a su vez, el Derecho y *Digital Forense*. Cuando hablamos de incidente informático, tenemos en cuenta que se involucra no solo información, en muchos casos da cuenta de datos personales, contenidos en *logs*. Para delimitar si la prueba pericial tiene relación o no con la privacidad, es necesario identificar si el incidente informático ha ocurrido, en una red pública o una red privada.

Por la naturaleza de lo establecido como *log*, es de uso privado, sin embargo, existe empresas dedicadas al ámbito estadístico, el cual solo es posible a partir de la información y datos recolectados. La recolección que realizan estas empresas se obtiene a partir del monitoreo de los puntos de acceso central a internet a los países para sacar información de navegación en la internet, sin o con permiso del titular de la información y del dato personal.

Por ello, la etapa que se surte para el desarrollo de los actos de investigación, sean dados por la fiscalía o por investigación privada, es en sí misma, un escenario de recolección de la información que dé cuenta del delito. De allí, que se pueda denominarse, una solicitud de *log* a los *ISP* o las empresas de servicio en correo, redes sociales, sitios web, entre otros, como son, sin limitarse a ellas, Facebook, Yahoo, Gmail, Terra, actos de investigación, los cuales, dependiendo de su naturaleza y disponibilidad requieren o no un control previo o posterior de legalidad y legitimidad ante el juez.

Las empresas y los prestadores de Internet, han adoptado procedimientos legales uniformes para que los funcionarios judiciales y entes investigadores tengan conocimiento de cómo debe solicitarse la extracción del *log,* procedimientos que se desarrollan a partir de la política de privacidad, la cual, se encuentra en constante dinamismo, sea por el cambio de las estrategias comerciales, o sea por dar cumplimiento a la protección del dato personal.

**CONCLUSIONES**

7. La creación de programas integrales de protección de datos personales a los que hacen referencia, tanto las guías de la OECD como las normas Colombianas, no se consideran una aplicación y uso restrictivo para la gran empresa, son procesos para cualquier empresa, escalables, que se deben hacer a la medida de cada organización que en su operación empresarial y comercial haga tratamiento de datos personales, obligando a repensar la manera de integrar procesos de análisis de información local y ahora nacional, igualmente a las entidades del Estado responsables de la supervisión, se deben repensar en su forma de operar y el direccionamiento de las políticas públicas, para dar respuesta a las necesidades nacionales y trasnacionales en materia de protección a la privacidad, enfrentando retos del presente siglo como es el denominado el BIG DATA.

*8.* Para preservar la privacidad de los *logs* y a su vez la conservación como fuente de información para probar el hecho delictivo,

se puede solicitar a los ISP de transito de datos, como pudieran ser en Colombia Telmex, Une, Edatel entre otros, guardan *logs* de estadísticas de acceso de las empresas a las cuales les prestan el servicio, y con fundamento a los acuerdos suscritos para la protección de la propiedad intelectual directamente con la DMCA -Digital Millennium Copyright Act.-, ha obligado que los ISP filtren el tráfico de *bittorrent*, por ello, para la obtención de log sin depender del trámite por vía judicial, se puede consultar los acuerdos firmados del ISP en procura de la preservación y protección de los derechos de autor ante la DMCA y dependiendo del nivel de privacidad podrá habilitarse la solicitud del *log* directamente a la empresa, eso sí, en este escenario igualmente la persona encargada de la extracción es el *record keeper.*

**REFERENCIAS:**

**BIBLIOGRAPHY \l 9226**(DDI), D. D. (2015).*OEA*. Obtenido de www.oas.org/es/sla/ddi/proteccion_datos_personales.asp

Black, E. (2001).*IBM Y ELHOLOCAUSTO.*Alemania: Atlantida.

Cano, J. (2010).*Computaciòn Forense.*Bogotá: Omega.

Cavero, J. M. (1993).*El derecho a la Intimidad en laJurisprudenciaConstitucional.*MadridEspaña: Civitas.

Development, O. S. (2015).*OSD GLOBAL*. Obtenido de www.osdglobal.com

ELNESER, A. M. (2013).*APROXIMACIÓN A LA INFORMÁTICA FORENSE Y EL DERECHO INFORMÁTICO: Ámbito Colombiano.*Medellín: (Departamento Fondo Editorial Funlam - FUNLAM.

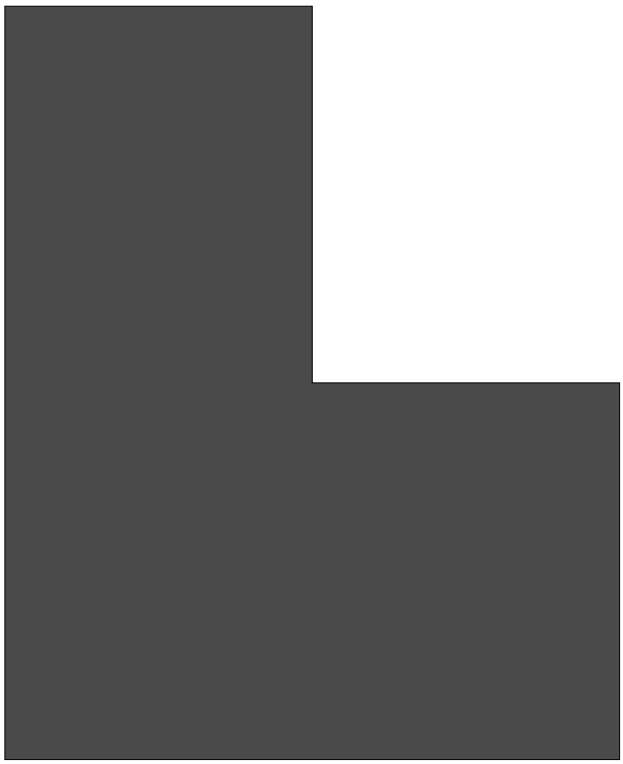
Fiscalía, L. F. (2008).*La Prueba en el Proceso Penal Colombiano.*Medellín: Fiscalía General de la Nación y Fenix Medina Group.

Peggy Valcke, J. D. (2012).*Computer, Law & Security Review – special issue Trust in the Information Society.*Oslo, Norway: Editorial Board - University of Oslo, .

Sentencia Constitucional, Sentencia T- 419 (Corte Constitucional 8 de julio de 2013).

Sentencia Good Will o Credito Mercantil , expediente 16274 (Consejo de Estado 26 de enero de 2013).

Timothy Morey, T. F. (2015). Customer Data: Desingning for Trasnparency and Trust.*Revista Harvard Business Review*, 96 - 105.




# Más que un blog.
# Toda la actualidad jurídica.

información jurídica ágil, eficiente y relevante

**aldiaargentina.microjuris.com**

Llámenos (5411) 5031-9300

microjuris.com
inteligencia jurídica

INTIMIDAD

SECCIÓN

# PRIVACIDAD

Responsable

INÉS
TORNABENE

**Texto compilado de la Conferencia Magistral presentada en la IX Conferencia Internacional de Derecho e Informática de La Habana , 2013.**

**Autora: Inés Tornabene**

**Introducción: Privacidad e intimidad**

La Real Academia Española (RAE) define el término privacidad como el "ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión". Por su parte, define el adjetivo privada (utilizado en la definición de privacidad) como algo "que se ejecuta a vista de pocos, familiar y domésticamente, sin formalidad ni ceremonia alguna".

Sin embargo, semánticamente, no hay acuerdo sobre si es correcto el uso del término "privacidad" o si sería más adecuado el uso de la palabra "intimidad". Incluso algunos han llegado a rechazar el uso de la palabra privacidad por considerarla un anglicismo y se sugiere que se reemplace por el término intimidad o vida privada, ya que según quienes sostienen esta opinión, tanto intimidad como vida privada son sinónimos preferibles al término privacidad, derivado del inglés.

En la legislación Española en materia de protección de datos, por ejemplo, encontramos ambos términos en distintos textos legales. La Constitución Española solo utiliza el término intimidad, mientras que la Ley Orgánica de Regulación del Tratamiento Automatizado de Datos (LORTAD) introduce el término privacidad en 1992. El Código Penal español, de 1995, define los delitos contra la intimidad y la Ley Orgánica de Protección de Datos de Carácter Personal de 1999 sostiene que su finalidad es proteger la intimidad personal y familiar (Díaz Rojo, 2002).

