

REVISTA DIGITAL DE LA RED IBEROAMERICANA DE DERECHO INFORMÁTICO

EL DERECHO Informático

REVISTA Nº 9 - OCTUBRE 2011

WWW.ELDERECHOINFORMATICO.COM



La Revista Electrónica de la Red Iberoamericana de Derecho Informático es una publicación de elderechoinformatico.com
Revista de publicación y difusión gratuita. Todos los contenidos de esta publicación están bajo Licencia Atribución-No Comercial-
Compartir Obras Derivadas Igual 2.5 Argentina de Creative Commons. (BY-NC-SA).

Colaboran en esta edición:

Jorge Larrea de Rossi; Abog. Leonor Guini; Sergio Mendoza; Abog. Sabrina Comotto; Abog. Tania Sagastume;
Prof. María C. Chimeno Fernández; Carla Pellegrini y Lorena Muracciole; Abog. Evangelina Checa; Abog.
Bárbara Peñalosa; Lic. José Luis Chavez Sanchez; Jorge Goulou (IBM)



Todo en un solo lugar



RED IBEROAMERICANA

ELDERECHO Informático.com

LA COMUNIDAD DE DERECHO INFORMÁTICO MÁS GRANDE DE IBEROAMÉRICA

REVISTA N° 9 - WWW.ELDERECHOINFORMATICO.COM

OCTUBRE 2011

REVISTA DIGITAL DE LA RED IBEROAMERICANA DE DERECHO INFORMÁTICO

pág. 5	El despido motivado en el uso irregular del mail laboral. <i>Jorge Larrea de Rossi</i>	
pág. 19	Opinión del proyecto S-3732/10 sobre imposición de remuneración por copia privada <i>Abog. Leonor Guini</i>	
pág. 23	Los costos del Software Privativo <i>Sergio Mendoza</i>	
pág. 25	Contrataciones Públicas Electrónicas <i>Abog. Sabrina Comotto</i>	
pág. 27	Análisis de la Política de Seguridad de Facebook <i>Abog. Tania Sagastume</i>	
pág. 33	Realmente hemos avanzado en lo que denominamos Gobierno Electrónico dentro de los Organismos que conformamos la APN. <i>Prof. María C. Chimeno Fernández</i>	
pág. 37	El crecimiento del Teletrabajo: Análisis de sus variables positivas y negativas. Su Contexto. <i>Carla Pellegrini y Lorena Muracciole</i>	 
pág. 41	El Teletrabajo y su previsión normativa en la República Argentina. <i>Abog. Evangelina Checa</i>	
pág. 45	Evidencia Digital: Admisibilidad y valoración en el derecho procesal civil y penal de la provincia de Mendoza (Argentina) - Parte 2 <i>Abog. Bárbara Peñaloza</i>	
pág. 51	Sellos de Confianza: Incrementando la Seguridad en el Comercio Electrónico <i>Lic. José Luis Chavez Sanchez</i>	
pág. 53	Entrevista a Jorge Goulu (Presidente de IBM Argentina)	

DERECHO Informático

ELDERECHOINFORMATICO.COM

Directores

Téc. Marcelo Temperini - mtemperini@elderechoinformatico.com

Abog. Guillermo Zamora - gmzamora@elderechoinformatico.com

Edición, Diseño y Maquetación

Téc. Marcelo Temperini - mtemperini@elderechoinformatico.com

Redacción y Edición

Abog. Guillermo Zamora - gmzamora@elderechoinformatico.com

Contacto: info@elderechoinformatico.com

Colaboradores Octubre 2011

Responsable Sección Seguridad de la Información

Lic. Cristian Borghello - segu.info@gmail.com

Colaboran en este número

Jorge Larrea de Rossi

Abog. Leonor Guini

Sergio Mendoza

Abog. Sabrina Comotto

Abog. Tania Sagastume

Prof. María C. Chimeno Fernández

Carla Pellegrini y Lorena Muraccione

Abog. Evangelina Checa

Abog. Bárbara Peñaloza

Lic. José Luis Chavez Sanchez

Jorge Goulu (IBM)

La Revista Electrónica de la Red Iberoamericana de Derecho Informático es una publicación de elderechoinformatico.com
Revista de publicación y difusión gratuita. Todos los contenidos de esta publicación están bajo Licencia Atribución-No Comercial-Compartir Obras Derivadas Igual 2.5 Argentina de Creative Commons. (BY-NC-SA).

Todas las opiniones publicadas en los artículos, reflejan únicamente la opinión de sus respectivos autores, no condicionando ni expresando opinión alguna por parte de los directores o colaboradores de la Red Iberoamericana de Derecho Informático - elderechoinformatico.com





No sólo de pan vive el hombre, y en mi caso, podría decirse que de derecho informático tampoco.-

Hace un tiempo, me toco acompañar a un cliente a una audiencia sobre cuestiones relativas a cuota alimentaria y el régimen de visita respecto de su hijo de 4 años.-

La audiencia en si era normal, la discusión, la de siempre, que vos no pasas la plata, que el chico no quiere venir a verme que lo malcrías, que le hablas mal de mi, etc etc, quienes hayan ejercido en cuestiones de familia sabrán de que les hablo y los que no... pues vaya suerte tienen!.-

Como decía todo transcurría relativamente dentro de los carriles normales de estas audiencias cuando uno de ellos, en un rapto de sincericidio dice:

- Padre 1: Lo que pasa es que el chico no me quiere porque vos haces todo lo posible para que no lo haga.-

Padre 2: Yo?? – respondió el otro – decime que hago..., dale decime!! Si lo levanto, lo baño, le doy de comer, lo llevo al parque, jamás le hablo mal de vos!!!.-

- Padre 1: Ves!!! Te parece poco!! Como el chico no te va a querer más si haces todo lo que el quiere!! Por eso no quiere estar conmigo, nosotros estamos en casa... tengo derecho a dormir una siesta y no salir... El silencio fue importante... nos miramos y nadie dijo nada... estaba pidiendo que atienda menos a su hijo, que en lugar de preocuparse, atenderlo, mimarlo, estar pendiente, no le diera tanto porque él no quería darle más...

Se me ocurrió que algo similar está pasando con el derecho la gente y la tecnología, esta/mos pidiendo a la ley que no sea tan ley, que la gente no puede cumplir lo que está pidiendo, que la tecnología es mucha, que la solución no está en las personas está en las cosas... y déjenme decirles que el problema nunca son las cosas...

Abog. Guillermo Zamora



En esta oportunidad, quisiera dedicar algunas palabras al uso responsable de la tecnología. Particularmente, he tenido la oportunidad de poder realizar varias charlas en escuelas secundarias, intentando explicarles a los chicos (y no tan chicos) que deben realizar un Uso Responsable de las Nuevas Tecnologías.

En estas charlas, si bien se da un repaso de los riesgos más comunes relativos a la Seguridad de la Información, se intenta hacer foco en que tomen conciencia de sus datos personales, y las probables consecuencias futuras que tiene que hoy bajen tanto la barrera de su derecho a la privacidad.

El panorama es realmente preocupante en este sentido, dado que es un mezcla explosiva entre la necesidad de muchos chicos de "pertenecer", de una sociedad (de grandes y chicos) que sobrevalore el hecho de tener X cantidad de amigos, o seguidores, o millas por volar. A eso, se le suma que los propios medios de comunicación (en especial de los nuevos dispositivos de celular y de servicios de Internet) que alimentan esta FALSA necesidad de estar conectado todo el día, y compartirlo absolutamente todo...

¿La explicación? Un NEGOCIO. Un negocio para las principales redes sociales, pero también para los que fabrican dispositivos, casi exclusivamente diseñados para conectarse a esas redes.

¿El problema? Cada vez conozco más personas (de más de 25) que no pueden dejar de chequear sus mails, que no pueden dejar de conectarse al msn, que no pueden dejar de chequear los últimos comentarios que les han dejado en el Facebook. Similar al que necesita salir del lugar para fumar un cigarrillo, muchos hoy no pueden concentrarse en sus trabajos o estudios por que cada 5 minutos necesitan chequear el móvil.

Mi pregunta es: Si esto pasa hoy con las personas que nacieron sin tanta tecnología, ¿Como será el futuro de esta nueva generación de chicos que ya han nacido conectados y no conciben la vida sin internet?

Marcelo Temperini

EL DESPIDO MOTIVADO EN EL USO IRREGULAR DEL E-MAIL LABORAL

I. INTRODUCCIÓN.-

Mucho se ha discutido ya, sobre los nuevos debates que surgen en las relaciones de trabajo, motivados por el uso de las tecnologías de la información (TICs) (1) y, en especial, el correo electrónico y la Internet. Y es que, estas -ya no tan nuevas tecnologías han revolucionado y modificado nuestras vidas, y se han interiorizado en los usos sociales de todos los países y culturas.

Así, la revolución informática –comparable a la revolución industrial- con la Internet como su principal carta de presentación, ha dado forma a nuestra actual y transformada “Sociedad de la Información” (2) caracterizada por estas nuevas formas de acceder a la “información” y de producirla -siendo, esta, uno de los bienes de mayor valor en la actualidad- así como nuevas formas de relacionarnos y comunicarnos con las personas y, desde luego, nuevas formas de organización del trabajo y de prestación de los servicios.

En efecto, los nuevos motivos de conflictos laborales vinculados al mal uso de las tecnologías facilitadas a los trabajadores pasan por –durante el horario de trabajo- hacer uso de la computadora para realizar trabajos de otros empleos; acceder a paginas web que no tienen vinculo alguno con las labores; mantener conversaciones vía Chat o Messenger; realizar cursos a distancia haciendo uso de la computadora y el Internet de la empresa; participar de juegos on-line, descargar documentos, foto-



Jorge Larrea de Rossi es Consultor en Temas Laborales. Miembro del Gabinete de Asesores de la Presidencia del Consejo de Ministros de la República del Perú.

grafías, audios o videos de ocio, humorísticos o pornográficos; sobrecargar y hasta bloquear la red de la empresa; infiltrar virus, gusanos, troyanos y otros que afectan los sistemas del empleador; usar para fines personales el correo electrónico asignado; situaciones de acoso o insultos, vía e-mail, entre trabajadores; responsabilidad de la empresa frente a terceros por el mal uso del email institucional; competencia desleal, espionaje industrial, fuga de información sensible o comisión de delitos informáticos y un largo etcétera...

¿Cuál es la respuesta del Derecho Laboral frente a estas situaciones?, el debate internacional sigue abierto -y se enriquece cada vez más- enfrentando posiciones divergentes y pudiéndose encontrar abundante información sobre los diferentes matices y complejidades que el uso de estas tecnologías puede suscitar en el seno de las relaciones de trabajo. Así, quien se aproxime al tema se vera frente a diferentes (y a veces contradictorias) posiciones doctrinales, jurisprudenciales y –en algunos países- incluso ya legislativas (3). No existe, pues, a la fecha una tendencia clara respecto a las solu-

nes que el Derecho Laboral debe dar a estos nuevos conflictos.

En todo caso, queda claro que la preocupación de los trabajadores gira en torno al desarrollo de su vida privada dentro de la empresa, mientras que el interés principal de los empleadores no es si los trabajadores gastan bromas a sus compañeros, si mantienen correspondencia electrónica con sus novias o si son adictos a la pornografía colgada en Internet. La preocupación empresarial, no es sino la misma de siempre: Productividad, ¿Que tan bien aprovechado esta el tiempo de trabajo que los empleadores pagan? y ¿Cómo se usan las herramientas de trabajo que el empleador pone a disposición de sus trabajadores?”

II. EN EL PERÚ, EL USO IRREGULAR DEL E-MAIL LABORAL ¿PUEDE MOTIVAR UN DESPIDO?.-

El uso del e-mail que el empleador asigna a sus trabajadores, ha generado gran controversia en el Perú y en el derecho comparado; pues si bien –y sin lugar a dudas- el e-mail laboral es una herramienta de trabajo, también es un medio de comunicación, cuyo uso “social” es una costumbre habitual y su rapidez y bajo coste no genera en los trabajadores mayor reflexión sobre el hecho de que el uso para fines personales de esa herramienta de trabajo constituye una infracción laboral sancionable.

El uso de los bienes de la empresa en beneficio propio o de terceros, su uso irregular o contrario a las indicaciones del empleador, el uso para fines distintos a los productivos o cualquier otra figura similar, que implique darle a un bien del empleador -que nos ha sido confiado o asignado- un fin distinto al que corresponde a las necesidades propias del empleador, constituye -sin duda alguna- un acto contrario a la Buena Fe Laboral.



Sin perjuicio de ello, nuestro ordenamiento laboral contempla expresamente como causal de despido, por conducta del trabajador, a la falta grave consistente en: “La apropiación consumada o frustrada de bienes o servicios del empleador o que se encuentran bajo su custodia, así como la retención o utilización indebidas de los mismos, en beneficio propio o de terceros, con prescindencia de su valor”

En consecuencia, el uso con fines extra laborales de la herramienta de trabajo “correo electrónico” es una infracción laboral (de por sí y sin importar su contenido).

Ahora bien, sin cuestionar ello, la sanción que corresponda a dicha infracción deberá ser razonable y proporcional; no es lo mismo los e-mail entre compañeros de trabajo para coordinar dónde almorzar, que un e-mail con fotos explícitas de pornografía infantil; por lo que el despido no siempre será la sanción que corresponda.

A su vez, la sanción que se determine, tendrá que –necesariamente- ser la consecuencia de un procedimiento de investigación y acreditación de la falta, que responda a criterios legales y técnicos informáticos, que respete los derechos fundamentales de los trabajadores.

El debate jurídico, entonces, no está referido a si el uso irregular del e-mail laboral es o no es una infracción laboral, o si la infracción podría llegar a ser de tal magnitud que resulte razonable y proporcional sancionar, la falta grave, con el despido del trabajador infractor. La controversia legal se presenta en el “¿cómo?” se debe llevar a cabo el procedimiento de investigación y acreditación de la falta, pues si tal procedimiento resulta ilegal, entonces el despido no será válido.

El conflicto jurídico aparece cuando ese e-mail laboral que no debió usarse para fines personales, en efecto se mal uso y contiene –o podría contener– información “personal” del trabajador, ante lo cual aparecen varias interrogantes: ¿cómo puede el empleador definir si un e-mail realmente contiene información personal o no sin acceder a su contenido? y ante la duda ¿cómo puede entonces el empleador ejercer eficazmente su facultad fiscalizadora sobre el uso de la herramienta de trabajo?