Siguiendo al Dr. José Antonio Díaz Rojo, del Consejo Superior de Investigaciones Científicas de Valencia, España, vamos a repasar algunas definiciones de privacidad de los principales diccionarios generales de la lengua española. Ya vimos el de la Real Academia Española, y coincidimos con Díaz Rojo en que se puede deducir que la definición deja entrever que en la vida privada hay ámbitos que pueden protegerse de cualquier intromisión y otros que escaparían a este derecho. El espacio o dimensión que sí podemos proteger es objeto de protección jurídica yesto implica que podemos repeler cualquier intromisión extraña.

El Diccionario de uso del español actual "Clave", define la privacidad de la siguiente forma: "Propiedad de lo que pertenece a la intimidad o

a la vida privada de una persona". Como ejemplo del uso de este sustantivo nos deja la siguiente frase: "La prensa muchas veces no respeta la privacidad de los famosos".

En el caso del Diccionario de uso IX Conferencia Internacional de Derecho e Informática de La Habana , 2013 del español María Moliner, edición 1999, define privacidad como "Cualidad o condición de privado", siguiendo la tradición de definir los sustantivos terminados en "dad" como cualidades. Este mismo diccionario define privado como aquello que "Se aplica a lo que se refiere a una persona como tal persona o como miembro de una familia y no como ciudadano o por su profesión". Así vemos como marca una diferencia entre lo privado como puesto del lado de lo familiar como característica contrapuesta a lo profesional o público.

Este último caso es un buen ejemplo de la distinción entre "lo privado" como concepto opuesto a "lo público". Este binomio hace referencia a un concepto jurídico, la "cosa pública", la res publica, origen del término república, y que se relaciona con todo aquello en lo cual el Estado tiene interés e injerencia, o sea, que no es privado o privativo de la esfera de la intimidad de las personas.

Lo íntimo es un adjetivo que proviene del latín intimus y que alude a lo interior, a lo interno, a lo recóndito, que está en el fondo de algo. Lo "íntimo" hace referencia a aquello que queremos ocultar de los demás, que queremos preservar sin que se vea, que únicamente destinamos a nosotros mismos y a quienes elegimos. El propio Diccionario de la Real Academia Española define "íntimo" como "lo más interior o interno", y el término "intimidad" como "zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia".

No parece que los términos privado e íntimo sean sinónimos. Lo privado se refiere a aquellas cuestiones particulares y personales que se encuentran fuera del alcance y la intromisión del Estado o de cualquier otra persona, en tanto que íntimo se aplica a las cuestiones mucho más profundas y relacionadas con relaciones personales íntimas y estrechas, a la confesión de sentimientos profundos.

Siguiendo a Díaz Rojo, vemos como privacidad e intimidad no son términos equivalentes. La intimidad, según este autor, es el conjunto de

sentimientos, pensamientos e inclinaciones más guardados en el interior -la ideología, la religión o las creencias-, las tendencias personales que afectan a la vida sexual, determinados problemas de salud que deseamos mantener en total secreto, u otras inclinaciones que forman parte del ámbito más reservado de una persona. Nuestra intimidad puede ser desconocida para las personas que más cercanas son a nuestra vida cotidiana, pero, en cambio, nuestra vida privada es compartida con ellos. Cada persona es la única con la potestad necesaria para fijar el límite hasta donde llega la intimidad. A partir de ese límite, cada persona es la única con potestad para decidir quien ingresa y quien no ingresa dentro de su ámbito íntimo.

No es lo mismo hablar de privacidad e intimidad hoy que hace quinientos años… ni siquiera hace veinte años. Lo que podía trascender de nuestras vidas antes del surgimiento de los medios masivos de comunicación era prácticamente nulo. Pensemos en un escritor y su libro antes de la invención de la imprenta: ¿cuántos ejemplares podía "distribuir"?.

Lo cierto es que los libros se leían (por alguien que supiera leer) en forma pública para que algunos privilegiados tuvieran acceso a los textos. La vida privada de los habitantes de los pueblos o ciudades podía ser objeto de difusión en una medida territorial exigua, y en todo caso, la difusión iba a alcanzar, para el ciudadano que no destacara por IX Conferencia Internacional de Derecho e Informática de La Habana , 2013 ninguna circunstancia particular, un número muy reducido de personas, a través del "boca en boca".

Con el surgimiento de la prensa, y luego con el resto de los medios de comunicación, como la radio y la televisión, la información en general empezó a circular por el mundo de otra forma. Pero no podemos escapar a la observación de que en los últimos veinte años, con el surgimiento de Internet y la posibilidad de acceder a esta red, las cosas han cambiado sustancialmente. La información se difunde en el mismo momento que los hechos están ocurriendo. Y muchas veces la información que se difunde tiene que ver con lo privado y con lo íntimo. Ya no se trata solamente de los medios de comunicación: ahora la difusión de la información está en manos de los ciudadanos. Con la proliferación de los teléfonos celulares "inteligentes", provistos de cámara de foto, filmadora y conexión a internet, lo que se ve se fotografía o se filma, se digitaliza y sube a la red. Una vez en la red, no hay forma de volver atrás los pasos.

De la misma forma que el acceso a internet se ha reconocido como un derecho humano, no podemos negar que el uso de la red digital sin los recaudos pertinentes puede generar daños en la privacidad e intimidad de las personas que son de muy difícil reparación. Por esta razón los países han ido tomando conciencia en los últimos años sobre la necesidad de legislar en la materia, con el objetivo de proteger el derecho de las personas a cuidar sus datos personales, su información privada y su información íntima.

Ya en el año 1998 algunos autores hemos reconocido la existencia de un derecho a la intimidad y a la privacidad, entendido como el poder o potestar de tener un domicilio particular, papeles privados, ejercer actividades, tener

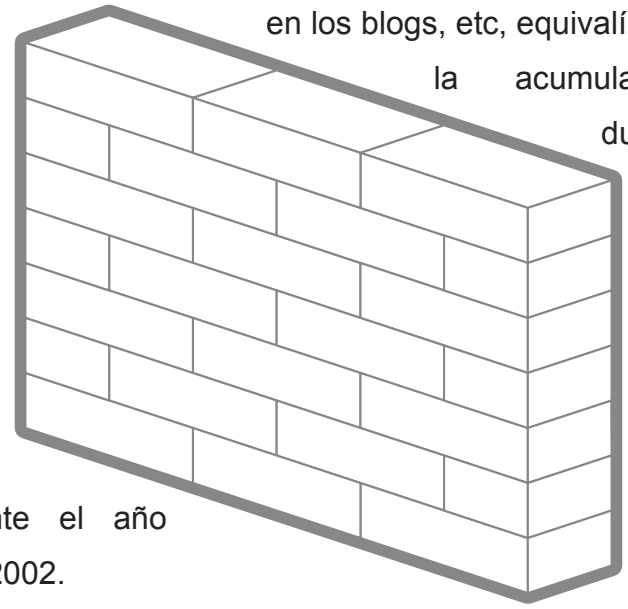
contactos personales y pensamientos que no trasciendan a terceros, en virtud del interés personal de mantenerlos en reserva y la discreción de quien se entera de no hacerlos públicos cuando se trata de hechos privados o datos sensibles de las personas(Pierini, Lorences y Tornabene, 1999). Se trata no ya de un derecho de tercera o de cuarta generación, sino un derecho tan antiguo como el hombre mismo, que lo acompaña y es inherente a su existencia misma como ser humano que vive en sociedad, pero que debe ser replanteado y reformulado a la luz del avance tecnológico y del uso de la informática como una medio que posibilita la interconectividad a nivel mundial y en forma ilimitada. El derecho a la intimidad podemos resumirlo en lo que se conoce como el derecho a estar sólo, es decir, el derecho a que el resto de las personas no conozcan, sepan, vean, escuchen lo referente a nuestra vida, pudiendo incluso agregarse también “y que nosotros no queramos que trascienda”. Es pensar en reafirmar que cada uno es dueño de su esfera más íntima, de ese ámbito nuclear perteneciente a los propios pensamientos y sentimientos.

A este derecho humano, individual y personalísimo a proteger la intimidad, se contrapone, y como una amenaza, el poder que otorga la acumulación y circulación de la información y la facilidad con que puede llevarse a cabo gracias a los medios informáticos actuales. En el año 2000 ya se sostenía que esta forma de producir información podía extralimitar los derechos de privacidad que los internautas poseen y por tanto infringir una lesión al derecho a la intimidad (Elias, 2000).IX Conferencia Internacional de Derecho e Informática de La Habana , 2013

En el año 2002 la capacidad de almacenamiento de información en forma digital ya había superado a la analógica.

Cinco años después, en el año 2007, se transmitieron 1,9 zettabytes de información por medio de tecnología de difusión como televisores y GPSs. Un zettabyte equivale a 1.024 exabytes 1. Es como si cada persona del planeta leyera 174 periódicos por día. En agosto de 2011, el director ejecutivo de Google, Eric Schmidt, afirmó que la humanidad había creado hasta el 2003 una cantidad de información equivalente a 5 exabytes, y que a esa fecha, agosto de 2011, esa cifra de 5 exabytes era lo que se generaba cada… dos días.

Los datos, sin embargo, no son unánimes, ya que en la misma fecha otras fuentes, como la consultora RJMetrics, sostenían que toda la cantidad de información que se generaba en ese momento en Internet en una semana, ya sea por medios en línea, redes sociales, vía streaming, en los blogs, etc, equivalía a la acumulada dura



nte el año 2002.

El gran crecimiento de internet en los últimos años ha posibilitado el desarrollo de nuevas herramientas de comunicación y nuevos equipos

con una portabilidad que facilita llevar los equipos con nosotros en todas las tareas cotidianas. Ya no se trata solamente del uso de computadoras de escritorio; las computadoras portátiles, las tabletas y los teléfonos inteligentes permiten el uso de herramientas de comunicación que antes sólo estaban reservadas para los ordenadores de escritorio. A eso le sumamos que el costo económico de los equipos ha descendido con el paso del tiempo.

Hoy, un teléfono portátil, de los llamados teléfonos inteligentes, permite que enviemos correo electrónico, que naveguemos por páginas, que mantengamos sesiones de chat, que recibamos y emitamos mensajes a través de programas gratuitos, que actualicemos nuestros blogs, que realicemos operaciones de comercio electrónico, que juguemos, que miremos videos, entre otras cosas. Y además podemos hablar por teléfono y mandar mensajes de texto.

O sea, que podemos dar un uso similar a un ordenador de escritorio, hablar por teléfono, y pagando por dicho equipo un precio muy inferior a una computadora de escritorio.

La información se comparte a nivel global. Los límites territoriales y las barreras físicas se desdibujan a través de la utilización de una tecnología que nos permite prescindir, a los usuarios finales, incluso del cableado. Las personas pasamos mucho tiempo intercambiando información con otras personas, a través de las denominadas “redes sociales”.

Nuestra información no sólo se almacena en nuestras computadoras, tabletas o teléfonos, sino que también se suben a la “nube”, “nube” de la cual, en la mayoría de los casos, desconocemos su ubicación real y la legislación vigente en materia de protección de datos personales del lugar donde se encuentran los centros de datos que la almacenan.

El tráfico de información ha permitido muchos beneficios a las personas en forma individual, pero también supone garantizar enormes beneficios económicos para grandes compañías. Son nuestros datos personales, nuestros gustos, nuestras actividades las que le dan contenido y valor económico a las redes sociales. Nadie puede desconocer hoy en día que la misma tecnología que nos permite conectarnos (preferimos reservar el termino “comunicarnos” a otro concepto) es la que también genera nuevos riesgos para la seguridad de la información personal y para la protección de nuestra intimidad. Es por eso que cada vez con más fuerza se habla del uso responsable y seguro de las tecnologías de la información y la comunicación.

En el medio de toda esta evolución lo que queda navegando en el océano de la información son los datos personales, que atañen a la privacidad y a la intimidad. Hoy, en el 2013, los desafíos deben enfocarse en dos aspectos principales:

a) la prevención, y concientización, ineludible si queremos que cada persona se haga responsable de la información que de si misma y en forma voluntaria difunde y aprenda a clasificar y cuidar sus propios datos; b) la existencia de mecanismos eficientes a la hora de defender a los ciudadanos de cualquier intrusión y difusión de datos íntimos y/o privados.

La comunidad internacional ha reconocido la necesidad de crear una normativa que responda a esta evolución tecnológica y ha tenido una

crecimiento paulatino en materia de legislación que protege la información personal.

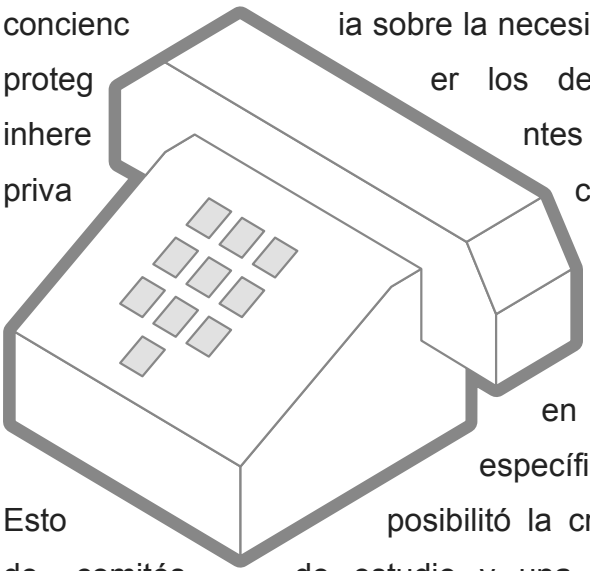
Vamos a presentar a continuaión los antecedes y el estado actual de la legislación en materia de protección de datos personales en la República Argentina.

Legislación sobre protección de datos personales en la República Argentina

1. Antecedentes internacionales

El derecho a la intimidad y la vida privada ha sido reconocido como un derecho universal. La Declaración Universal de los Derechos Humanos de 1948 así lo dispone al establecer en su artículo 12 que “nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques”.

En muchos países se fue gestando una concienc ia sobre la necesidad de proteg er los derechos inhere ntes a la priva cidad de los ciudad anos en forma específica.



Esto posibilitó la creación de comités de estudio y una amplia discusión y debates que culminaron en el dictado de leyes sobre protección de datos personales. En los años 70 y 80 podemos mencionar la Ley de Suecia de Datos, de 1973, la Ley de Informática e Información de Francia, de 1978 y la Ley de los Países Bajos sobre datos personales y registro, de 1988. Mencionamos casos europeos porque hay un consenso general de considerar que el modelo europeo garantiza un alto nivel de protección de datos personales por ser garantista, riguroso y efectivo (Bertoni, 2012). No vamos a entrar, sin embargo, en detalles sobre el modelo europeo, porque escapa al objetivo de esta ponencia. Sí vamos a mencionar que en Latinoamérica se ha tomado como eje rector en la materia el derecho fundamental del habeas data, que se trata no sólo de una acción judicial concreta, sino de una herramienta de protección tendiente a facilitar a todas las personas: a) el acceso a la información que sobre ella conste en un registro o en un banco de datos; b) que se actualicen los datos obsoletos o atrasados; c) que se rectifiquen los datos inexactos; d) que se asegure la confidencialidad de cierta información legalmente obtenida para evitar su conocimiento a terceros, y e) la supresión de la obtención de la denominada información “sensible”, entre las que podemos mencionar toda la relacionada con la esfera de intimidad, ideas políticas, religiosas o gremiales, preferencias sexuales, origen étnico y cualquier tipo de información que pueda ser utilizada en forma discriminatoria.

2. Constitución Nacional Argentina y leyes nacionales

a. Tratados internacionales a los cuales la República Argentina ha adherido en materia de protección de datos personales

El Sistema Internacional de protección de datos personales se encuentra conformado por: el Artículo 12º de la Declaración Universal de Derechos Humanos de 1948, antes citado. Y, el Artículo 17º del Pacto Internacional de Derechos

garantías no enumerados pero que nacen del principio de la soberanía del pueblo y de la forma republicana de gobierno". La redacción de este artículo, mantenida luego de la reforma, se refiere a que la enumeración de declaraciones, derechos y garantías de ninguna forma deberá ser considerada taxativa; por lo tanto, no se consideran negados el resto de los derechos y que fueron acogidos por los tratados, concordatos, acuerdos o declaraciones internacionales a los que la Nación haya adherido y ratificado, las leyes que en su consecuencia se dictaran, el resto de las normas y los pronunciamientos jurisprudenciales. La Constitución no agota el reconocimiento de los derechos por su falta de inclusión concreta.