Y es allí donde empiezan a darse, a nivel internacional, las diferencias interpretativas, legislativas, jurisprudenciales y doctrinales sobre cuál es la forma en que se debe llevar a cabo esta vigilancia sobre el buen uso de los e-mails laborales; existiendo posiciones que lo reducen a un control casi ineficaz y otras que lo vuelven un control excesivo, donde el principal punto de conflicto es la discusión sobre si el control del empleador puede alcanzar la posibilidad de tener, eventualmente, acceso al contenido de los e-mails remitidos o recibidos por los trabajadores en la cuenta de correo electrónico que se les ha asignado para sus labores.

En consecuencia, el control que el empleador realiza sobre el uso del e-mail asignado a sus trabajadores ha generado gran debate, entre lo que podría ser un conflicto del derecho fundamental al secreto de las comunicaciones privadas del traba-

jador, frente a las facultades de control y fiscalización del empleador, derivadas de su derecho fundamental a la libertad de empresa.

Por ello, somos de la opinión que ante la pregunta “¿el uso irregular del e-mail laboral puede motivar un despido?”, la respuesta jurídica laboral es un contundente Sí. Pero, ante la pregunta “¿puede el empleador fiscalizar el e-mail laboral para acreditar validamente la infracción cometida?”, la respuesta no es pacífica.

Una posible respuesta, sostiene que como parte de las facultades del empleador, este control es válido, pues sostener lo contrario desprotege a la empresa frente a los usos indebidos de sus bienes informáticos; por lo que si los trabajadores están debidamente informados y conocen de las prohibiciones, los controles y las posibles sanciones no cabe que –luego– pretendan sentirse afectados en su privacidad al hacer un uso indebido del e-mail.

Otra posición, sostiene que llevar a cabo tal control sobre los e-mail, afecta el derecho a la privacidad del trabajador, en consecuencia es ilegal; lo que nos lleva a un sin sentido por el cual los empresarios legalmente pueden ordenar a los trabajadores no hacer uso privado del e-mail, pero en ningún caso pueden abrir los correos electrónicos que los trabajadores puedan enviar o recibir incumpliendo la citada orden, con lo cual la infracción resulta imposible de acreditar y, por tanto, la sanción resulta jurídicamente imposible de aplicar.

Por la primera posición, a favor del control del e-mail laboral, se ha pronunciado –entre otros– el Tribunal Supremo Español (4); por la segunda postura ha optado –junto a otros– el Tribunal Constitucional Peruano (5).

En efecto, nuestro Tribunal Constitucional (TC) –en el celebre caso “Serpost”–, ha señalado que si

bien se reconocen las facultades del empleador y se señala el uso extra laboral del e-mail como una infracción, el control sobre estos e-mail requiere de autorización judicial previa, reconociendo un derecho al secreto de las comunicaciones "privadas" de los trabajadores, incluso cuando hacen uso personal y no autorizado de la herramienta de trabajo, correo electrónico.

Nuestra posición frente al conflicto –ardamente debatido- es que el control del empleador sobre el uso del e-mail asignado a sus trabajadores, sustentando bajo determinados parámetros y cumpliendo ciertas condiciones, puede ejercerse de forma legal y sin afectar derecho fundamental alguno, cuando se verifica que el trabajador no puede alegar una razonable expectativa de privacidad sobre el uso del email laboral en su calidad de herramienta de trabajo.

En consecuencia, y así lo hemos sostenido en trabajos anteriores (6), creemos que la sentencia del TC puede ser re-interpretada y abarcar la posición por la cuál, cuando el empleador haya establecido razonables y proporcionales mecanismos de control del e-mail y sus trabajadores tengan conocimiento de las políticas, regulaciones, controles, infracciones y sanciones vinculadas al uso del correo electrónico, no podría alegarse ninguna razonable expectativa de privacidad por parte del trabajador infractor, que hizo uso personal de la herramienta de trabajo, por lo que no podría alegarse validamente ninguna afectación del derecho al secreto de las comunicaciones "privadas" allí donde estas –expresamente- no podían darse de forma válida.

En tal sentido, el requerimiento de orden judicial previa, sería exigible sólo a aquellos empleadores que –como en el caso "Serpost"- no hayan tomado las medidas pertinentes para procurar no

generar en sus trabajadores una falsa expectativa de privacidad sobre el uso que le dan al e-mail laboral.

II. EL E-MAIL LABORAL: UNA HERRAMIENTA DE TRABAJO FISCALIZABLE.-

Por útiles y/o herramientas de trabajo puede entenderse a todos los elementos puestos a disposición del trabajador por la empresa, directamente vinculados con la prestación de servicios, y a los que facilitan la misma.(7)

El Diccionario de Derecho Laboral de Guillermo Cabanellas (8), precisa que las herramientas que la empresa les asigne, originan -para los operarios- los deberes de uso adecuado y el de custodia.

La legislación nacional no hace mayores referencias sobre los útiles y/o herramientas de trabajo, aunque el Proyecto de Ley General del Trabajo establecería explícitamente entre los deberes del trabajador el de cuidar y conservar en buen estado los instrumentos y útiles que se le hubieren proporcionado para ejecutar sus labores.(9)

En todo caso, la referencia legal expresa no resulta indispensable pues a partir del Principio de Buena Fe Laboral, se entiende que todo trabajador esta obligado a dar un uso adecuado a los útiles y/o herramientas de trabajo que su empleador le proporcione. La legislación nacional –sin embargo- sí contempla la posibilidad de sanción, sea en virtud al inciso a) y/o al inciso c) del Art. 25° de la Ley de Productividad y Competitividad Laboral (LPCL).

Los medios informáticos (10) que la empresa pone a disposición de sus trabajadores son, sin lugar a dudas, herramientas de trabajo y por tanto el uso razonable que se espera de ellas es únicamente con fines acordes a las labores encomendadas; en consecuencia -y como toda herramienta de

trabajo- el uso de los medios informáticos esta sujeto al establecimiento de condiciones y regulaciones de acuerdo a las disposiciones del empleador, a la fiscalización pertinente y la eventualidad de sanciones laborales.

Salvo en particulares actividades, el e-mail no es una condición de trabajo sino una herramienta de trabajo, la diferencia resulta importante pues siendo herramienta de trabajo, la regulación de su otorgamiento y uso depende –en principio- únicamente del empleador, en cambio si fuese una condición de trabajo, este instrumento seria exigible por los trabajadores.

Así, las condiciones de trabajo son necesarias e indispensables para el adecuado desempeño de las labores, resulta claro que en actividades riesgosas no es validamente posible que el trabajador realice sus labores sin contar con un adecuado equipo de protección personal; en cambio las herramientas de trabajo facilitan la ejecución del mismo y así resulta evidente que para una secretaria la asignación de una computadora le facilita las labores, pero no le resulta indispensable para trabajar por lo que validamente podría prestar sus servicios con una maquina de escribir o una libreta y un lapicero.

Señala VALDÉS DAL-RÉ (11) que en su calidad de herramienta de trabajo (y no de condición de trabajo) y, por tanto, perteneciente al patrimonio de la empresa, la ordenación del uso de las nuevas tecnologías encuentra en los empresarios una fuerte resistencia a integrarse en el contenido de los convenios colectivos, pues las reglas de uso del utillaje productivo no han formado parte históricamente de las materias sujetas a negociación colectiva.

Tal como lo señala THIBault (12) “el correo electrónico es una herramienta de trabajo de propiedad de la empresa (...) no cabe un derecho social al

uso del e-mail laboral, en la medida en que, no lo olvidemos, ello puede significarle al empleador unos determinados gastos, además de tener repercusiones negativas sobre la prestación laboral de sus empleados”

Es claro entonces que, el empleador no esta obligado a proporcionar un e-mail a sus dependientes, ni a tolerar un uso personal del mismo y tiene la facultad de fiscalizar el adecuado uso que se le de a esta herramienta de trabajo. Sin embargo, la discusión jurídica continua sobre la legalidad de los mecanismos de control, las formas de acreditación de la infracción y la sanción adecuada y proporcional que puedan ejercerse.

II. LA SITUACIÓN DE HECHO Y LAS FORMAS DE “CONTROL”.-

Un congresista estadounidense es sorprendido enviando correos electrónicos con propuestas sexuales a su practicante menor de edad; un trabajador español -de un importante banco alemán- es despedido en Barcelona por enviar 140 e-mails a sus amigos; un empleado de un banco estadounidense envía por “error” los datos de 1,300 clientes a una dirección electrónica equivocada; una secretaria -de un reconocido estudio de abogados limeño- es sancionada por usar el e-mail institucional para difundir cuestionables comentarios políticos en pasadas épocas electorales; un oficinista san isidrino –por error- envía un e-mail con “chistes” sumamente groseros y sexistas a todos los usuarios de la red (incluida la Gerencia); un funcionario de recursos humanos de una importante clínica limeña envía por email, a un representante de una AFP, los nombres, cargos y remuneraciones del personal sin autorización de ellos o del empleador; un ingeniero de una empresa industrial del Callao es detectado

cuando por e-mail ofrecía a una empresa competidora información sensible de su empleador; un ejecutivo de Serpost acusado de enviar imágenes pornográficas a través del e-mail de la empresa a –por lo menos- uno de sus compañeros de labores.

Los ejemplos podrían ser tan numerosos y variados como la infinidad de posibilidades y recursos que nos ofrecen, hoy por hoy, el e-mail y la Internet. Las situaciones comentadas no son ejemplos académicos sino hechos de la vida real, que seguirán produciéndose en tanto los medios informáticos de un empleador sean mal utilizados por sus dependientes.

Entonces, la situación de hecho es –en principio- tan simple como el que un trabajador utilice el correo electrónico asignado por su empleador con fines extra laborales, ello de por sí ya es una infracción laboral, tal como lo es hacer llamadas personales utilizando el teléfono de la empresa. Si ello amerita o no un despido u otra sanción más leve, deberá analizarse de forma casuística.

Ahora bien, del contenido de ese e-mail extra laboral podría –eventualmente- derivarse una segunda y quizás mas grave falta, como acoso o insultos a otros trabajadores, espionaje industrial, revelación de secretos o fuga de información sensible del empleador, competencia desleal, delitos informáticos, posesión o transmisión de pornografía infantil, etc. o quizás la verificación del bajo rendimiento o mala calidad de la prestación del servicio, cuando por ejemplo el trabajador se vincula con los clientes de la empresa vía e-mail.

El empleador, entonces, podría tomar conocimiento del mal uso que uno de sus trabajadores le viene dando al e-mail laboral, mediante “denuncia” de alguno de los destinatarios del e-mail, mediante un sistema de “control” informático permanente o mediante auditorias informáticas específicas para casos concretos.

Las empresas de cierta envergadura, suelen tener sus propios servidores de correo corporativos y asumen los costos que implican contar con las computadoras, el software apropiado, el programa de navegación y el de correo electrónico, el pago del derecho a usar el dominio que hayan establecido, la habilitación de las cuentas de e-mail asignadas a sus trabajadores, la arquitectura de la red empresarial (LAN), el mantenimiento de un servidor corporativo propio, el soporte técnico informático, la actualización y pago de licencias de todos ellos, los programas y herramientas antivirus, antispam(13), Proxy(14) y Firewall(15), así como los filtros de seguridad necesarios, el pago del acceso a Internet que brinda el ISP(16) y de ser el caso el pago adicional de la “data” es decir la infraestructura para lograr la conexión (CableNet o similares, ADSL, Red Telefónica, Fibra Óptica, etc.)

Desde el punto de vista técnico, pueden utilizarse una variedad de programas y filtros para “monitorizar” el e-mail asignado a los trabajadores; los servidores de correo corporativos –por los que debe pasar todo email antes de salir a Internet- pueden ser programados para casi todo lo imaginable: desde filtrar los correos, detectar las keywords (17), bloquear la salida o el ingreso de ciertos e-mails, registrar los títulos, documentos adjuntos, remitentes y destinatarios de los e-mails, hasta guardar copia del e-mail que se intenta enviar fuera de la empresa o hacerle llegar copia del mismo al Gerente General, etc.

Incluso, si este control no se hiciera a nivel del servidor de correo corporativo de la LAN de la empresa, eventualmente se podría hacer a nivel del Router6 del ISP –es decir el servidor gigante que maneja el ISP y al que llegan necesariamente todos los e-mails de los diferentes clientes del ISP antes de salir a Internet.

En Inglaterra, por ejemplo, un estudio(19) señala que el 55% de los empleadores encuestados controlaban el e-mail de sus trabajadores, mientras que otro estudio(20) señalaba que el 75% de los directivos empresariales encuestados pensaba que controlar y filtrar las actividades de los trabajadores en Internet era absolutamente necesario. En Estados Unidos, la AMA (21) en un estudio del año 2001 señaló que el 46.5% de los encuestados registran o controlan los e-mails de sus empleados. Mientras que la Fundación para la Privacidad publicó que la fuerza de trabajo "on-line"(22) en los Estados Unidos, en el 2001, era de 40.7 millones, de los cuales el 34% (14 millones) estaban sometidos a vigilancia continuada del correo electrónico (23).

Así, el control del e-mail laboral -que realiza la empresa- puede tener por fin:

1) Fin Preventivo o de Mantenimiento: evitar los perjuicios que causan los virus informáticos, evitar la sobrecarga de la red empresarial, evitar el exceso de capacidad de almacenamiento de las cuentas de correo o del servidor, etc. (lo cuál se puede llevar a cabo mediante un control externo de los e-mails y utilizando herramientas informáticas sin necesidad de ingresar a los contenidos)

2) Fin Organizativo: precisar la productividad individual de los trabajadores mediante la supervisión de su trabajo plasmado en e-mails y hacer un seguimiento de la correcta forma en que se brindan los servicios (por ejemplo, una adecuada atención al cliente cuando se da respuesta por e-mail para lo cuál es indispensable acceder al contenido del e-mail laboral)

3) Fin Fiscalizador: controlar de forma fiscalizadora y con afán disciplinario, el buen uso de las herramientas de trabajo a fin de aplicar sanciones a los infractores y/o reunir pruebas para sancionar

diferentes faltas laborales (se trata de buscar, detectar y/o verificar situaciones irregulares para lo cuál es indispensable acceder al contenido del e-mail laboral)

V. LA LEGALIDAD DEL PROCEDIMIENTO.-

Resulta perfectamente claro que una cuenta de correo solicitada directamente por el trabajador a un proveedor de e-mail (con costo o no) y cuya dirección electrónica contenga un dominio diferente al del empleador, por ejemplo el popular Hotmail o Yahoo, es –sin lugar a dudas- un e-mail personal al que por ninguna razón podría tener acceso el empleador (ni en los datos externos del e-mail ni mucho menos en su contenido) así se haya ingresado a dicha cuenta desde una computadora de trabajo y usando la Internet de propiedad de la empresa.

Sin perjuicio de ello, el empleador validamente podría bloquear el ingreso a dicha web de correo electrónico personal, restringir y delimitar la navegación y el acceso de sus trabajadores a esa y otras determinadas web de Internet, evitando así el uso de cuentas de correo personales y navegación extra laboral, durante la jornada de trabajo, facultad del empleador sobre la cuál no existe mayor discusión en el derecho comparado.

En cuanto al email laboral (es decir el asignado por el empleador y que tiene un dominio que suele identificar a la empresa), siguiendo a TOYAMA (24), el acceso al contenido del correo electrónico debe ser el último medio a ser usado por el empleador para detectar una falta laboral, y es que –en principio- bastaría con ubicar los destinatarios, los nombres de los archivos adjuntos o el "asunto" del e-mail, para detectar un uso extra laboral del correo electrónico que ya de por sí resulta siendo una infracción laboral.

Así cuando no exista una intromisión en el contenido del e-mail, no se requerirá discutir sobre la necesidad o no del consentimiento o autorización del trabajador para la fiscalización o del requerimiento de una orden judicial.

Ciertamente en el año 2004 el TC Peruano, en la sentencia recaída sobre el expediente N° 1058-2004-AA/TC, conocido como el caso "SERPOST", consideró que el trabajador que demandaba la acción de amparo, había generado cierto nivel de "autodeterminación personal" sobre el instrumento de comunicación "correo electrónico" que la empresa le había asignado, es decir se habría dado lo que aquí hemos llamado una "expectativa de privacidad" y esto fue así pues SERPOST carecía de una regulación interna sobre el uso del e-mail como herramienta de trabajo y no advirtió a sus trabajadores de los controles sobre las cuentas de correo electrónico.

Por tanto, consideramos que los criterios establecidos por nuestro TC (en los fundamentos 17, 18 y 21 de la sentencia) y la exigencia que se hace sobre iniciar un procedimiento judicial para poder acceder al e-mail asignado al trabajador, debería considerarse únicamente aplicable a casos de similares características al que motivo la sentencia, es decir, en los que el empleador no haya tenido una clara regulación sobre el uso de las TICs en la empresa y en consecuencia haya, negligentemente, permitido que sus trabajadores tengan una razonable expectativa de privacidad sobre el uso que le vienen dando a sus e-mails laborales.

La obtención de la mencionada orden judicial –que nos exige el TC- para poder ejercer control sobre los e-mails asignados a los empleados, será ciertamente una odisea jurídica pues la Ley N° 27697, de desarrollo constitucional, regula la facultad de fiscales y jueces para la intervención y

control de comunicaciones y documentos privados en casos excepcionales vinculados única y taxativamente a dieciséis delitos y sólo en el marco de una investigación penal, dejando fuera toda posibilidad a la investigación de una infracción laboral.

Por lo que en estas situaciones el empleador deberá limitarse a un control externo de los e-mails restringidos a remitentes y destinatarios, títulos y "tamaño" del e-mail, etc. pero nunca a su contenido.

Pero, en toda empresa donde haya existido o desde la fecha existan políticas y reglamentos de uso del correo electrónico, se advierta a los trabajadores sobre la existencia de los controles y se les informe sobre las infracciones y sanciones, no cabe tener una razonable expectativa de privacidad y sólo puede darse al e-mail el uso que el empleador haya establecido.

Por lo que consideramos, con criterio similar al del Tribunal Supremo Español, que en las empresas donde gracias a sus claras políticas y regulaciones, no cabe tener una razonable expectativa de privacidad, podrá hacerse un control no sólo externo sino también de contenidos sobre el e-mail asignado a los trabajadores, pero para que sea válido que el empleador pueda llevar a cabo estos controles y eventualmente pueda aplicar sanciones a sus trabajadores, el Empleador tendría que:

- Debe contar con una clara política de uso de las TICs de la empresa y comunicársela a los trabajadores, definiendo allí los usos, mecanismos, procedimientos, restricciones, etc. que sean aplicables a las TICs de acuerdo a la política de la empresa.

- Deberá precisar en los contratos de trabajo y/o en el Reglamento Interno de Trabajo, que el e-mail asignado es una herramienta de trabajo de uso exclusivo para fines laborales y señalar las restricciones, prohibiciones y sanciones aplicables

por el mal uso del e-mail institucional haciendo referencia a la política de uso de las TICs de la empresa.

- Deberá alertar a los trabajadores sobre la existencia de los controles, sus mecanismos y sus fines, procurando que estos sean controles mecanizados permanentes, aplicables a la totalidad de trabajadores o a aquellos escogidos de forma aleatoria y sin ningún ánimo discriminador

- Deberá procurar utilizar prioritariamente los mecanismos técnicos que permitan un control automatizado antes que un control manual, dando prioridad a un control externo de los e-mails para sólo acceder al contenido de aquellos considerados realmente “sospechosos”.

- Deberá procurar contar con un servidor de correo propio y asistirse por personal especializado a fin de llevar a cabo auditorías informáticas serias y confiables.

- Cuando realice auditorías específicas, deberá realizarlas en presencia del trabajador afectado y de ser el caso en compañía de un representante sindical, algún otro trabajador como testigo y/o un notario público.

Así, desde nuestro punto de vista y sin apartarnos de lo dispuesto por nuestro TC, consideramos que será la razonable expectativa de privacidad que validamente pueda generarse en el trabajador, el elemento que determine en que casos el empleador pueda proceder al control del e-mail laboral en virtud a sus solas facultades o cuando deberá cumplirse con lo exigido por nuestro TC.

II. LA TIPICIDAD DE LA INFRACCIÓN.-

Como hemos señalado, resulta indispensable que los trabajadores estén advertidos, previamente,

sobre la existencia de los controles y se les informe sobre las infracciones y sanciones, sólo así se podrá argumentar validamente que no cabe que los trabajadores tengan una razonable expectativa de privacidad al hacer uso indebido del e-mail laboral.

Por ello, consideramos que un empleador diligente debería asesorarse en materia legal laboral y técnica informática y hacer referencia al uso del e-mail laboral (y demás medios informáticos) hasta en tres instrumentos: Una cláusula contractual (cuando exista contrato de trabajo por escrito), un documento interno sobre las políticas y regulaciones de uso de las TICs de la empresa y en el reglamento interno de trabajo.

Los usos indebidos del email laboral deberán entenderse, por tanto, como una infracción a las políticas de uso de las TICs, cuya inobservancia resulte en un incumplimiento contractual y la sanción se encuentre tipificada en el reglamento interno de trabajo.

El eventual despido de un trabajador motivado por el uso irregular del email laboral podría basarse, en consecuencia, en la causal de “incumplimiento injustificado de las obligaciones de trabajo que supone el quebrantamiento de la buena fe laboral y/o la inobservancia del reglamento interno de trabajo”, falta prevista en el literal a) del artículo 25° de la LPCL, así como la causal de “uso indebido de bienes o servicios del empleador en beneficio propio o de terceros”, falta prevista en el literal c) del artículo 25° de la LPCL.

Pudiendo derivarse otras causales de despido, a partir de la fiscalización del e-mail, como, por ejemplo, la de proporcionar información reservada del empleador a terceros, falta grave tipificada en el literal d) del artículo 25° de la LPCL.

VII. LA PROPORCIONALIDAD DE LA SANCIÓN.-

Al detectarse un uso indebido del e-mail laboral, partiendo del supuesto de la existencia de un adecuado procedimiento de control del uso del mismo y de la inclusión de su uso indebido como falta grave en el Reglamento Interno de Trabajo, el empleador podrá aplicar las sanciones correspondientes, teniendo en consideración los principios de razonabilidad y proporcionalidad, es decir, que exista un equilibrio entre la falta cometida y la sanción aplicada, lo cual se determinará en cada caso concreto.

NÚÑEZ (25) señala: El caso de la indebida utilización de la correspondencia electrónica en materia laboral debe analizarse sobre el caso particular, siendo muy arriesgado el establecer sanciones pre-determinadas para ciertos casos por la variedad de posibles faltas que se pueden presentar y la configuración que les de el empleador, dado que no será lo mismo que, un trabajador remita pornografía a sus amigos, que un profesor de educación primaria remita pornografía a sus alumnos. En ambos casos, el hecho es el mismo (remisión de pornografía) siendo que en el segundo caso el tema se agravaría, dado que el remitente es un profesor y los destinatarios sus alumnos, y ello sí ameritaría el despido.

Por ello, creemos que sólo un uso irregular, abusivo y/o desproporcionado del e-mail laboral podría sustentar una medida disciplinaria de tal gravedad como el despido; así creemos que será irregular todo uso extra laboral -que revista gravedad- contrario a las políticas sobre uso de las TICs de la empresa o que infrinja el Reglamento Interno de Trabajo; será abusivo un uso del e-mail que cause graves perjuicios al empleador (desprestigio, difamación, revelación de secretos industriales,

etc.) o que por su contenido resulte en inaceptable (acoso moral o sexual, pornografía infantil, comisión de delitos, etc.) y/o será desproporcionado un uso del e-mail laboral que exceda los razonables límites de tolerancia que pudiese haber fijado el empleador o que por sus características de número, tamaño, frecuencia, costos, etc. resulte exagerado y reprochable.

Entendiéndose que la “tolerancia” del empleador frente a algunos usos extralaborales del e-mail no genera un derecho a su uso social y personal, siendo potestad del empleador perdonar o sancionar la falta, siempre ciñéndose a criterios de razonabilidad y proporcionalidad, no pudiéndose alegar luego que se haya generado una “costumbre” dentro de la empresa que impida al empleador sancionar lo que de por sí es un acto irregular.

Los casos menos graves tendrían que ser sancionados con amonestaciones o suspensiones y creemos válido que se tomen medidas organizativas a fin de que técnicamente se puedan hacer modificaciones de control y restricción sobre el e-mail de trabajadores infractores. Consideramos que sería válido también sancionar de formas más grave las conductas reincidentes luego de las advertencias o sanciones previas.

II. EL RIESGO DE DESPEDIR POR USO IRREGULAR DEL EMAIL LABORAL.-

Hay que resaltar (y advertir) que la discusión sobre la viabilidad de un despido motivado en el uso irregular del email laboral no es pacífica y como ya se ha mencionado, el debate jurídico se da con mayor fuerza en cuanto a la legalidad del “control” que pueda o no ejercer el empleador sobre el contenido de los email de los trabajadores.

Por un lado existen quienes sostienen que el ejercicio de la vida privada dentro del ámbito de la relación laboral, implica que el trabajador extiende parte de su “privacidad” sobre algunas facilidades que el empleador le otorga y las hace (o siente) “suyas”; por lo que tendría que poderse dar un “uso social” al correo electrónico asignado a los trabajadores, como un medio de comunicación que pueda usarse de forma privada para fines extra laborales y que en consecuencia su uso con fines personales quedaría protegido por el derecho al secreto de las comunicaciones privadas.

Llegando –incluso- a señalarse que se requeriría de autorización del trabajador para que el empleador pueda ejercer cualquier tipo de control o fiscalización sobre el e-mail que la empresa le ha asignado y que cualquier tipo de autorización general o previa a la situación concreta resultaría en ilegal pues sería una “renuncia de derechos”.

Aunque no consideramos necesaria la “autorización” del trabajador para el control del e-mail que se le asignó, cabe señalar que si esta se diera no podría hablarse de la “renuncia de un derecho” pues el trabajador no está renunciando a su posibilidad de mantener comunicaciones privadas con quiénes guste, ni renuncia al secreto de estas, sino que se está comprometiendo a no dar un uso personal (y por tanto inadecuado) a una herramienta de trabajo, pudiendo validamente sostener comunicaciones privadas a su costo, por sus propios medios y fuera del horario y/o el centro de trabajo.

Según la posición de esta parte de la doctrina, el trabajador ingresaría a la empresa con un derecho a la “comunicación social extra laboral”, protegida por el secreto y la privacidad, factible de ejercerse en las instalaciones de trabajo, durante el horario de trabajo y haciendo uso –para ese fin- de las herramientas de trabajo o los bienes del em-

pleador (y bajo el costo de este) quien no podría oponerse a tal situación, ni controlarla, fiscalizarla o sancionarla pues ello limitaría las posibilidades de desarrollo de la vida privada del trabajador en la empresa, sus posibilidades de comunicación y finalmente se terminaría violando el secreto de las comunicaciones privadas, al momento del procedimiento de acumulación de pruebas de lo que el empleador consideraba una infracción.

Frente a ello, estamos quienes sostenemos que realizar un control empresarial del correo electrónico asignado a los trabajadores –en sus aspectos exteriores y su contenido- de forma legal, razonable, proporcional y sin afectar ningún derecho constitucionalmente protegido, es posible en virtud a la sola facultad de fiscalización del empleador (sin querer una orden judicial como lo ha señalado nuestro TC).

Esto es así en tanto el e-mail institucional es una herramienta de trabajo fiscalizable como cualquier otra; el uso indebido del e-mail con fines extra-laborales implica no sólo un aprovechamiento desleal de los recursos de la empresa, sino también un perjuicio al empleador por las horas acumuladas de improductividad, así como diversos perjuicios que eventualmente pudiesen derivarse del mal uso del correo electrónico asignado a los trabajadores; la facultad del empleador para poder ejercer tal control deriva del poder de dirección, fiscalización y sanción del empleador (Art. 9° de la LPCL) los cuales son una expresión de su derecho fundamental a la libertad de empresa (Art. 59° de la Constitución) y en consecuencia, el empleador tiene reconocida la facultad legal de sancionar las situaciones de un uso indebido del e-mail en virtud al literal a) y c) del artículo 25° de la LPCL.