La reforma de la Constitución de 1994 implicó la tipificación de una serie de derechos trascendentes y ya reconocidos como inherentes a las garantías individuales y colectivas necesarias para la vida en sociedad y para la defensa del ecosistema.

El artículo 1071 del Código Civil, incorporado por la ley N° 21.173, contiene el siguiente texto: "El que arbitrariamente se entrometiere en la vida ajena, publicando retratos, difundiendo correspondencia, mortificando a otro en sus costumbres o sentimientos o perturbando de cualquier modo su intimidad, y el hecho no fuere un delito penal, será obligado a cesar en tales actividades, si antes no hubieren cesado, y a pagar una indemnización que fijará equitativamente el juez, de acuerdo con las circunstancias; además, podrá éste, a pedido del agraviado, ordenar la publicación de la sentencia en un diario o periódico del lugar, si esta medida fuese procedente para una adecuada reparación". Este artículo representó una norma de carácter general y de gran y abarcativo contenido relacionado con la intromisión en la vida privada y en la intimidad de las personas.

c. La reforma de la Constitución Nacional de 1994

A través de la ley N° 24.309 se dispuso la necesidad de la reforma constitucional, pero en la misma se estableció, en su artículo 7, que la Convención Constituyente no podría introducir modificaciones en las Declaraciones, Derechos y Garantías contenidas en la primera parte de la Constitución Nacional. Por ello fue necesario crear un nuevo capítulo para el tratamiento de los denominados nuevos derechos y garantías. Allí se incorporó el instituto del hábeas data, en el artículo 43, párrafo tercero: "Toda persona podrá interponer acción expedita y rápida de amparo, siempre que no exista otro medio judicial más idóneo, contra todo acto u omisión de autoridades públicas o de particulares, que en forma actual o inminente lesione, restrinja, altere o amenace, con artibrariedad o ilegalidad manifiesta, derechos y garantías reconocidos por esta Constitución, un tratado o una ley. En el caso, el juez podrá declarar la inconstitucionalidad de la norma en que se funde el acto u omisión lesiva.

Podrán interponer esta acción contra cualquier forma de discriminación y en lo relativo a los derechos que protegen al ambiente, a la competencia, al usuario y al consumidor, así como a los derechos de incidencia colectiva en general, el afectado, el defensor del pueblo y las asociaciones que propendan a esos fines, registradas conforme a la ley, la que determinará los requisitos y formas de su organización.

Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística.

Cuando el derecho lesionado, restringido, alterado o amenazado fuera la libertad física, o en caso de agravamiento ilegítimo en la forma o condiciones de detención, o en el de desaparición forzada de personas, la acción de hábeas corpus podrá ser interpuesta por el afectado o por cualquiera a su favor y el juez resolverá de inmediato, aun durante la vigencia del estado de sitio".

Entendemos que la norma no debe entenderse en forma restrictiva y que, además, reconoce su idoneidad para resolver todos los conflictos referidos o que tengan relación directa con el almacenamiento de datos, su obtención, su publicidad o su reproducción, y con las consecuencias, abusos e intromisión en la privacidad. Y creemos que también podría haberse hecho mención al tratamiento de datos a través de sistemas informáticos, ya que la reforma constitucional data de 1994 y el legislador constituyente ya se encontraba al tanto de los avances tecnológicos del momento.

d. La ley nacional de protección de datos personales

Luego de la reforma constitucional de 1994 hubo acuerdo doctrinal y jurisprudencial respecto de la operatividad de la acción de hábeas data, en especial teniendo en cuenta que se reconocía a la acción de amparo como el remedio idóneo para el acceso, la rectificación o la anulación de las registraciones, según el caso.

Luego de una primera ley de protección de datos personales que fuera vetada en forma total por el poder ejecutivo en diciembre de 1996, la ley N° 25.326 fue sancionada el 4 de octubre del año 2000 y publicada en el Boletín Oficial el 2 de noviembre del mismo año.

La norma contiene prescripciones sobre disposiciones generales, principios generales relativos a la protección de datos, derechos de los titulares de datos, usuarios y responsables de archivos, registros y bancos de datos, órganos de control, sanciones administrativas y penales, y acción de protección de los datos personales, o sea, la acción de hábeas data.

Con fecha 9 de enero de 2008 se publicó en el Boletín Oficial la ley N° 26.343 que incorpora la nueva redacción del art. 47 a la ley N° 25.326, referida a los bancos de datos prestadores de servicios de información crediticia.

e. Reforma al Código Penal en materia de Delitos Informáticos

Con el dictado de la ley N° 26.388, promulgada el 24 de enero de 2008, se incorporaron reformas al Código Penal de la Nación en materia de delitos informáticos.

El artículo 77, en el cual se define la significación de conceptos empleados en el Código, se incorporó: "El término "documento" comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión. Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o

firmar digitalmente. Los términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente".

En el capítulo sobre delitos contra la integridad sexual se incorporó el artículo 128 sobre pornografía infantil: "Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores. Será reprimido con prisión de cuatro (4) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización. Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años".

Se sustituyó el epígrafe del Capítulo III, del Título V, del Libro II del Código Penal ("violación de secretos"), por "Violación de Secretos y de la Privacidad".

Dentro del mismo capítulo III, el artículo 153 quedó redactado luego de la reforma de la siguiente manera: "Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida. En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido. La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.

Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el

doble del tiempo de la condena".

Se incorporó el artículo 153 bis: "Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido. La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros".

El artículo 155 quedó redactado de la siguiente forma: "Será reprimido con multa de pesos un mil quinientos ($ 1.500) a pesos cien mil ($ 100.000), el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros. Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público"

Se sustituyó el artículo 157 por el siguiente: "Será reprimido con prisión de un (1) mes a dos (2) años e inhabilitación especial de un (1) a cuatro (4) años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos".

El artículo 157 pasó a tener la siguiente redacción: "Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:

1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.

3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4)

años".

Dentro del título VI, Capítulo III, delitos contra la propiedad, se incorporó el inciso 16 al artículo 173: "Inciso 16. El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos".

En el mismo título VI, pero en el Capítulo VII referente al delito de daños, se incorporó como segundo párrafo del artículo 183 lo siguiente: "En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños".

El artículo 184 pasó a quedar expresado en los siguientes términos: "La pena será de tres (3) meses a cuatro (4) años de prisión, si mediare cualquiera de las circunstancias siguientes:

1. Ejecutar el hecho con el fin de impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones;

2. Producir infección o contagio en aves u otros animales domésticos;
3. Emplear substancias venenosas o corrosivas;
4. Cometer el delito en despoblado y en banda;
5. Ejecutarlo en archivos, registros, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público; o en tumbas, signos conmemorativos, monumentos, estatuas, cuadros u otros objetos de arte colocados en edificios o lugares públicos; o en datos, documentos, programas o sistemas informáticos públicos;
6. Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público".

En el Título VII, de la Seguridad Pública, Capítulo II, Delitos contra la seguridad de los medios de transporte y comunicación, se sustituyó el artículo 197: "Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida".

Finalmente, en el Título XI, Delitos contra la Administración Pública, Capítulo V sobre violación de sellos y documentos, se sustituyó el artículo 255: "Será reprimido con prisión de un (1) mes a cuatro (4) años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo. Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de pesos setecientos cincuenta ($ 750) a pesos doce mil quinientos ($ 12.500)".

3. Legislación provincial

La República Argentina está conformada por un total de 23 provincias y la Ciudad Autónoma de Buenos Aires. Cada una de estas provincias, por mandato del artículo 123 de la Constitución Nacional, "dicta su propia constitución, conforme a lo dispuesto por el artículo 5° asegurando la autonomía municipal y reglando su alcance y contenido en el orden institucional, político, administrativo, económico y financiero".