Y es que amparar que un trabajador mal utilice el argumento del secreto de comunicaciones

“privadas” para obstruir la probanza de una infracción laboral es una situación de Abuso de Derecho (26), siendo que NO existe el mal llamado “derecho” a un “uso social” de la herramienta de trabajo correo electrónico –ni de ninguna otra- por parte de los trabajadores.

El Tribunal Constitucional Peruano (27), la Cour de Cassation Francesa (28), el Tribunal de Trabajo de Bruselas (29) y otros, se han pronunciado en contra de la facultad de control y fiscalización del empleador sobre el email laboral asignado a sus trabajadores.

Los Jueces de Estados Unidos (30), Argentina (31), Uruguay (32) y Costa Rica (33), así como el Tribunal Supremo Español (34), la Dirección de Trabajo de Chile (35), entre otros, se han pronunciado a favor del control empresarial del e-mail asignado a los trabajadores.

En consecuencia, el debate sobre la facultad de control y el despido que, en virtud, a ella pudiese darse, ha sido, es y –seguramente- seguirá siendo un tema en constante discusión y evolución.

Lo cierto es que nuestro Tribunal Constitucional (equivocado o no) ha señalado ya el principal precedente que sobre la materia existe en el país y por tanto debe cumplirse, pero para ello se hace necesaria una re-interpretación de sus criterios que resulte acorde a la realidad de las relaciones laborales.

Frente a la sentencia del TC en el caso “serpost” y su exigencia de contar con una orden judicial antes de verificar el contenido de un email asignado a un trabajador, los empleadores (y sus asesores legales) tendrán que optar entre, cuando menos, estas opciones para enfrentar el uso irregular del email laboral de sus trabajadores:

1.NO controlar los contenidos de los emails laborales.

2.Solicitar a los trabajadores una autorización expresa para controlar sus cuentas de correo electrónico, en cada oportunidad en que se pretendan realizar auditorias informáticas (y depender de la voluntad del trabajador de autorizar o no ello)

3.Establecer un email interno (no fiscalizable) que sólo comunique a los trabajadores entre sí y establecer que sean ellos quienes deban solicitar autorización por cada email que quieran enviar fuera de la empresa (condicionado a fiscalización).

4.Establecer, como hemos sugerido, cláusulas contractuales, políticas de uso, regulaciones en el reglamento interno de trabajo y, de ser posible, convenios colectivos que permitan argumentar que no es válida una razonable expectativa de privacidad al hacer uso indebido del e-mail laboral y en virtud a ello ejercer los controles y aplicar las sanciones. Pudiendo fijarse márgenes de tolerancia respecto a ciertos usos no sancionables o estableciendo alguna especie de “cabina pública”, dentro de la empresa, desde la cuál se pueda usar emails personales.

Proponemos pues, con respaldo legal y en base a jurisprudencia y legislación de derecho comparado, una ampliación y re interpretación del criterio de nuestro TC que creemos resulta sólo aplicable a supuestos donde, como en caso Serpost, el trabajador se haya generado una expectativa de privacidad, pero no exigible en las empresas que han sido diligentes sobre el control de sus medios informáticos.

Pero somos concientes, que aunque nuestra posición es coherente y defendible jurídicamente, para los empleadores peruanos –en el contexto actual- podría ser un riesgo aplicar un despido motivado en el uso irregular del email laboral asignado a un trabajador.

Se requerirá, pues, de un empleador que gravemente afectado por el uso indebido del email laboral, este dispuesto a sostener los argumentos jurídicos que defiendan sus facultades de control y sanción, hasta procurar un nuevo pronunciamiento de nuestro Tribunal Constitucional.

Autor: Jorge A. Larrea De Rossi

Referencias:

1- Según la OCDE (Organization for Economic Cooperation and Development) las TICs son aquellos dispositivos que capturan, transmiten y despliegan datos e información electrónica y que apoyan el crecimiento y desarrollo económico de la industria manufacturera y de servicios. OECD Reviewing the ICT sector definition: Issues for discussion. Working party on indicators for the information society. Stockholm, 25-26 Abril 2002

2- El Gobierno del Perú, en su "Plan de Desarrollo de la Sociedad de la Información en el Perú: La Agenda Digital Peruana" (Puede consultarse en: <http://www.peru.gob.pe/AgendaDigitalPeru/agendadigitalperu.htm>) señala que: "(...) definimos la Sociedad de la Información como: un sistema económico y social donde el conocimiento y la información constituyen fuentes fundamentales de bienestar y progreso (...)"

3- La más reciente es la modificación, en marzo del 2009, de la "Ley de Protección de las Comunicaciones Electrónicas" de Finlandia, que –ahora- permite expresamente el control del empleador de los emails asignados a sus trabajadores. Estados Unidos cuenta con un marco regulatorio a favor del control empresarial del correo electrónico de los trabajadores (véase, entre otras, la Electronic Communications Privacy Act y The Federal Wiretapping Act, ambas de 1986). El Reino Unido también ha optado por establecer normas que permiten el control del e-mail laboral (véase, entre otras, la Human Rights Act 1998, la Data Protection Act 1998, la Regulation of Investigatory Powers Act 2000 y la Lawful Business Practice Regulation 2000). En nuestra región, puede consultarse -entre otros- los siguientes proyectos de Ley: en Perú el Proyecto de Ley N° 01610/2007-CR y –más recientemente- el Proyecto de Ley N° 04345/2010-PE; en Argentina el Proyecto de Ley N° 0623-D-2007 y en Chile el Proyecto de Ley N° 5662-13.

4- Sentencia del Tribunal Supremo Español del 26 de septiembre de 2007.

5- Sentencia del Tribunal Constitucional Peruano, recaída sobre el expediente N° 1058-2004-AA/TC

6- Véase: LARREA De Rossi, Jorge. "La Libertad Sindical y el Uso de los Medios Informáticos de la Empresa" En: Actualidad Jurídica N° 189, Lima, Agosto del 2009; "El Control de los Correos Electrónicos en el Centro de Trabajo. Releyendo la Sentencia del TC Sobre el Control del e-mail Laboral" En: Dialogo con la Jurisprudencia N° 124, Lima, Enero del 2009. y "La Legalidad del Control del Empleador sobre el Correo Electrónico Asignado a sus Trabajadores" En Laborem N° 7 Revista de la Sociedad Peruana de Derecho del Trabajo y de la Seguridad Social, Lima, Octubre del 2007.

7- AGUT García, Carmen. Las facultades empresariales de vigilancia y control sobre útiles y herramientas de trabajo y otros efectos de la empresa. Revista Tribuna Social, Valencia, fascículo 163, año 2004. Pág.24-36

8- CABANELLAS de Torres, Guillermo. Diccionario de Derecho Laboral, Buenos Aires, Heliasta, 1998.

9- Esto quedaría establecido en el inciso 10 del artículo 50° de la Ley General de Trabajo, siendo una norma sobre la cuál se ha alcanzado consenso en el Consejo Nacional de Trabajo.

10- Dentro de estas herramientas de trabajo tendríamos –entre otras- a los teléfonos, telefax y celulares, las computadoras y todas sus partes integrantes y accesorias, las impresoras, fotocopadoras y escáneres, el acceso y navegación en Internet, las diferentes aplicaciones y recursos electrónicos que se puedan facilitar mediante –por ejemplo- una intranet institucional, las bases de datos, los programas, documentos, archivos y carpetas de archivos "colgados" –por ejemplo- en la red corporativa de la empresa y, desde luego, el correo electrónico como una herramienta de trabajo, hoy en día fundamental.

11- VALDÉS DAL-RE, Fernando. En la presentación del especial monográfico "La utilización de los medios informáticos en la empresa" de la revista Relaciones Laborales N° 5-6, Madrid, Marzo del 2009.

12- THIBAULT ARANDA, Javier. "El uso del e-mail por los trabajadores y las facultades de control del empleador". Ponencia presentada el 30 de marzo de 2001 en el Seminario "Poder informático e intimidad: límites jurídico- laborales y penales al control empresarial", organizado por los Estudios de Derecho y Ciencia Política de la UOC. En: <http://www.uoc.es/web/esp/art/uoc/0109040/thibault-imp.html>.

13- SPAM es un término inglés utilizado para definir el envío indiscriminado de mensajes de correo electrónico no deseados. Normalmente se aplica a mensajes publicitarios que bombardean el correo electrónico del usuario que los recibe en contra de su voluntad. En Perú, la Ley N° 28493 se refiere al SPAM como comunicaciones comerciales, publicitarias o promocionales no solicitadas, realizadas por correo electrónico.

Continuación de Referencias:

14 - Servidor especial encargado, entre otras cosas, de centralizar el tráfico entre Internet y una red privada, de forma que evita que cada una de las máquinas de la red interior tenga que disponer necesariamente de una conexión directa a Internet. Algunos pueden contener al mismo tiempo mecanismos de seguridad que impiden accesos no autorizados desde el exterior hacia la red privada (como el firewall).

15- El firewall (cortafuegos) es un dispositivo que se coloca entre una red local e Internet y cuyo objetivo es asegurar que todas las comunicaciones entre los usuarios de dicha red e Internet se realicen conforme a las normas de seguridad de la organización que lo instala.

16- Internet Service Provider o "Proveedores de Internet", compañías que han creado una conexión directa y permanente a Internet y que ofrecen la posibilidad de entrar en Internet a través de la señal que proveen.

17- Palabras claves previamente determinadas (por ejemplo "pornografía infantil") que al ser detectadas bloquean el ingreso o salida de un e-mail.

18- Dispositivo que distribuye el tráfico entre redes. La decisión sobre a donde enviar los datos se realiza en base a información de nivel de red y tablas de direccionamiento.

19- Publicado en IRS Employment Trends, N° 703,2002 Pág. 5

20- Mencionado en la BBC News el 6 de Junio de 2001, Citado por Mark Jeffery En: Tecnología Informática y Privacidad de Los Trabajadores, monografía asociada a Revista Aranzadi de Derecho y Nuevas Tecnologías, Navarra, Aranzadi, 2003, Pág. 122

21- La Asociación Empresarial Americana (AMA) estudia regularmente la gestión de recursos humanos en un grupo de empresas que en su conjunto emplean alrededor de una cuarta parte de la fuerza de trabajo de EE.UU.

22- Se refiere a aquellos trabajadores que usan regularmente el correo electrónico o tienen acceso a Internet en el trabajo.

23- Ambos informes son citados por Matthew W. Finkin En: Tecnología Informática y Privacidad de Los Trabajadores, monografía asociada a Revista Aranzadi de Derecho y Nuevas Tecnologías, Navarra, Aranzadi, 2003, Pág. 281

24- TOYAMA Miyagusuku, Jorge. Correo electrónico: entre la facultad de fiscalización, control del empleador y el derecho a la intimidad del trabajador. En: Dialogo con la Jurisprudencia N° 83, Agosto de 2005

25- NUÑEZ PAZ, Sandro Alberto. ¡Alerta: tienes un e-mail! La facultad fiscalizadora y la inviolabilidad de las comunicaciones. En: Revista Actualidad Laboral, Octubre 2004, Pág. 23

26- Entiéndase la figura del Abuso de Derecho como la que comete el titular de un derecho subjetivo cuando actúa de modo tal que su conducta concuerda con la norma legal que concede la facultad, pero que resulta contraria a la buena fe, la moral, las buenas costumbres, o los fines sociales y económicos del derecho.

27- El Tribunal Constitucional resuelve un caso de despido por uso indebido del e-mail en el Exp. 1058 - 2004-AA/TC, conocido como caso "Serpost"

28- La Cour de Cassation resuelve un caso de despido por uso indebido del e-mail en su sentencia del 2 de octubre de 2001, conocido como caso "Nikon"

29- Sentencia del Tribunal de Trabajo de Bruselas del 2.05.2000 citada por Oviedo, Maria Natalia. Control empresarial sobre los e-mails de los dependientes, Buenos Aires, Hammurabi, 2005. Pág. 249 y sgtes.

30- Véase las resoluciones judiciales en los casos: Fraser v. Nationwide Mutual Ins. Co., Smith v. Pillsbury Co., Restuccia v. Burk Technology Inc., Bonita P. Bourke v. Nissan Motor Co., Steve Jackson Games Inc. v. United States, United Sates v. Reyes, Egle Investment Systems Co. v. Einar Tamm, McLaren Jr. v. Microsoft Co., entre otras.

31- Véase la sentencia del 27 marzo del 2003 de la Sala VII de la Cámara Laboral de la Ciudad de Buenos Aires

32- Véase la Sentencia N° 312 del 26 de agosto de 2004, del Tribunal de Apelaciones del Trabajo.

33- Véase el voto de minoría en el fallo de la Sala Segunda de la Corte Suprema de Justicia (Expediente No. 02-300243-641-LA Ordinario Laboral de Paola Melissa Barboza Quirós contra Baxter Productos Médicos Limitada)

34- Sentencia del Tribunal Supremo Español del 26 de septiembre de 2007.

35- Véase el Ordinario 0260/0019, de fecha 24 de enero de 2002, de la Dirección del Trabajo de Chile.

OPINIÓN DEL PROYECTO S-3732/10 SOBRE IMPOSICIÓN DE REMUNERACIÓN POR COPIA PRIVADA

Tenemos que comprender este proyecto partiendo de la base que el concepto de derecho de autor en el Siglo XX y XXI, se extiende a nuevos tipos de obras y a períodos mayores de protección.

Las corporaciones como consecuencia de esto, se resisten a cambiar sus modelos de negocios en relación al paradigma de la comunicación digital distribuida y al libre intercambio de información, por lo que el derecho de autor se sostiene con el desarrollo de mayores tecnologías de control.

Las sociedades de gestión de derechos a la fecha no se adaptan al nuevo negocio ni pueden controlar el uso de las obras de los autores que representan.

En síntesis la industria no se adapta al mundo digital y a las nuevas formas de explotación y distribución de contenidos conforme a las exigencias del mercado y de los consumidores, lo que lleva a la llamada crisis de las sociedades de gestión, por el cambio del modelo económico producido por la concentración e integración de la industria musical.

Comentarios respecto del proyecto en análisis

La remuneración por copia privada a favor de



Leonor Gladys Guini, abogada
Especialista en Propiedad Intelectual
y Derecho de la Alta Tecnología.
<http://www.guiniyalbarells.com.ar>

los autores de obra musical, dramática, cinematográfica, audiovisual y producción fonográfica, comprendidos en el proyecto en examen, comprende sólo la copia para uso personal del copista (persona física) y siempre que se trate de una obra editada o publicada.