La mayoría de las provincias argentinas han ido dictando a lo largo del tiempo su propia legislación en materia de protección de datos. Actualmente solo cinco de las 23 provincias no se han pronunciado al respecto con normativa local.

a. Provincia de Buenos Aires: Constitución provincial, artículo 20, punto 3, incorporado en 1994 y Ley de Hábeas Data, N° 14.214, del 14.01.2011, regulatoria del procedimiento del recurso de habeas data.

b. Provincia de Chaco: Constitución provincial, artículoículo 19, modificado en 1994 y Ley de Hábeas Data, N° 4.360, reglamentada el 21.11.1996

c. Provincia de Chubut: Constitución provincial, artículo. 56, modificado en 1994 y Ley de Hábeas Data, N° 4.244, del 05.12.1996

d. Provincia de Córdoba: Constitución provincial, artículo. 50, modificada en 1987. La ley de Hábeas Data del año 2000 fue VETADA.

e. Provincia de Entre Ríos: Constitución provincial, artículo. 63, modificada en 2008

f. Provincia de Jujuy: Constitución provincial, artículo. 23, del 22.10.1986

g. Provincia de La Rioja: Constitución provincial, artículo 28 bis, incorporado en la reforma constitucional de 1998. A partir de la reforma del año 2008 dicho artículo es el 29, Art. 31

h. Provincia de Neuquén: Constitución provincial, artículo 61, reforma de 1994, Ley de Hábeas Data, N° 2.307, del 07.12.1999. Ley N° 2.399 de adhesión a la ley nacional de Protección de Datos Personales N° 25.326.

i. Provincia de Río Negro: Constitución provincial, artículo 20, reforma de 1988 y Ley de Hábeas Data N° 3.246 del 16.11.1998

j. Provincia de Salta: Constitución provincial, artículo 89, reforma de 1998

k. Provincia de San Juan: Constitución provincial, artículo 26, reforma de 1986 y Ley N° 7.444, del 20.11.2003, sobre la insripción de bases en el Registro Público de Comercio

l. Provincia de San Luis: Constitución provincial, artículo 21, de 1987 – Reforma constitucional del 11.11.2011 • Ley I-0733-2010 sobre Garantía de la Intimidad y Privacidad, del 13.10.2010.

m. Provincia de Tucuman: Código Procesal Constitucional, Capítulo IV, Artículo 67, 02.03.1999: Amparo informativo (hábeas data)

n. Provincia de Santiago del Estero: Constitución provincial, artículo 60, del 2002

o. Provincia de Tierra del Fuego, Antártida e Islas del Atlántico Sur: Constitución provincial, artículo 45, del 17.05.1991

p. Provincia de Mendoza: Ley Nº 7.261, 01.08.2004, creación del Registro de Empresas Privadas de Información de Deudores, conocida como ley de hábeas data.

q. Provincia de Misiones: Ley de Protección de Datos Personales N° 3.794, del 25.10.2001

r. Provincia de Corrientes: Constitución provincial, artículo 68, año 2007

Las provincias La Pampa, Formosa, Santa Cruz, Santa Fe y Catamarca no han incluido en sus respectivas cartas magnas referencias a la privacidad, a la intimidad ni al recurso de hábeas data hasta la fecha.

4. Legislación de la Ciudad Autónoma de Buenos Aires

En la Ciudad de Buenos Aires el hábeas data está legislado en el artículo 16 de su Constitución, promulgada el 1 de octubre de 1996 y la Ley N° 1845, Protección de Datos Personales, sancionada el 24 de noviembre del año 2005, sufriendo un veto parcial publicado en el Boletín Oficial 2351 del 4 de enero de 2006. Fue reglamentada por el Decreto 725 del año 2007.

Esta norma regula el tratamiento de datos personales asentados en bancos de datos del sector público de la Ciudad, a los fines de garantizar el derecho al honor, a la intimidad y a la autodeterminación informativa, de conformidad a lo establecido por el artículo 16 de la Constitución de la ciudad y sigue en general los lineamientos de la ley nacional de protección de datos N° 25.326. La autoridad de aplicación es la Defensoría del Pueblo de la Ciudad de Buenos Aires.

Dentro de su ámbito se ha creado el Centro de Protección de Datos Personales con compentencia sobre los bancos de datos

públicos en toda la Ciudad Autónoma de Buenos Aires.

Próximos desafíos

Como podemos observar a lo largo del recorrido efectuado, la mayoría de la legislación vigente en la República Argentina equipara la privacidad a la intimidad. Encontramos una excepción en la ley I-0733-2010 de la provincia de San Luis, en la cual se hace una distinción entre el derecho a la intimidad y el derecho a la privacidad, aunque sin hacer una diferenciación concreta que permita identificar claramente uno del otro.

Consideramos que resulta eficaz efectuar una distinción entre ambos conceptos, distinción que es sólo una cuestión de grado dentro de la misma especie; la intimidad pertenece al ámbito de la privacidad, todo lo íntimo es privado, en cambio no toda la información privada es información íntima.

Incluso un claro acto voluntario del titular de la información puede cambiar la calidad de dato íntimo para convertirlo en un dato privado. Si entendemos que la esfera de la intimidad es la esfera personal, donde hay información que las personas no comparten con nadie y otra información que comparten con las personas del grupo más íntimo, cercano y de confianza, será la persona titular de la información la única con derecho y potestad a transformar un dato íntimo en un dato privado o incluso público.

Cuanto mayor claridad conceptual podamos aportar, mejores serán las herramientas que podamos desarrollar a la hora de prevenir, concientizar y legislar.

La influencia de la informática, su verginoso avance y el atravesamiento cultural y la globalización que permitió el crecimiento de internet, como hecho social y tecnológico revolucionario del siglo anterior y del actual, presenta aspectos multifacéticos y pluridisciplinares. Los intereses económicos involucrados en el tratamiento de la información impulsa el desarrollo de nuevas tecnologías y genera “necesidades” que antes no existían. Ese poder debe ser necesariamente tenido en cuenta a la hora que los estados en forma particular y la comunidad internacional ejerzan su función de garantes de los derechos humanos más fundamentales. La intimidad es parte constitutiva, estructural y subjetivizante del ser humano y es un concepto más restringido y puntual que el de privacidad.

Cuando nos referimos al poder de las comunicaciones globales, de la telefonía y de los medios de geolocalización ya no hablamos de un poder futuro sino de un poder actual, presente e inminente. Frente a ese desmesurado poder, los ciudadanos del mundo merecen una adecuada protección a su intimidad, única forma de mantener la subjetividad en un mundo globalizado.

Referencias

DIAZ ROJO, José Antonio, Privacidad: ¿neologismo o barbarismo?, Consejo Superior de Investigaciones Científicas, 2002, Disponible en: http://pendientedemigracion.ucm.es/info/especulo/numero21/privaci.html

PIERINI, Alicia, LORENCES, Valentín, TORNABENE, Inés, Hábeas Data, Derecho a la Intimidad, Buenos Aires, Editorial Universidad, 1998, pág. 237 y segunda edición actualizada y mejorada de 1999, pág. 219.

ELIAS, Miguel Sumer, Régimen Jurídico de los Bancos de Datos, Situación legal de los datos de carácter personal
frente a las nuevas tecnologías, Programa de Actualización en Derecho Informático,2000, Disponible en: http://
http://www.aaba.org.ar/bi130015.htm.
BERTONI, Eduardo -Compilador, Hacia una Internet libre de censura. Propuestas para América Latina, Buenos Aires,
Centro de Estudios en Libertad de Expresión y Acceso a la Información, Universidad de Palermo, Facultad de Derecho,
2012.

# Autora: Inés Tornabene

# 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

**Protección de datos y habeas data: una visión desde Iberoamérica.**

Esta obra ha sido premiada con un Accésit en la XVIII Edición del Premio Protección de Datos Personales de Investigación de la Agencia Española de Protección de Datos, correspondiente al año 2014, en la modalidad de trabajos originales e inéditos sobre países iberoamericanos.

La obra, que puede ser consultada aquí http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/premios_2015/Proteccion_de_datos_y_habeas_data.pdf , ha sido coordinada por Daniel López Carballo y Francisco Ramón González-Calero Manzanares (coordinador adjunto) y en ella han participado juristas de once nacionalidades: Aristeo García González, Claudio Ragni Varga, Claudio Roberto Santos, Cynthia Téllez Gutiérrez, Daniel López Carballo, Dulcemaría Martínez Ruíz, Edgar David Oliva Terán, Francisco Ramón González-Calero Manzanares, Héctor E. Guzmán Rodríguez, Javier Villegas Flores, João Ferreira Pinto, Jorge Augusto Tena Ramírez, Jorge Luís García Obregón, José Luís Colom Planas, Laura Vivet Tañà, Marta Sánchez Valdeón, Matilde Susana Martínez, Romina Florencia Cabrera, Ruth Benito Martín, Salvador Serrano Fernández y Wilson Rafael Ríos Ruiz.

La protección de la privacidad es un derecho fundamental y este derecho contiene dentro de sí la protección de datos y la figura del Habeas Data. Cada vez son más los países iberoamericanos que cuentan con una legislación específica en materia de protección de datos, así como de medios legales y organizativos para proteger el derecho a la privacidad y al honor de los ciudadanos.

Y en este contexto nace la presente obra, como análisis de los diferentes países, sus normas y

Autor: Francisco Calero

Abogado ejerciente por el Ilustre Colegio Oficial de Abogados de Madrid se encuentra especializado desde enero de 2003 en protección de datos, comercio electrónico y seguridad de la información.

Accésit de Investigación Agencia Española de Protección de Datos 2014 por: "Protección de datos y habeas data: una visión desde Iberoamérica", siendo coordinador y coautor del mismo. Certified Data Privacy Professional por ISMS Forum Spain.

Master en Relaciones Internacionales y Comercio Exterior por el Instituto de Formación y Empleo y Master Profesional en Unión Europea por el Real Instituto de Estudios Europeos. Grado en Derecho por la Universidad de Castilla-La Mancha.

jurisprudencia, clasificándolos en cuatro bloques temáticos: países con legislación específica en materia de protección de datos, países con legislación en materia de privacidad, países con legislación en materia de habeas data y otros países y el tratamiento de la protección de los datos personales. Dentro de los países del primer grupo se analizan aspectos fundamentales como bien jurídico protegido, calidad de los datos, autoridades de control, información y consentimiento o medidas de seguridad, lo que otorga a la obra una visión de derecho comparado.

Por su especial interés y actualidad se trata en tema aparte el equilibrio entre acceso a la información o transparencia y protección de datos. Igualmente cuenta con un capítulo dedicado a las especiales relaciones existentes entre Iberoamérica con Estados Unidos y Canadá, y otro dedicado a la Unión Europea, en la que se ha analizado la Propuesta de Reglamento General de Protección de Datos, actualmente en proceso legislativo, destacando las nuevas figuras, tendencias y herramientas para una mejor protección de este derecho fundamental. Cuenta finalmente con un capítulo destinado a las transferencias internacionales de datos y los requisitos que establecen las diferentes legislaciones nacionales para su validez y eficacia jurídica.

La obra cuenta finalmente con diversas tablas y anexos comparativos entre las diferentes normativas, proyectos legislativos en trámite y aquellos que han quedado en meras tentativas, así como una tabla recogiendo el tratamiento de las transferencias internacionales de datos y los requisitos que establecen los diferentes países.

La utilidad de esta obra, su valor, su justificación y la necesidad de llevarlo a cabo, nace de la necesidad de contar con una panorámica sobre las diferentes normativas en Iberoamérica que facilite a los actores políticos, económicos y sociales la toma de decisiones que puedan afectar a la protección de datos de carácter personal.

Para Daniel López Carballo: ‘Este Estudio constituye un referente internacional de consulta para aquellos que deseen tener una visión global de la normativa y jurisprudencia en materia de protección de datos de los diferentes países’. En palabras de Francisco Ramón González-Calero Manzanares, abogado español y coordinador adjunto de la obra: ‘La visión integral que aporta sobre las legislaciones iberoamericanas en materia de privacidad la convierte en una obra imprescindible para la toma de decisiones por los operadores de tratamiento de datos’.

Laura Vivet Tañá, abogada en Grupo Adade, apunta que ‘el trabajo es una recopilación de normativas, obligaciones, sentencias y cuadros comparativos que incluyen España, Andorra, Portugal y los distintos países iberoamericanos, así como sus relaciones con Europa, Canadá y EEUU que nos ayuda a tener una visión más global de la protección de datos’.

‘En un mundo globalizado e interconectado por Internet, considero que la privacidad y la protección de datos son derechos inherentes a las personas que deben ser tutelados por los ordenamientos jurídicos de todos los países y, en relación a Iberoamérica, estoy convencido de que este estudio comparado puede aportar

su “granito de arena”. Es importante conocer dónde nos encontramos ahora para así, todos juntos, poder llegar más lejos si cabe’ opina José Luís Colom Planas, Consultor Senior en Gesconsultor.

De acuerdo con Wilson Rafael Rios Ruiz, abogado colombiano especialista en propiedad intelectual y tecnologías de la información, ‘el Estudio es un documento de actualidad, ya que se analizan los proyectos de ley de Honduras, Chile y México, lo que, sin duda “muestra una radiografía” actualizada y completa de la situación actual protección de datos en Iberoamérica’.

Los autores valoran muy positivamente el trabajo realizado, en el que han jugado un papel fundamental las nuevas tecnologías. A este respecto ‘Internet ha acercado a los profesionales que trabajábamos desde nuestros diferentes países, eliminando las distancias y las barreras geográficas’, apunta Cynthia Téllez Gutiérrez, responsable del proyecto Datea Seguro en Perú. Una experiencia muy enriquecedora desarrollada ‘entre tantos compañeros desde diversos puntos de toda Iberoamérica, lo que refleja también el avance y las nuevas capacidades de trabajo colaborativo y a distancia’ manifiesta Ruth Benito Martin, titular del despacho Bussola.

Por su parte, João Ferreira Pinto, abogado portugués especialista en privacidad, afirma, en su lengua natal, que ‘o prémio AEPD para esta obra coletiva sobre proteção de dados no espaço Ibero-americano constitui, pessoalmente, mais um reconhecimento internacional da importância da sintonia dos princípios orientadores do “elevado nível” de proteção de dados pessoais, muito para além da União Europeia. Em particular, num espaço com uma forte identidade e afinidade linguística e cultural, como sucede com a “comunidade” Ibero-americana, com as suas múltiplas diferenças e especificidades’.

Héctor Guzmán Rodríguez, director del Área de Protección de Datos Personales y Privacidad de BGBG Abogado en México, concluye afirmando que ‘el nivel de investigación y la calidad de los trabajos que cada año recibe la AEPD, nos debe hacer sentir muy orgullosos por el reconocimiento que los colaboradores del Estudio hemos recibido. Es, además, un incentivo para continuar promoviendo la cultura de la protección de datos que promueve el Observatorio, y que tanta falta hace’, mismo sentido en que Jorge Luis García Obregón, abogado nicaragüense especialista en nuevas tecnologías, explica que ‘este premio refuerza el trabajo realizado y nos anima a seguir avanzando, plantear nuevos proyectos e ideas y afrontando nuevos retos’.

# El Consultor en seguridad informática

**Responsable:**
**Franco**

# Vergara

# Troyano SMS a la carga de Android.

**Autor: Franco Vergara**

Un conocido diario de Buenos Aires, El Cronista Comercial, alertó con respecto al significativo número de amenazas del malware Troyano SMS registradas durante el segundo trimestre de 2014, dichas amenazas se triplicaron en el último año.
No soy muy conocedor de Android pero esta noticia me generó curiosidad y hacer este artículo me obligó a empaparme un poco más en esta tecnología que muchos utilizamos a diario, que crece a diario y seguramente tiene mucho camino por delante.

Ahora empecemos a profundizar un poco en esto del "malware Troyano SMS" que dice el diario que viene amenazando a los dispositivos con Android en crescendo. La palabra "Malware" no es ni más ni menos que "software maligno" asi que no hay que hacer mucho hincapié en esta, vamos directamente a enfocarnos en los Troyanos SMS.

Cualquier persona sin mucho conocimiento de informática entendería a la palabra "Troyano" como un habitante de Troya, porque realmente ese es el significado, pero informática y sobre todo en seguridad informática un Troyano (o un Caballo de Troya) es un software malicioso que se muestra al usuario como un programa genuino e inofensivo, pero que, al ejecutarlo, otorga a un atacante el acceso remoto al equipo infectado. El término "Troyano" aparece de la historia del Caballo de Troya mencionado en la epopeya griega "La Odisea" de Homero.

Si bien pueden realizar diferentes tareas, mayormente los troyanos crean un backdoor (una puerta trasera) que le permite a un usuario no autorizado la administración remota del equipo, y si bien los troyanos entran dentro de la clasificación de virus informático pueden no funcionar como tales. La diferencia fundamental entre ambos es que el virus siempre provoca daños en el equipo infectado mientras que el troyano puede ser utilizado solo para monitorear o robar información sin provocar perjuicio. Recuerdo el primer acercamiento que tuve con este tipo de programas allá por los albores del 2000. Habián 2 muy populares: Sub7 y Netbus y que eran muy, pero muy faciles de usar y que por eso era peligroso que ese programa cayera en manos de alguna persona con pocos conocimientos y malas intenciones.