En consecuencia el pago de los obligados establecidos en el artículo 4 del proyecto no es por el uso concreto de la obra, sino por la posibilidad que los aparatos de reproducción ofrecen para realizar copias.

El pago o remuneración por copia privada mediante la reproducción reprográfica o bien por la reproducción casera de grabaciones sonoras y obras audiovisuales, justifica la intervención del sector industrial ya que no es la obra en sí misma sino su grabación, edición o fijación la que es objeto de reproducción.

El proyecto del Senado establece el pago de un impuesto legal o remuneración por copia privada a todos los obligados en su artículo 4. Si lo considera-

mos un impuesto, esta imposición debería provenir de la iniciativa de la Cámara de Diputados de la Nación y luego ser aprobada por el Senado.

El análisis del proyecto debería partir de la concepción de "obra" establecida por la N° 25036 modificatoria de la ley N°11723 de derechos de autor, fue extendida por la referida normativa a la obra de software cualquiera sea su forma o método de reproducción, considerándose a esta última como una obra literaria. No se entiende entonces porque el proyecto sólo se refiere a obras audiovisuales, dramáticas y musicales y a los derechos de autor o conexos que se devengaren a favor de autor, intérprete, ejecutante y/o productor de fonogramas, dejando de lado a los restantes autores, los que también sufren el flagelo de la piratería y de la reprografía se trate de fotocopias de libros ya editados bien cuando hablamos de piratería de software.

El proyecto se encuentra en línea con lo establecido por la Convención de Berna en cuanto establece cuál es el límite al derecho de reproducción que en exclusiva corresponde al autor, pero no se adecua a lo establecido en la ley 24.425 por la cual Argentina adhirió a los Tratados OMPI sobre derechos de autor y conexos, tratados conocidos con el nombre de Acuerdo TRIP's, los que fueron ratificados por nuestro país a fin de adaptar nuestra legislación a la era digital.

El derecho de remuneración equitativa de copia privada establecido en el proyecto, se establece sólo en beneficio de los titulares de derechos de autor y conexos establecidos en el artículo 4 b), sería percibido por SADAIC en representación de las restantes Sociedades de derechos, quien luego lo liquida y distribuye a los autores previa deducción de sus aranceles administrativos. Sin embargo no obstante lo expuesto, el artículo 6 del proyecto en su cuarto párrafo establece una contradicción, ya



que establece que las sociedades de gestión representarán a los autores en la liquidación y distribución de sus derechos por copia privada, pero que estos últimos tendrán la carga de individualizar a los deudores principales e iniciar contra ellos las medidas cautelares establecidas en el artículo 79 de la ley 11.723.

Entiendo que el peligro de establecer una remuneración por copia privada que será abonada por los fabricantes o importadores de soportes, aparatos o elementos aptos para la reproducción en la forma que establece el proyecto, es que dicho costo será luego trasladado sobre los adquirentes de dichos bienes, encareciéndose todos los productos electrónicos en nuestro país e incluso impactando sobre toda adquisición de bienes informáticos que realizara el estado.

Por otro lado hay que ser muy cuidadoso con la interpretación del artículo 3 del proyecto en análisis que se refiere a que se entiende por soporte o aparatos o elementos aptos para la reproducción, ya que al hablar de "almacenamiento", abarca a los discos rígidos de las computadoras que son elementos aptos para la reproducción, sin olvidar que

el mero almacenamiento de una obra en memoria de computador ya implica su reproducción y, que el almacenamiento transitorio necesario como parte esencial de un proceso tecnológico también quedaría gravado si el proyecto no efectuara la salvedad correspondiente, por lo que se debería analizar con mayor detenimiento que se entiende por aparatos o elementos aptos para la reproducción y que se entiende por reproducción, estableciendo un concepto más preciso y acorde con lo establecido en el Acuerdo Trip's sobre derechos de autor ratificado por Argentina.

También es objetable que el artículo 5 involucre al Poder Ejecutivo en la ampliación y o modificación de la nómina de nuevos soportes, equipos o aparatos que serían susceptibles de quedar gravados, cuando el resultado de la aplicación concreta de esta normativa generaría aquello que el estado justamente quiere evitar, que es el aumento de la llamada brecha digital en nuestra sociedad.

Conclusiones

Finalmente entiendo que este proyecto debe tratarse como una modificación de la ley 11723, debiéndose diferenciar en el mismo todos y cada uno de los supuestos de utilización libre y gratuita de obras (supuestos de "fair use" o uso leal), a fin de no crear confusión con el supuesto en estudio, requiriéndose una mayor análisis, investigación y consulta a especialistas en la materia.

Si bien el propósito del proyecto es luchar contra el flagelo de la piratería no se entiende por qué no aplica a la piratería de software que es también incontrolable y también produce grandes pérdidas.

Se desprende del proyecto que lo que se recauda en concepto de "Remuneración equitativa de copia privada" no está destinado al estado ni a impulsar la cultura o la creatividad, sino a las llamadas sociedades de Gestión de derechos, que no son más ni menos que aquellas que deberían poder controlar el uso de las obras que administran, adaptando sus modelos de negocios a las nuevas tecnologías.

La compensación genera una gran ineficiencia económica el que recibe la compensación, que además es repartida de manera completamente arbitraria y conforme los intereses de la industria y de las sociedades de gestión, no percibe la necesidad de evolucionar en su modelo de negocio, ni mucho menos de incrementar la calidad de sus servicios respecto de aquellos cuyos intereses representan.

Si bien en el momento que escribo este artículo el tratamiento del proyecto se encuentra suspendido, entiendo que el mismo se queda a mitad de camino, por lo que entiendo que el camino más acertado hubiera sido flexibilizar el concepto de derecho de autor trabajando sobre nuestra legislación a fin de evitar contradicciones con el proyecto en análisis.

Por último sería importante resaltar las limitaciones por copia privada que establece la sentencia "Padawan" dictada por el Tribunal de Justicia de la Unión Europea, las que paso a sintetizar a continuación:

Para que proceda la compensación por copia privada debe existir un justo equilibrio entre la copia privada y el daño causado.

Si el daño producido al autor es mínimo no sería procedente la compensación, por lo que se debería regularmente examinar cuanta copia privada se realiza y el efectivo daño que genera.

Asimismo el criterio del Tribunal establece tres nuevas limitaciones, a) que se aplique a casos concretos, es decir que como principio general la copia privada es excepcional; (no puede ser un impuesto general a favor de personas privadas); b) que la copia privada no entre en conflicto con la explotación de la obra, es decir que si ya se paga licencia de utilización de la obra por otro lado, no procedería su cobro; y c) que no perjudique los intereses legítimos de los titulares.

Autora: Leonor Guini



1ER POSGRADO 2011 DE ESPECIALIZACIÓN EN **DERECHO Informático**

Modalidad a Distancia para Latinoamérica con clases dictadas en vivo

Inicio: Abril 2011

Duración: 16/20 hs por cada Módulo

Módulos: Derecho Informático en la Sociedad de la Información
Protección a las creaciones intelectuales
Régimen Legal de los sitios web
Comercio Electrónico - Contexto Latinoamericano
Informática Forense: Problemática Jurídica de la Prueba Electrónica
Reciclaje Electrónico, Cloud Computing y Nuevas tecnologías
Relaciones Laborales y Tecnológicas
Delitos Informáticos / CRIMES INFORMÁTICOS
Certificación Digital – Contexto Latinoamericano
Disputas de Nombres de Dominio y Marcas Registradas
Protección de Datos Personales
Gobierno Digital

Dirigido a: Profesionales que acrediten título de grado

Inversión: USD 300 por cada Módulo

Informes: info@elderechoinformatico.com
www.elderechoinformatico.com
www.fcj.unp.edu.ar

Carlos Dionisio Aguirre (Argentina)
Fernando Barrio (Argentina)
Horacio Fernandez Delpech (Argentina)
Heidy Balanta (Colombia)
Freddy Ossio Onofre (Bolivia)
German Realpe Delgado (Colombia)
Carlos Reusser (Chile)
Laine Souza (Brasil)
Natalia Enciso (Paraguay)
Beatriz Rodriguez (Uruguay)
Joel Gomez Treviño (México)
Martín Horacio Barrandeguy (Argentina)

Docentes



Organiza:

Certifica:



RED IBEROAMERICANA
ELDERECHOInformático.com
LA COMUNIDAD DE DERECHO INFORMÁTICO MÁS GRANDE DE IBEROAMÉRICA



Facultad de Ciencias Jurídicas
UNIVERSIDAD NACIONAL DE LA PATAGONIA
SAN JUAN BOSCO
(Argentina)

LOS COSTOS DEL SOFTWARE PRIVATIVO

Debido a que está muy arraigada la piratería, no caemos en la cuenta de lo que cuesta tener software pago y cerrado. Sorprendete.

Muchas veces me puse a pensar que esto del soft libre además de las ventajas de su uso, tenía otras virtudes que muchas veces por una cuestión de desidia, ignorancia, etc, no tomamos en cuenta

En nuestro país también está de moda desde hace años, esto de los crack, seriales, ilegal por cierto (en Latinoamérica en general) y la comodidad de uso de algo masivo

Como dije alguna vez las mismas empresas creadoras de hard trabajan para el señor ventanas, y claro, las pocas ganas de probar cosas nuevas también ayudan a esto

Ahora bien, detrás del soft libre, está la libertad de usar lo que a uno le conviene sabiendo también que apoyamos a muchos desarrolladores a perfeccionar nuestro entorno tecnológico, con calidad y programas a la altura de los más exigentes

Haciendo una evaluación sencilla y sin demasiados tecnicismo veremos los costos de ser legales, lo que sorprenderá a todos



Por Sergio Mendoza

Moderador www.informaticaxp.org

Editor <http://geeksroom.com/>

Miembro activo de www.forosuse.org

Blog <http://caligulandia.blogspot.com/>

Win 7 ultimate -	\$ 1200
Microsoft Office -	\$ 995
Antivirus +firewall+escudos	\$ 400
Dibujo, corel o photoshop (versiones básicas)	\$ 400
Optimizadores ,limpiadores	\$ 90
Copia ,extracción dvd ,cd	\$ 150
Total aproximado basico	\$ 2835

Como verán el numero para lo que seria una pc domestica y sol contando el soft, es muy alto, y estamos hablando de una sola pc en el hogar o tu empresa

Cuando sabemos que por lo general se posee al menos dos terminales en la mayoría de los hogares, por lo tanto el número seria mas alto incluso-

Además seamos honestos, un solo virus seria suficiente para arruinar todo el sistema y volver a reparar todo de nuevo, y claro seguro porque

omento el soft libre, pensarán que porque fomento el soft libre ,digo esto, y es que además las pruebas son contundentes, muchas de esas licencias son por tiempo determinado ,lo que te lleva a renovarlas, y sus costos extras.

Es que a la larga los controles y programas anticopia de los fabricantes serán mas efectivas y si no puedes pagarlas tendrás una pc propensa a daños y si tu caso es empresarial puede llevar también a intimaciones por parte del autor ,teniendo en cuenta el tipo de lector de esta revista, saben de lo que hablo

Y es lógico dado que dichas empresas cuidan su dinero, quien no en definitiva

Sin embargo contamos con la posibilidad de usar nuestra pc de otra forma y con costos bajos o nulos,

Todo eso que te mostré podes tenerlo con linux y suites ofimáticas como libre office, open office, ubuntu, open suse como operativos diseño el gimp.

Instalando en tu pc linux ,ya de serie podes contar con todo esto ,sabiendo además que no tendrás virus ni malware para preocuparte, pudiendo desarrollarte en la web y socialmente , ya mas adelante iré planteando en forma estricta aplicaciones puntuales y sus usos y como instalarlos fácilmente

En mi caso particular (hogar) poseo un arranque dual y así se fueron acostumbrando de tal manera que hoy, les da igual si es linux o Windows

Ya que en definitiva contamos con las herramientas habituales de libre disponibilidad, para personalizar libremente nuestra terminal algo que vos podes hacer también

Me parece muy tentador y te invito a que pruebes, no es necesario que lo instales ya que todas las distribuciones linux, tiene el modo prueba



que desde el dvd trabajan hasta que te acostumbras y opcionalmente lo instalas

La posibilidad de virtualizar como opción también es buena para ese soft que no tiene reemplazo (virtualbox) donde se puede instalar un operativo en un entorno simulado con todas las funcionalidades del original

Ya como propuesta concreta los invito a descargar y probar Linux opensuse

Para recién iniciados yo diría que con escritorio kde muy intuitivo y de fácil uso >> aquí <http://software.opensuse.org/114/es>

La versión cd permite probarlo antes sin tocar el sistema boteando (arrancando desde el cd) y así familiarizarse ya mas adelante charlaremos de particularidades

Como verán, seguridad, usabilidad y potencia en tu pc pero lo mas importante BAJO COSTO, algo que no es para desperdiciar en estos días

Y desde ya una comunidad dispuesta a ayudarte

Sorpréndete como yo, hacete fan del soft libre

Saludos

CONTRATACIONES PÚBLICAS ELECTRÓNICAS

El uso de las TICs ha transformado sensiblemente los mercados nacionales e internacionales de compras públicas, contribuyendo a su transparencia, eficiencia y accesibilidad, así como al control social de los gastos públicos. Las compras públicas electrónicas son parte importante de este fenómeno.

Las contrataciones públicas electrónicas (e-public procurement) son aquellas en las cuales todo o parte del procedimiento de selección del contratista -convocatoria, presentación de ofertas, evaluación de las mismas, etc.- es gestionado por medios electrónicos. Dichas contrataciones integran, a su vez, un fenómeno más amplio: el gobierno electrónico (e-government) entendido como la aplicación sistemática de las TICs a la gestión pública, al servicio de una mayor eficiencia, transparencia y accesibilidad ciudadana a los actos realizados por las distintas dependencias gubernamentales.

En la Unión Europea, la cuestión de las compras públicas electrónicas ya era mencionada en un documento de la Comisión de 1996 -Public Procurement in the European Union, Exploring the Way Forward, también conocido como el "Green paper"-, que subrayaba la necesidad de estudiar cómo el mercado de adquisiciones y otras contrataciones públicas podría verse favorecido a través del uso del e-procurement. Dos años antes, el Bangeman Report -un informe especial producido por el Alto Grupo sobre la Sociedad de la Información-, sugería la implementación de procedimientos de compra



Sabrina Comotto es Especialista en Contrataciones Públicas y Maestranda en Políticas Públicas para el Desarrollo con Inclusión Social.

electrónica y, posteriormente, la creación de un Canal Europeo de Licitación Electrónica.