Estos programas estaban divididos en 2 archivos ejecutables, uno iba instalado en la máquina de la víctima y el otro se utilizaba para controlar dicha máquina remotamente y con la ayuda del empaquetador que Windows 98 traia en forma nativa era muy fácil camuflar al primer archivo con un ícono de ICQ, de Microsoft Messenger o de cualquier otro programa que a la víctima le genere confianza instalar en su computadora. También recuerdo el repudio de los hackers de elite contra estos programas que hacian sencillo el trabajo que a ellos les tomaba largas horas de investigación y pruebas.

## ¿Que es Troyano SMS?

En agosto del 2010 Kaspersky Lab, una empresa Rusa que se encuentra entre las cuatro mejores soluciones de seguridad informática del mundo, anunció la detección del primer programa malicioso clasificado como “Troyano-SMS” para smartphones (teléfonos inteligentes) con sistema operativo Android de Google. Bautizado como Trojan-SMS.AndroidOS.FakePlayer.a. El infectó a numerosos dispositivos móviles en todo el mundo.

El Troyano SMS es un tipo de malware que se instala en el dispositivo de la vítcima y utiliza el servicio de mensajeria SMS para generarle gastos al dueño del teléfono. Estos

gastos se convierten en dinero que va a parar a la cuenta del ciberdelincuente.

## ¿Cómo llegan y Cómo se van?

Al mejor estilo "empaquetador de Windows 98" este programa malicioso llega a los smartphones Android disfrazado de un inofensivo software multimedia como puede ser un Ajedrez, Sudoku, Dominó o cualquier programa popular y gratuito que se pueda descargar del Playstore de Google. Luego, y con la ayuda del desinterés del usuario que acepta las condiciones de uso del programa recientemente descargado que incluyen el acceso a las fotos, mensajes de texto, datos presonales del teléfono y un sin fin de requerimientos más que solicita un juego este juego de dominó, por ej, el malware tiene vía libre para hacer de las suyas.

Por suerte y para los distraidos existen en PlayStore reconocidas soluciones de seguridad gratuitas y no como Avast, Avg y McAffe que trabajan en tiempo real consumiendo poca memoría y otorgando muy buenos resultados. particularmente utilizo en mi teléfono móvil el antivirus de Avast y me viene dando muy buenos resultados.

Todos los programas que descargamos e instalamos necesitan algún tipo de privilegio sobre nuestro teléfono para poder funcionar. Lo que yo recomiendo es leer en detalle cuál/cuales son los permisos que estan solicitando. Por ej. si descargamos un software de gps estaría bien que solicite permiso a la red de nuestro equipo pero no que necesite ver todas nuestras fotos. Es muy común ver en Playstore que 4 programas de la misma temática, un juego de cartas por ejemplo, soliciten permisos completamente diferentes en nuestro teléfono para poder funcionar y lo que vamos a hacer nosotros en este caso es descargar e instalar el que solicite los requerimientos mínimos e indispensables y así evitamos cualquier futuro problema.

Otro modo de evitar infectarse con este peligroso tipo de software malicioso asociado con el robo de dinero y de datos personales, es instalar aplicaciones sólo desde tiendas oficiales como Google Play, Amazon y App Store. Asegurarse de desactivar la opción de (in)seguridad “Permitir la instalación desde fuentes desconocidas” de el menú de ajustes.

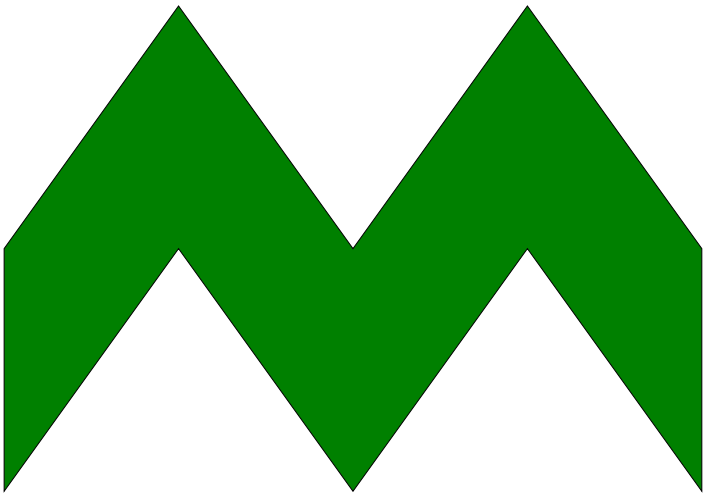
## Malas noticias

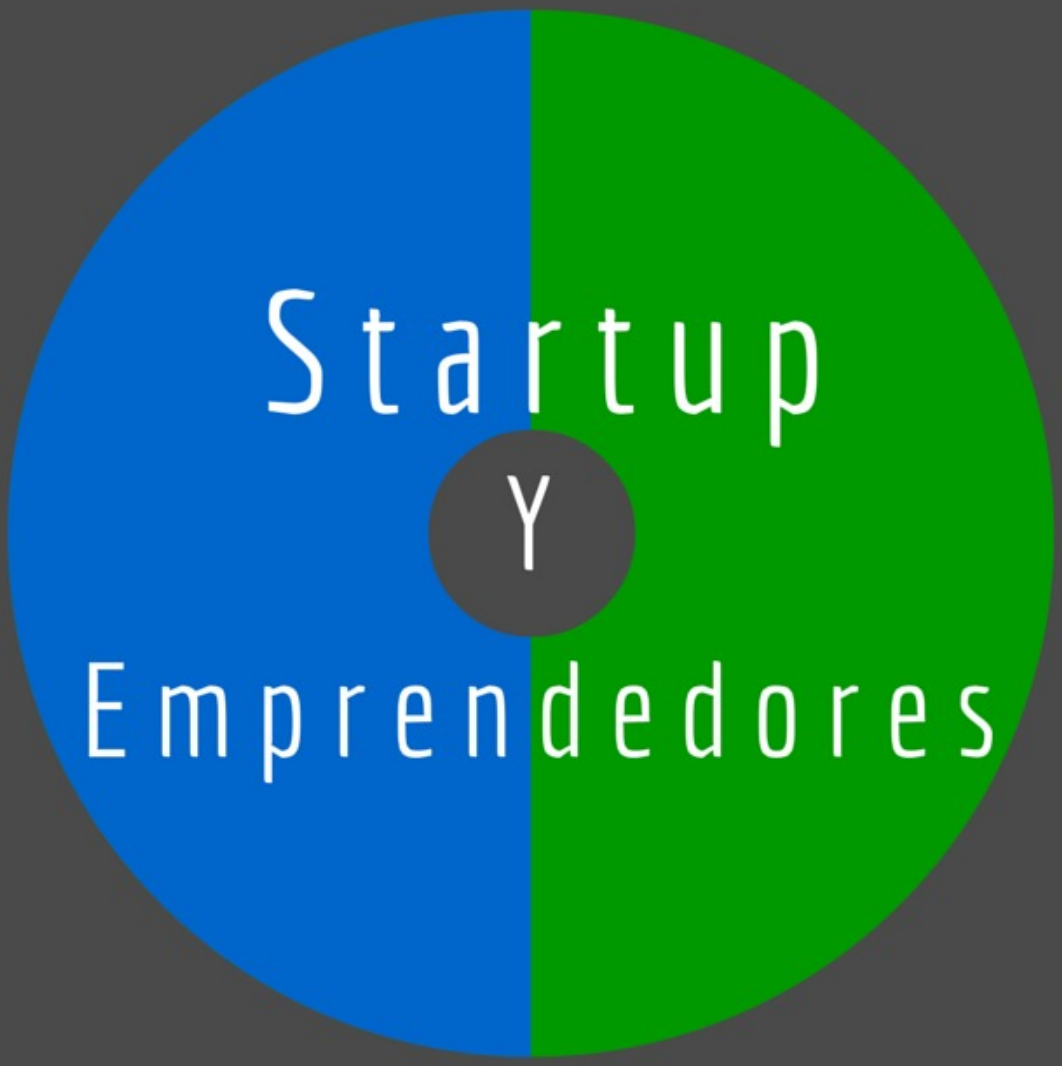
En el primer trimestre de 2014 se descubrió un troyano para iOS. Este malware es un plugin para Cydia Substrate, un popular framework para los dispositivos "liberados" (iOS jailbreaking). Lo que hace el troyano es hacerse del dinero de la publicidad que dejan algunos programas reemplazando en sus módulos el ID de los creadores del software por el de los delincuentes.

## Conclusión

Android es uno de los sistemas operativos para dispositivos móviles más populares en el mundo, por lo tanto atrae la atención de delincuentes informáticos que apuntan sus cañones directamente a la información privada y al dinero de los usuarios. Para mantenernos seguros debemos pensar en nuestros dispositivos móviles (celulares, laptop) como en nuestra casa, es decir, ambos son contenedores de información privada y sensible por lo tanto si a nuestra la casa le ponemos una buena cerradura, pagamos un seguro y hasta contratamos un sistema de alarma usemos en nuestros dispositivos móviles una clave robusta de acceso, un buen antivirus y hasta un firewall si lo creyeran necesario.

Lic. Franco Vergara
Especialista en Seguridad Informática






Responsable: Dr. Jorge Luis Garcia Obregón

Hace pocos días estaba leyendo un artículo en una revista de Telefónica, titulado ***¿Cómo convertirse en una pyme digital?*** Escrito por David Álvarez de la cuenta en twitter @cicloencicloped.

El artículo en si aborda temas muy interesantes como son ***<<la necesidad de migrar de la forma de negocios tradicionales al cloud>>***, por ejemplo se retoma el muy conocido caso de KodaK, compañía internacional dedicada a la venta de cámaras fotográficas y la venta de rollos de cámara, la cual dejó escapar la oportunidad de incursionar en el mercado de cámaras digitales por conservar el jugoso negocio de revelación de rollos. Sin embargo, esta oportunidad fue aprovechada por la competencia como Sony, Canon y Nikon, que no escatimaron en pasar por encima su gran rival y tomar su cuota de mercado.

La transformación hacía la esfera digital no es algo imperativo de las grandes compañías, pues el que manda es el cliente y quien exige es él.

Por eso es imperativo reinventarse, saber cambiar la estrategia. Son varios los ejemplos que podemos tomar de las empresas que en un tiempo relativamente corto han pasado de la supremacía a la insignificancia total y absoluta, tales como: Daewoo, Nokia y Blackberry (por cierto este último era uno de mis *smartphones* favoritos).

Otro ejemplo que podemos tomar es la de *Sega Megadrive*, que fue la mamá de tarzán (frase nicaragüense ocupada para referirse a algo espectacular) de todas las consolas de videojuego hasta el 94 que fue destronada por otros competidores, como *Nintendo*. Sin embargo, hicieron un poco de fuerza y lanzaron al mercado una consola llamada *Saturn* y luego la *Dreamcast*, pero no fueron oponente digno para la versátil y magnifica caja encantada que atacó al segmento juvenil y maduro a la vez, el *Playstation* de Sony.

Los beneficios para convertirse en Pyme Digital son muchos, dentro de los que podemos enunciar de manera indicativa, aunque sabemos que hay más, veamos:

1) ***Ahorro de tiempo y dinero:*** La utilización de TIC's ayuda a minimizar algunos gastos como espacios, muebles para tener libros y otros más.
2) ***Un universo de clientes:*** Las RRSS han exponenciado el ***target*** de clientes que podemos tener, tanto a nivel nacional como internacional.
3) ***Agilidad en los servicios:*** A través de las TIC's, podemos acceder de manera más rápida a cualquier información o gestionar nuestro negocio, inventario, ventas, etc.
4) ***Fidelización de clientes:*** Las TIC's nos ayudan a estar en contacto constante con los clientes, logrando crear un lazo de personalización en los servicios brindados.

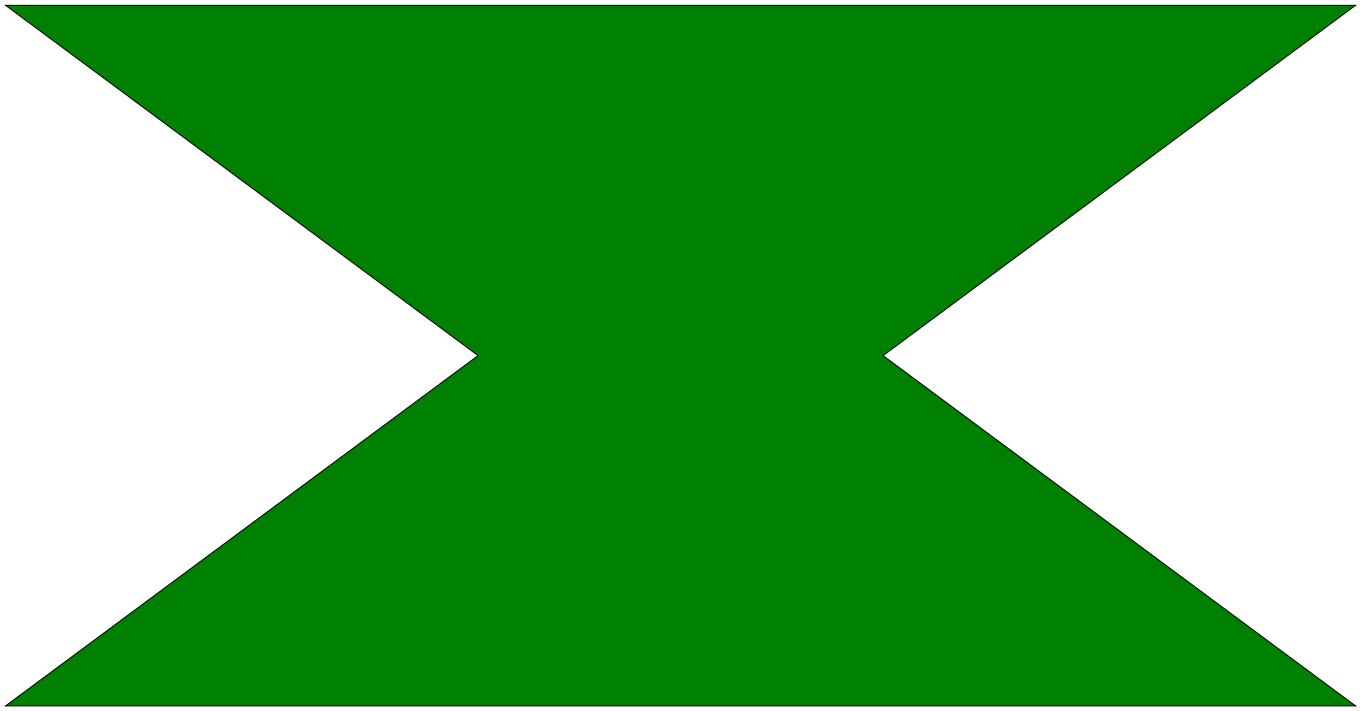
Hay muchas formas de pasar de la venta tradicional a la virtual, por ejemplo veamos el caso de una librería. Para poder funcionar esta requiere tener un espacio físico, inventarios, muebles, personal, etc… Para una librería virtual (sea de entrega de libros en físico o en formato digital), los costes se te reducen en un 90% por cuanto ya no requerís tener el espacio físico que mencionamos, basta y sobra con la sala de tu casa y tu ordenador, para los inventarios bien puedes guardar los libros en un espacio cualquier y mandar vía *courier* el que vayas vendiendo, en muebles y personal, olvídate! Vos serás el ***manager***, ***sales representative*** and ***office boy***…

En lo particular he conocido de caso donde la transición de empresa tradicional a digital ha sido paulatina y poco organizada, donde los gastos en TIC's han sido sin retorno alguno por la falta de estrategia, tales como no tener una referencia de como quieres verte y hacía donde

quieres ir… También, solo montar un website para tener una tarjeta de presentación, no es vender online, eso es estar en internet, solo por estar.

En la web hay mucha información para que te nutras y puedas tener un ***training*** digno de un futuro emprendedor digital. Busca la información capacítate, crea diferencia y márcala, pero que se note.

Mientras tanto nos seguimos por estas vías…



www.itaxlegal.com

TAXLEGAL

Derechos de Negocios/ Planificación Fiscal/ Derecho deTICs

El Blog de Jorge Garcia

# ELDERECHOINFORMATICO.COM

## TODA LA INFORMACIÓN EN UN SOLO LUGAR