En América Latina, el país pionero y líder indiscutido en materia de compras públicas electrónicas es Chile, cuyo sistema (ChileCompra), ha sido objeto de numerosos premios y reconocimientos a nivel nacional e internacional -Mejor práctica en la región (Banco Mundial, 2004), Premio al Desarrollo de las TICs 2004 de parte de la Asociación Chilena de Tecnologías de Información (ACTI), Mejor solución de Gobierno Electrónico en materia de transparencia (reconocimiento otorgado por la Red de Líderes de Gobierno Electrónico de América Latina y El Caribe, bajo el liderazgo de la Organización de Estados Americanos, el Instituto para la Conectividad en las Américas (ICA), el Banco Interamericano para el Desarrollo (BID) y la Agencia Canadiense de Desarrollo Internacional); entre otros reconocimientos-.

En relación a Argentina, si bien el proceso de implementación del e-public procurement no se encuentra tan avanzado como su par chileno, durante los últimos años se han registrado importantes progresos. El primer paso a nivel legislativo se dio en 2001, cuando el Decreto N° 1.023, nuevo Régimen

de Contrataciones de la Administración Pública Nacional, autorizó la realización de procedimientos de selección en formato digital, equiparando los documentos electrónicos –ofertas, informes, impugnaciones, notificaciones, etc.-, a los presentados en forma impresa.

Cinco años más tarde, el Decreto N° 1818 estableció que las entidades comprendidas en el inciso a) del Artículo 8° de la Ley de Administración Financiera –N° 24.156-, deberían realizar los procedimientos de contratación por trámite simplificado (aplicables cuando el monto estimado sea inferior a la suma de \$10.000.-), a través del sistema electrónico que al efecto habilitara la Oficina Nacional de Contrataciones. Nace así el Sistema Electrónico de Compras Públicas (SECOP), que comenzaría a tener operatividad en 2008, y que continuó vigente hasta 2010, momento en que fue reemplazado por e-com.

E-com es una plataforma totalmente web-based –es decir, que corre totalmente en Internet-, y que permite que el procedimiento de selección del contratista estatal sea realizado en completamente en forma electrónica. A través del uso de la firma digital, se asegura la integridad y autoría de los dictámenes de los servicios jurídicos de cada Unidad Operativa de Contrataciones (UOC), y de los actos administrativos del procedimiento. La presentación de ofertas también funciona con un mecanismo de encriptación que permite garantizar su autoría e inviolabilidad.

La plataforma opera, además, integrada con el Sistema de Información de Proveedores (SIPRO) y el Sistema de Identificación de Bienes y Servicios (SIByS), y se vincula también con el SLU –programa presupuestario del Ministerio de Economía-. Cuando se carga una erogación en E-com, dicha carga impacta automáticamente en el SLU, permitiendo generar la correspondiente solicitud de gasto.

Otra innovación de importancia ha radicado en la implementación del e-etap, que habilita a gestionar en línea la intervención de la Oficina Nacional de Tecnologías de la Información (ONTI) –organismo con competencia específica en materia de adquisición de bienes y servicios informáticos-. Se suma así otro recurso tecnológico de importancia que permite otorgar mayor celeridad a los procedimientos, contribuyendo así al logro de los principios de economía procedimental, transparencia y eficiencia de las contrataciones.

No obstante, y sin perjuicio de la importancia de los avances señalados, también es relevante señalar –a título de conclusión o de breve reflexión final-, que el énfasis no debe ponerse en las TICs en sí mismas, sino “...en su utilización combinada con los cambios organizativos y con nuevas aptitudes encaminadas a mejorar los servicios públicos, los procesos democráticos y las políticas públicas” (Comunicación de la Comisión Europea N° 2003 0567). En síntesis, para que todos los adelantos citados tengan efectos concretos en términos de mejora de la gestión y de los servicios brindados a las ciudadanas y ciudadanos, deben acompañarse con acciones específicas tendientes a generar cambios en la cultura organizacional, no sólo de las entidades contratantes, sino también de los oferentes, y de todas las áreas que intervienen, directa o indirectamente, en los trámites de contratación.

Autora:



ANÁLISIS DE LA POLÍTICA DE SEGURIDAD DE FACEBOOK

En el siguiente artículo se presenta un análisis de los principales aspectos de la política de seguridad de Facebook (FB), legislación vigente, así como medidas a implementarse por los usuarios de FB para proteger su información.

Aspectos Generales

La política de seguridad de FB inicia señalando que es de exclusiva aplicación para ellos y no para aplicaciones o sitios web que utilizan su plataforma, Asimismo establece que no se crean cuentas a menores de 13 años y en caso de detectar un perfil de un menor de 13 años la cuenta se bloquea. Sobre este punto FB recalca la responsabilidad de los padres de enseñar a sus hijos menores a cumplir políticas mínimas de seguridad como no revelar contraseñas, pensar bien antes de realizar una publicación, aceptar solo solicitudes de personas que conozca, entre otras.

Un aspecto a resaltar es que su política contempla la posibilidad de que un padre les solicite acceder al perfil de un menor de 13 años pero debe acreditar mediante poder que es el tutor oficial. Asimismo puede solicitar la cancelación de la cuenta pero FB se reserva el derecho de hacerlo exclusivamente cuando compruebe razonablemente que en efecto se trata de un menor.



Tania Sagastume Bulnes-Bueso es Abogada-Magister en Derecho Empresarial- Universidad Católica de Chile. Superintendente de Valores y Otras Instituciones, Comisión Nacional de Bancos y Seguros de Honduras.

Por lo tanto para FB su política general es no abrir cuentas a menores de 13 años pero al no validar la información basta que un menor cambie su año de nacimiento y podrá crear su perfil, por lo que los padres son en última instancia los responsables del uso de internet por sus hijos menores de 13 años.

Manejo de la Información

FB señala que su objetivo es compartir información por lo que se recalca que si no quiere compartir información la remueva previo a incluirla en su perfil. Señala que es posible que la información de los pagos sea retenida por FB por lo que se recomienda asegurarse que se borre el número de cuenta.

La política también especifica que cuando el usuario se conecte por computadora, celular u otro dispositivo es posible que FB obtenga información como tipo de browser, ubicación, dirección IP y páginas visitadas.

En cuanto a la relación con los anunciantes FB señala que pueden solicitarles que le detallen como

los usuarios respondieron a un anuncio o si han interactuado lo que justifican como medio para medir la satisfacción del cliente.

Por lo tanto, FB expresamente declara su facultad de revelar información incluida en su perfil, información de cuenta usada en sus pagos, datos IP, así como interactuar con los anunciantes sobre su perfil como consumidor.

Información que se comparte en Facebook

En cuanto a la información que comparte un usuario la política señala que no hay opciones de privacidad en el nombre y la foto, pero que si cuenta con opciones de privacidad en cuanto personas que pueden ver su perfil, publicaciones en el muro, fotos, pero que dichas opciones deben ser configuradas por el usuario dentro de su perfil. Destacan que la falta de privacidad significa que su perfil sea accedido por cualquier persona, aunque no cuente con una cuenta de FB, ya que estará disponible en los buscadores de internet.

La política de FB es clara en que toda información pública a la que el usuario no le ha configurado perfiles de seguridad puede ser accedida por cualquier otro usuario de FB o por no usuarios cuando se utilicen buscadores.

Información que se comparte con terceros

En este punto se señala que cuando se usa aplicaciones y sitios web disponibles en la plataforma de FB. La información es disponible para otros lo que significa que terceros tiene acceso a la información de su perfil, pero que en ningún momento pueden asegura que el tercero no cometa violaciones a la política de seguridad de FB.

En cuanto su relación con terceros como proveedores FB señala que no puede asegurar el cumplimiento total por sus anunciantes así como



que se reserva la facultad de compartir su información con anunciantes pre-seleccionados.

Uso de la información por Facebook

De acuerdo a lo establecido en la política la información en FB se utiliza para proveer servicios y mejorarlos, contactar al usuario, establecer publicidad orientada al usuario o cuentas comerciales. Asimismo enfatizan que la información se comparte al momento de realizar un pago con terceros con el único fin de procesar la transacción, al aceptar compartir información con un anunciante y para las herramientas de información pública.

Como se protege la información

Finalmente la política de seguridad de FB recomienda al usuario tomar medidas de seguridad como encriptación de información sensible, conciencia de que no hay seguridad impenetrable e importancia de denunciar cualquier violación de la política establecida.

Es indudable que después de una lectura profunda de la política de seguridad encontramos que existen ciertos aspectos de la misma que la hacen vulnerable tales como la no verificación de la cuenta de un menor, la seguridad depende de que el usu-

ario configure sus opciones y la falta de garantía que terceros como anunciantes cumplirán la política de seguridad.

Un análisis más completo debe conducirnos a concluir que FB basa enteramente la política de seguridad en trasladar su responsabilidad a los usuarios. Pero esto nos debe llevar a plantearnos: ¿no debería FB hacer más? Para mí la respuesta es una sola SI, FB debe recordar que su responsabilidad es mantener el sitio seguro así como mantener la privacidad del usuario intacta, por mientras no vuelva a asumir dicho rol se continuara leyendo a través de los medios las diferentes fallas de seguridad que tiene FB, sus fallas son tan reales que recientemente ha ofrecido US\$500.00 para todo aquel que pueda descubrir la existencia de fallas en su seguridad.

No obstante tal como lo abordaré en el siguiente apartado es importante conocer cuál es el marco legal regulatorio aplicable a FB conforme la normativa vigente en los Estados Unidos de América por ser el lugar donde está alojado FB. No obstante así como las políticas de seguridad se tornan complejas y confusas, también los marcos legales aplicables ya que existen situaciones en que no se viola la ley de los Estados Unidos pero si se viola la legislación de otros países, por ejemplo el caso actual en que la aplicación de reconocimiento facial viola políticas de Alemania pero no de Estados Unidos.

LEGISLACIÓN APLICABLE

En Estados Unidos no existe una ley de protección de los datos del consumidor a nivel federal, solo leyes específicas para datos que aplican a datos médicos, bancarios o gubernamentales, lo cual crea un alto riesgo legal ya que siendo ellos el

país donde se alojan centros de datos de proveedores como FB resulta difícil regular las políticas de dicha empresa si no se cuenta con leyes de privacidad de los datos.

Lo anterior ha llevado a situaciones donde recientemente la Unión Europea que si cuenta con una Directiva acerca del tema estableció que exigirá a proveedores como FB cumplir con los requisitos de su Directiva.

La Directiva 95/46 de la Unión Europea sobre Protección de Datos se basa en los siguientes siete principios:

1. Deber de notificación a los usuarios de la razón por la cual se ha recabado los datos;

2. Facultad del usuario de decidir acerca de la finalidad y destino de los datos de carácter personal;

3. Transferencia de datos exclusivamente a países que brinden un nivel adecuado de protección;

4. Posibilidad del usuario de hacer efectivos sus derechos;

5. Deber de adopción de medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, tratamiento o acceso no autorizado;

6. Calidad de los datos; y,

7. Establecimiento de mecanismos de resolución para asegurar el cumplimiento de la directiva.

Debido a la directiva anterior y con el fin de asegurar la participación de las empresas de Estados Unidos con el mercado comunitario europeo, en el año 2000 Estados Unidos y la Unión Europea celebraron un acuerdo basado en el principio de "Safe

Harbor”, bajo lo cual se exige a las compañías norteamericanas de ser demandadas por infracción a la privacidad, a iniciativa de los ciudadanos europeos, si han comunicado al Departamento de Comercio o a una autoridad de protección de datos europeo que cumplieron con la directiva de protección de datos, en caso de falsa declaración pueden ser acusados de prácticas comerciales engañosas.

Sin embargo, tampoco se puede afirmar que la existencia de dicho convenio garantiza el efectivo cumplimiento de las políticas de privacidad en Estados Unidos ya que el año 2001 a raíz de los ataques a las Torres Gemelas se aprobó la Patriot Act que obliga a las empresas estadounidenses o aquellas que alojan sus centros de datos a proporcionar a las autoridades acceso a los mismos. Es decir que se ignora cualquier ley o convenio de privacidad de datos teniendo Estados Unidos libre acceso, sin notificar a nadie a cualquier información que está en los centros de datos ubicados en su territorio. En este punto debo señalar que la lucha recién inicia y debe dársele seguimiento en los próximos años.

No obstante alejado de los conflictos anteriores me parece importante señalar cual es la responsabilidad de las partes en la prestación de servicios mediante FB, para lo cual se asumirá que el dueño del perfil se ubica en España, por ser la Unión Europea la que cuenta con una Directiva clara sobre la materia.

Es así como en toda relación de “cloud computing” participan tres partes:

a.El proveedor del servicio quien es el que presta el mismo, en el caso de la red social FB, el proveedor es FB;

b.El abonado o cliente al servicio quien es la persona natural o jurídica que suscribe un contrato

con el proveedor de servicios, es decir el usuario que crea un perfil en FB y al aceptar las condiciones de prestación del servicio suscribe un contrato con FB; y,

c.El usuario final quien usa los servicios de cloud computing, que en el caso en mención es el mismo cliente.

Después de realizar un análisis de FB podemos concluir que el mismo maneja datos personales tales como correo electrónico, contenido de perfiles y direcciones de IP de sus usuarios, que la directiva europea ha definido como datos personales por lo que debe aplicarse dicha regulación. Asimismo debido a que el servicio se presta a un usuario localizado en un miembro de la UE el proveedor debe cumplir el marco legal vigente, donde siempre éste será responsable del tratamiento debido de los datos y facilitando el ejercicio de los derechos de los usuarios en el tratamiento de dicha información.

Sin embargo, no todos los casos son claros como el anterior y cada día evoluciona la materia por lo que la aplicación del marco legal vigente sigue siendo un reto que se continuará desarrollando en los próximos años.

RESPONSABILIDAD DEL USUARIO DE FB

Resulta difícil después de leer el complejo panorama de las políticas de seguridad de FB y la legislación vigente no llegar a la conclusión de que la mejor opción es no seguir en FB. Sin embargo, las redes sociales son una realidad y un medio eficiente de comunicación, por lo que antes de cancelar su cuenta de FB, el usuario debe tomar consciencia de su responsabilidad en la protección de su propia información. El usuario de FB debe saber que su protección no vendrá por políticas de seguridad o regulaciones sino vendrá por el hecho que él se empodere del papel que debe jugar en la protección de su

información; así como el inversionista en mercado de valores asume su responsabilidad en el manejo de su dinero, el usuario de FB debe asumir su responsabilidad en el manejo de su información.

Es así como cualquier usuario que desee utilizar FB debe como mínimo implementar las siguientes configuraciones de privacidad en su perfil de FB, las que se explican plenamente en la página web <http://www.allfacebook.com/facebook-privacy-settings-2011-02> las cuales se resumen así:

1. Clasificar los amigos en grupos con configuraciones de privacidad determinadas;
2. Modificar el acceso de ubicación;
3. Removerse de búsquedas de FB;
4. Removerse de buscadores públicos;
5. Permitir solo a amigos "tag" en fotos y videos;
6. Habilitar la seguridad https;
7. Privacidad de la información de contacto;
8. Privacidad de acceso al muro;
9. Deshabilitar personalización instantánea; y,
10. Deshabilitar información disponible en aplicaciones.

Asimismo con independencia de la implementación de políticas y opciones de seguridad, la verdadera prevención inicia con que el usuario entienda la importancia de su información y el papel fundamental que juega en proteger su información.

CONCLUSIONES

Las redes sociales son una realidad de un mundo que cada vez más se basa en las tecnologías de la información, pretender aislarse de dicho desarrollo no es una opción viable ya que significa un aislamiento del mundo, sobre todo en presencia de redes sociales como FB que agrupan alre-

dedor de 600 millones de usuarios en continuo crecimiento. Alejarse de la existencia de FB lo aleja del mundo real, sin embargo el problema fundamental es como proteger la información personal que incluimos en un perfil de FB.

El principal paso que debe seguir todo aquel que decide utilizar FB es entender que los servicios de FB que el acepta se incluyen en sus políticas de seguridad la cual lastimosamente muy pocos usuarios leen, lo que les conduce a exponerse a posibles riesgos en el manejo de su información, pero sin contar con medidas preventivas para mitigar dicho riesgo.

Un análisis de las políticas de seguridad de FB nos revelan que presenta aspectos ambiguos tales como tratamiento de información de menores, por terceros usuarios y sobre el responsable del manejo de dicha información. Se podría entonces ante tal falencia recurrir a la legislación vigente la cual lastimosamente es ambigua ya que presenta brechas tales como Estados Unidos que no presenta una regulación nacional hasta Europa con una regulación estricta pero de difícil aplicación ante la realidad de proveedores de servicios, clientes y usuarios ubicados en jurisdicciones diferentes con regulaciones disimiles.

Lo anterior indudablemente conducirá a los países a buscar soluciones homogéneas, pero presenta una disyuntiva para el usuario, que es si debe esperar dicha regulación para beneficiarse de las redes sociales o debe asumir su responsabilidad como usuario en ser el protagonista en las acciones dirigidas a proteger su información.

La respuesta nos conduce a una sola realidad: el usuario se apropia de la responsabilidad de cuidar su información para lo cual adopta estándares mínimos de configuración de la privacidad y se beneficia de ser miembro de las redes sociales, basado en un solo principio: al único que le importa la privacidad de su información es a el mismo.

VIDEOCONFERENCIA 100% WEB PARA REUNIONES Y CAPACITACIONES

REÚNETE CON TUS CLIENTES Y PARTICIPA CON AUDIO Y VIDEO EN VIVO.



The interface displays a video conference with two participants: Ignacio and Leticia. The main content area shows a 3D pie chart titled "Resultados encuesta satisfacción 2009" with a legend:
■ Muy conformos (blue)
■ Conformos (red)
■ Poco conformos (green)
■ Disconformes (purple)
The "Participantes" list on the right includes:
- Rodrigo (checked)
- Maria (checked)
- Ignacio (checked)
- Leticia (checked)
- Emilio (checked)
Below the list are options:
- Habilitar audio y video
- Habilitar sólo audio
- Habilitar Pizarrón
- INICIAR CHAT PRIVADO
The "Chat Público" shows a message from Emilio:
Emilio:
Ignacio: Son los mismos números de la planilla del año pasado.
An "ENVIAR" button is at the bottom right of the chat area.

- ✓ 100% WEB. ACCEDES DESDE CUALQUIER PC O MAC SIN IMPORTAR DONDE ESTÉS.
- ✓ HASTA 3 CÁMARAS Y MICRÓFONOS EN SIMULTÁNEO
- ✓ HASTA 25 USUARIOS SIMULTÁNEAMENTE EN LA MISMA SALA
- ✓ NO NECESITAS INSTALAR SOFTWARE, ESTA TODO EN LA WEB.



¡Prueba WWC gratis ahora mismo!

Solicita tu cuenta de prueba por un mes:

Vía email

info@wormholeit.com



Por teléfono

(011) 5254-0115 / 0116



En nuestro sitio

www.wormholeit.com/wwc



REALMENTE HEMOS AVANZADO EN LO QUE DENOMINAMOS GOBIERNO ELECTRÓNICO DENTRO DE LOS ORGANISMOS QUE CONFORMAMOS LA ADMINISTRACIÓN PÚBLICA NACIONAL.....

A partir del año 2005 comienzan a delinearse dentro de los organismos el comienzo hacia un cambio en la forma de gestionar de cara a las necesidades que el usuario/ ciudadano necesita avanzando hacia un modelo diferente el de gestión por resultados bajo lo que se denominaría: gobierno electrónico, el Estado es el mayor ente productor/tomador de información del país, por lo que resulta esencial la utilización de herramientas tecnológicas para aumentar los niveles de transparencia de los actos públicos y dar rápida respuesta a las necesidades y requerimientos de la población.

El empleo de las Tecnologías de la Información y las Comunicaciones, y especialmente Internet, está transformando las relaciones entre las personas y las organizaciones públicas y privadas, resultando un instrumento idóneo para facilitar el acceso a la información y a los servicios del Estado, integrar los distintos niveles de la ADMINISTRACION PUBLICA NACIONAL, dotar de transparencia a la actividad del Estado, digitalizar con validez legal la documentación pública y permitir el intercambio de información entre el Estado y los particulares mediante canales alternativos al papel.

Para tal fin y con muy buen tino desde el organismo rector se impulsa a que se presente un Diagnóstico de Estado de Situaciones, de esta manera se pudo saber el estado de cada Organismos no solo a nivel informático sino también en procedimientos y operatoria, esto incluía en tipo de tra-



*Prof. María C. Chimeno Fernández,
Especialista en e-government, Coor-
dinadora Área Unidad Gobierno Elec-
trónico del Ministerio de Industria de
la Argentina.*

mitación realizada ya sea en papel, cantidad de días de tramitación y la utilización de algún medio informática para concretar la tramitación.

Siguiendo con la misma línea se debía presentar a posteriori un Informe de avances, obviamente que esto conllevaba a que los organismos presentaran un plan anual de procedimientos y operativas a realizar ese año para ir mejorando su estadio inicial.

Mientras se fueron delineando tanto los diagnósticos como los avances podemos decir que se fue acompañando de cambios estructuras en la normativa hasta ahí vigente podemos nombrar a la firma digital como a la protección de datos personales, pero fueron suficiente y apuntalaron al trabajo que se debería realizar dentro de los organismos? Aporto? Nos ayudó? O solo fue un apuntalamiento corto placista?. Las reglamentaciones fueron rápidas de las normativas Base?

En el ámbito de la ADMINISTRACION PUBLICA NACIONAL se ha registrado una aplicación desigual de los avances en las Tecnologías de la Infor-

mación, según las incumbencias de cada jurisdicción, sin una visión integral desde el punto de vista de la ADMINISTRACION PUBLICA NACIONAL y de las necesidades de los habitantes y ciudadanos en su conjunto.

Oportunamente hace ya dos años (estamos hablando del 2009) se comenzó un trabajo que considero como la mejor iniciativa de trabajo, fue un excelente avance, en el trabajo que estábamos comenzando a hacer entre organismos, una mesa en la cual estaban sentados todos los involucrados: la sociedad civil, las ONG, los organismos, las provincias y los organismos vectores. Los cuales pudimos observar cuales eran las problemáticas reales y que se necesita para avanzar, en los que todos coincidimos fue que lo primero y principal era la visión y decisión política que no solamente es necesario tenerla a nivel ejecutivo sino dentro de cada línea media de las áreas de funcionamiento de los organismos, que las autoridades a cargo tengan esa visión y sepan como hacerla más confiable a los directores y funcionarios a cargo de las áreas. El tema genera miedo, desconocimiento, pensamiento en un desempleo a corto plazo, una manera diferente de gestionar...

Creo que el estar sentado en una mesa de trabajo así generó ver diferentes aristas del mismo problema, conocer a fondo necesidades y demandas, ese tipo de trabajo transversal tiene que existir no se pueden delinear solo políticas vistas desde un solo sector desde un solo organismo o solo desde un solo vector porque se hacen inalcanzables, erradas y sin poder cumplir con la verdadera necesidad de generar políticas publicas adecuadas al tema en el cual estamos haciendo referencia.

Creo que el trabajo esta dado no solamente puertas afuera sino también puertas adentro, se empieza con lo que denomino la "Evangelización" de las áreas.



Es muy bonito decir que la Web 2.0 ofrece a los medios el nuevo gobierno para escuchar la voz de los ciudadanos y el hablar con ellos en otro tipo de diálogo. Pero realmente cuando queremos avanzar con escuchar al ciudadano es así o solo generarle un poco más de confusión en sus derechos y obligaciones?.

El entorno en línea se convierte en un medio adicional por el cual los analistas en el gobierno pueden acceder a la opinión pública como una forma de mejorar el diseño y prestación de servicios hacia los ciudadanos

No es que no se han realizado actividades en pos del desarrollo del tema de referencia pero si se denota que los Organismos como ANSES y AFIP han sido vedette en este tema, tal vez porque el presupuesto, visión y decisión, necesidades políticas y usuarias e infraestructura hicieron posible este crecimiento.

Hay actividades, propuestas y necesidades que se han ido trabajando en diferente medida desde Nación así podemos nombrar una Agenda Digital, grupos de trabajo Multisectorial pero realmente a nivel global si se nota avances pero en lo especifi-

cos en lo cotidiano de los Organismos seguimos remando contra la corriente y con necesidades expuestas. Se necesita de técnicos específicos, que si sabemos que los hay, que vengan a los Organismos como en otros tiempos, y nos ayuden a “evangelizar” a los funcionarios medios de los Organismos. Nos aporten sus ideas y experiencias.

Muchas veces esas mesas de trabajo no tienen los actores e involucrados que realmente deberían estar en ellas o también faltan los que deberían estar participando, con una visión clara y concisa.

Desde las ciudades se denota que no tienen un crecimiento sostenible y por fases en el ámbito de estrategias de gobierno electrónico. Se ve claramente la necesidad de una estrategia a largo plazo en la implantación del gobierno electrónico Municipal de forma que se cree una arquitectura digital sostenible. Aunque se denota que el trabajo realizado por esta fue muy diferente al que estamos denotando desde Nación.

No debería existir una estrategia a mediano y largo plazo? Con un plan desarrollado en cada organismo que sigan ese “mandato” desde el organismo de aplicación? realmente sirvió de la manera que fue planteado hasta ahora o como fue planteado en estos últimos años?

Creo que en las administraciones locales han hecho grandes esfuerzos para potenciar la implantación y el uso de las tecnologías de información en esta materia.

Los portales Municipales se han ido convirtiendo en una importante fuente de información para los ciudadanos tenemos varios casos para ir nombrando el más destacado a mi entender fue el de la Municipalidad de Tigre siendo este un pro-

grama de gobierno destinado a dotar a todas las localidades con infraestructura digital; modernizar y descentralizar la gestión municipal incrementando

el número y la calidad de los servicios prestados tomando como eje el protagonismo del ciudadano. Además de promover acciones tendientes a la disminución de la brecha digital existente entre diferentes sectores sociales.

De tal manera observamos lo que antes expongo de la necesidad de realizar un trabajo de manera transversal ya sea a nivel local como a nivel de Organismos Nacionales, creo que en todos los niveles se necesita de la misma dinámica de trabajo y el compromiso de todos aquellos involucramos.

Existen varias definiciones sobre gobierno electrónico y cada uno enfatizando la importancia de la interacción entre ciudadanos y gobierno usando diferentes formas.

En los próximos años transformará no solo la manera en que muchos servicios públicos son distribuidos, sino también pilares (contexto institucional) en los que se asientan las relaciones entre las administraciones públicas y los ciudadanos, porque eso ya lo venimos denotando en estos últimos años.

Después del e-commerce y del e-business la próxima revolución asociada a Internet es el de e-government.

La OCDE-1998 ha definido gobierno electrónico como la aplicación de tecnologías basadas en Internet para actividades comerciales y no comerciales en el seno de las administraciones públicas.

El gobierno electrónico es un programa que tiene sus raíces en la agenda de modernización es presentado como un proceso implicando un cambio transformacional, a nivel organizacional de cambios en los procedimientos de gestión en un amplio sentido.

Muchas veces pensamos en un programa solo de necesidades informáticas y en realidad debe ser pensado como destinado a dotar a todas las áreas con infraestructura digital, modernizar y descentralizar de la gestión, con la idea de incrementar el número y la calidad de los servicios prestados tomando como eje el protagonismo del ciudadano.

La participación del Estado resulta esencial para la construcción de los intereses colectivos y su desarrollo con inclusión social.

La calidad Institucional es uno de los pilares del orden democrático, del desarrollo económico y social y de las políticas públicas. En tal sentido la gestión de la cosa pública adquiere una relevancia especial, exigiendo la profesionalización permanente del capital humano, la adaptación y modernización de sus recursos técnicos y materiales de manera de fortalecer las instituciones públicas, de manera de dignificar la figura de sus empleados, como así también simplificar los procedimientos, renovar los dispositivos de gestión y facilitar las relaciones del ciudadano con las Administraciones públicas fundamentalmente para garantizar a los habitantes el acceso oportuno y universal al disfrute de las prestaciones y servicios públicos de calidad.

Siendo la práctica del buen gobierno y la creación de valor público creo que son requisitos imprescindibles para asegurar la consecución de los programas gubernamentales con eficacia y eficien-

cia, creo que es la meta a seguir y vamos en camino solo falta hacer un poco más de fuerza, estar involucrados en pos de la meta deseada y hacer un examen de conciencia de lo que realmente queremos lograr, con buena voluntad y un plan estratégico en serio creo que lo hemos de lograr por supuesto no a corto plazo, todo lleva su tiempo pero con metas claras a corto, mediano y largo plazo se que lo lograremos, por supuesto me incluyo.

Autora: Profesora Maria C. Chimeno



EL CRECIMIENTO DEL TELETRABAJO: ANÁLISIS DE SUS VARIABLES POSITIVAS Y NEGATIVAS. SU CONTEXTO.

El desarrollo de nuevas tecnologías de la información y de la comunicación nos plantea el desafío de adaptarnos a la existencia de cambios significativos en distintas áreas. El área laboral no escapa a este fenómeno.

Teletrabajo... ¿Qué es?

El fenómeno de la informática y de las telecomunicaciones se ha ido adentrando en forma vertiginosa en la sociedad planteando como desafío nuestra adaptación a la existencia de tecnología avanzada, y formulando cambios significativos en distintas áreas. El área laboral, no escapa a este fenómeno. Las TIC han introducido una nueva fórmula organizacional y estructural de trabajo, que ha inducido a la amplia doctrina a investigar y enmarcar un contexto adecuado que se aproxime a esta nueva era tecnológica, eje medular del teletrabajo.

El teletrabajo aparece entonces como una nueva forma de organización laboral. Quien trabaja ya no se desplaza hacia las instalaciones de la empresa -de la cual depende- para la realización de sus actividades, sino que es el trabajo el que va hacia donde está el trabajador (1). Es una forma de empleo que se ejecuta en un lugar alejado de las oficinas centrales o de las instalaciones de producción, mediante la utilización de las nuevas tecno-



Carla Pellegrini y Lorena Muracciolo son estudiantes de la Universidad Nacional de Córdoba - Argentina.

logías de la información y de la comunicación (TIC).

El concepto “trabajo” sigue siendo el mismo -trabajo humano y voluntario que surge de la actividad productiva y creadora del hombre con el fin de procurar su realización personal y económica (2), lo que cambia es la modalidad: la organización y la realización del trabajo es diferente.

El teletrabajo es, sobre todo, un modo de organización y ejecución de la actividad laboral que difiere del tradicional. Teletrabajar no es sólo trabajar a distancia y utilizando las telecomunicaciones y/o la informática, teletrabajar es servirse de estos elementos para laborar de un modo distinto. Por consiguiente, no es teletrabajador todo aquél que emplea las herramientas propias del teletrabajo (TIC), sino sólo aquel que por el hecho de utilizarlas de manera regular escapa al modelo tradicional de organización del trabajo (3).

Apreciación cuantitativa y cualitativa

La creciente utilización de esta modalidad laboral se ha objetivizado dentro de cifras estadísticas por diversas empresas mundialmente, una de ellas en el marco nacional, la consultora especializada en teletrabajo: Jobbing (4), ha publicado cifras que enmarcan el crecimiento anual en un 20%, con un total de teletrabajadores aproximado de 1.6 millones de personas, de las cuales un 10% trabaja en relación de dependencia y el resto dentro de una modalidad de freelance (5). A raíz de este crecimiento exponencial, se han comenzado a estudiar dentro del mundo comercial, social y jurídico las importantes connotaciones que esta modalidad ha tenido en los últimos años. Dentro de este marco de trabajo, se han analizado las diversas ventajas y desventajas que se presentan a la hora de materializar esta forma de e-trabajo.

Abriendo camino a este panorama, nos encontramos, por un lado, frente a las denominadas “ventajas del teletrabajador”. Desarrollaremos a continuación diversas enunciaciones que intentan mostrar cómo el teletrabajo ha venido a generar beneficios para quien trabaja bajo esta modalidad.

A nivel económico, el teletrabajador se verá beneficiado por el ahorro en los gastos de traslado a la planta de trabajo (6). Pero no sólo eso, el ahorro también alcanzará cuestiones de vestuario y alimentación (7).

A nivel social, el teletrabajo fomentará la unión familiar, es decir, hay una conciliación del ambiente familiar con las responsabilidades laborales, ya que quien teletrabaja desde su hogar permanecerá allí durante gran parte del día, posibilitando compartir en familia espacios importantes. Mencionaremos también aquí la comodidad para el teletrabajador en



relación a sus horarios de trabajo y al ahorro de tiempo en los traslados, y libertad de distribución de las tareas. Por último, y siguiendo con los beneficios a nivel social, encontramos la inclusión de sectores de grupos vulnerados.(8) El teletrabajo se presenta como una importante fuente de generación de empleo para aquellas personas víctimas de discriminación como son las “personas con capacidades diferentes” y las “madres que encabezan el seno familiar”, que podrían trabajar desde sus hogares, en el caso de los primeros, sin problemas por el desplazamiento, y en el caso de las segundas, sin descuidar sus obligaciones como madres (9).

A nivel ambiental, el teletrabajo genera un gran beneficio ecológico gracias a la reducción de medios de transporte circulando en las calles como consecuencia de que ya los trabajadores no se desplazan para ir a trabajar. Además en muchos casos y gracias a las TIC la utilización del papel cada vez se ve más reducida. (10)

Si bien, muchas de estas ventajas han sido promovidas dentro de diversos ámbitos, corresponde que analicemos ahora aquello que no aparece

como favorable para quien teletrabaja. En este orden de ideas, es necesario resaltar la situación de falta de un marco jurídico que encabece los parámetros necesarios de un contrato de trabajo acorde a las necesidades que vivencian los teletrabajadores, como hemos mencionado, un contexto claramente apartado de la organización laboral que poseemos dentro de la Ley de Contrato de Trabajo, siendo producto claro del proceso globalizador de la sociedad actual.

Con esto dicho, se puede exponer el marco de “desventajas para el teletrabajador”, partiendo de la crítica a las recién mencionadas ventajas, y además adicionando aquellas que han surgido de la amplia discusión doctrinaria por los vacíos legales que presenta esta materia.

Frente a lo que mencionáramos mas arriba como beneficio de ahorro para el teletrabajador, se nos presenta la situación que suele generarse en estos casos de trasladar los gastos del empleador (luz, internet, etc.) al trabajador, entonces los ahorros se desdibujan, y ya no serían tales. En relación al fomento de la unión familiar, deberíamos tener en cuenta que esta situación de llevar la “oficina a casa” podría generar conflictos, dificultad para distinguir el ambiente laboral del familiar, dificultades de concentración, jornadas laborales extensas e ilimitadas, que en definitiva resulta contraproducente a la hora de buscar el fortalecimiento del círculo familiar

Enunciaremos ahora algunas desventajas ampliamente debatidas por la doctrina, aunque no a título taxativo: falta de protección del régimen de las ART en el marco de riesgos de trabajo, casos de eliminación del aporte por parte de los empleadores de las herramientas de trabajo que conforman la estructura de las TIC (notebooks, red inalámbrica de internet), carencia de un control del espacio de tra-

bajo y las comodidades aportadas, pérdida del contacto personal con los demás trabajadores presenciales, y demás cuestiones que deben evaluarse a la hora de poder aplicar esta forma organizacional de trabajo en forma efectiva.

Será necesario canalizar estas variables dentro de lo que corresponde la situación actual de los teletrabajadores, y la urgencia de la implementación de plataforma normativa que amerite esta actividad como la modalidad organizacional de trabajo del futuro, en un marco de continuo avance tecnológico y comunicacional.

Argentina y el Teletrabajo

El fenómeno de teletrabajo, no ha escapado a su recepción y repercusión en la República Argentina. En nuestro país el Ministerio de Trabajo y Seguridad Social de la Nación conformó en 2003, una Comisión de Teletrabajo (11) que elaboró un proyecto de ley que ha perdido estado parlamentario. Sin embargo, mediante diversas fuentes periódicas (12), se sabe del ingreso de un nuevo proyecto de ley al Congreso de la Nación, que busca establecer condiciones mínimas que marquen reglas claras, para dependientes como para empresas, de aquellos que trabajan en su casa. Por último, cabe destacar que con fecha muy reciente -Marzo de 2011- se ha dado ingreso a tratamiento parlamentario a un nuevo proyecto de ley titulado: RÉGIMEN DE PROMOCIÓN Y REGULACIÓN DEL TELETRABAJO, cuyo objeto es promover y regular el Teletrabajo como un instrumento de generación de empleo mediante la utilización de tecnologías de la información y las telecomunicaciones (TIC); y como una herramienta de estimulación de la conciliación entre la vida familiar y laboral.(13)

Conclusión

El desarrollo permanente y acelerado de las TIC hace que el teletrabajo cada vez sea más común entre nosotros, y esto genera la necesidad de darle un marco legal adecuado para el desenvolvimiento del mismo. Debiendo tener en cuenta, los aspectos positivos y negativos, resaltando los ámbitos de influencia de esta modalidad de trabajo, se hará viable un marco legal en donde las necesidades reales de los teletrabajadores se tengan en mira. En donde se considere la amplia magnitud de esta modalidad de trabajo en los años venideros, marcando solo el el comienzo de una etapa de desarrollo y plenitud para esta área laboral.

Referencias

- 1- "Teletrabajo y salud: un nuevo reto para la psicología". <http://redalyc.uaemex.mx/pdf/778/77808308.pdf> Ultima consulta: 06/09/11
- 2- TOSELLI, CARLOS ALBERTO. (2005). Derecho del trabajo y de la seguridad social. Córdoba, 2da edición, Ed. Alveroni.
- 3- JURADO SEGOVIA & THIBAUT ARANDA, "Algunas consideraciones en torno al Acuerdo Marco Europeo sobre Teletrabajo", Temas laborales, N° 72, 2003.
- 4- Ver <http://www.jobing.com.ar>
- 5- Ver <http://www.jobing.com.ar/2010/09/hablemos-cifras-%C2%BFcuantos-teletrabajadores-hay-en-argentina/> Fecha de consulta: 09/07/2011.
- 6- Ver: <http://www.equiposytalento.com/noticias/2011/08/23/el-por-que-de-confiar-en-el-teletrabajo> y <http://laboralnews.blogspot.com/2011/09/ventajas-del-teletrabajo.html> Fecha de consulta: 25/08/2011,
- 7- MARCELA RODRÍGUEZ MEJÍA (2007) "El teletrabajo en el mundo y Colombia". Gaceta Laboral. Universidad de Zulia, Venezuela.
- 8- <http://www.trabajo.gov.ar/teletrabajo/?cat=18&subc=3>. Fecha de Consulta: 20/06/2011
- 9- MARCELA RODRÍGUEZ MEJÍA (2007) "El teletrabajo en el mundo y Colombia". Gaceta Laboral. Universidad de Zulia, Venezuela.
- 10- MARCELA RODRÍGUEZ MEJÍA (2007) "El teletrabajo en el mundo y Colombia". Gaceta Laboral. Universidad de Zulia, Venezuela.
- 11- La Comisión de Teletrabajo fue creada en el mes de septiembre de 2003 y de allí en más no han cesado las reuniones. El expediente de creación es el N° 1.079.053/03. www.trabajo.gov.ar/unidades/teletrabajo/antecedentes. Coordinación de la Comisión a cargo: Dra. Viviana Laura Díaz .
- 12- Páginas web: http://www.argentina.ar/_es/economia-y-negocios/C3307-proyecto-de-ley-para-regular-el-teletrabajo.php Fecha de consulta: 26/05/2011 - http://www.argentina.ar/_es/pais/C4701-proyecto-de-ley-para-regular-el-teletrabajo.php - Fecha de consulta: 26/05/20
- 13- <http://www1.hcdn.gov.ar/proyxml/expediente.asp?fundamentos=si&numexp=1172-D-2011> Fecha de consulta: 26/05/2011

EL TELETRABAJO Y SU PREVISIÓN NORMATIVA EN LA REPÚBLICA ARGENTINA.

Una aproximación acerca de los intentos legislativos de Argentina por regular el teletrabajo.

El fenómeno de teletrabajo, no ha escapado a su recepción y repercusión en la República Argentina (1). En nuestro país normativa legal vigente que regula las relaciones laborales abarca desde la Constitución Nacional, la Ley de Contrato de Trabajo 20.744 y modif., Ley Nacional de Empleo 24.013 (2), Ley 24.557 (Ley de Riegos de Trabajo), la Ley 11.544 (Jornadas), Ley 19.587 de "Higiene y Seguridad" y su Decreto Reglamentario, etc. Pero esta normativa es insuficiente a la hora de encuadrar y dar respuesta a las necesidades que plantean el uso de las TIC en el trabajo.

Podríamos adelantar que aún nuestro país no cuenta con un régimen jurídico especializado sobre teletrabajo, razón por la cual, hasta el día de hoy se han ensayado numerosos proyectos que todavía ninguno de ellos ha sido sancionado y promulgado con fuerza de ley (3).

Al 20 de octubre de 2010 la actividad legislativa fructificó siete proyectos, tres de los cuales proponían la inclusión del teletrabajo como Capítulo VI del Título III de la LCT De las Modalidades del Contrato de Trabajo entre ellos: el suscripto por la senadora (M.C.) Olijela del Valle Rivas (expte. 6077-D-2002); el propuesto por el diputado (M.C.) Dr. Oscar



Evangelina Magali Checa, es Abogada (UNC), empleada de la Secretaría Laboral del Tribunal Superior de la Provincia de Córdoba.

Lamberto (expte. 0941-D-2006) y el de la senadora (M.C.) Prof. Graciela Bar (expte. 2337-S-2007). Los cuatro restantes, en cambio proponían una regulación especial estatutaria, denominándolo como "Régimen Jurídico del Teletrabajo en Relación de Dependencia", uno enviado por el Poder Ejecutivo (expte. 0159-PE-2007), elaborado por la Comisión de Teletrabajo del Ministerio de Trabajo, Empleo y Seguridad Social; otro denominado "Regulación del Trabajo a Distancia Producido a través de Medios Tecnológicos de Información y Comunicación" suscripto por la Senadora Adriana Bortolozzi de Bogado (expte. 2537-S-2008); en tanto que los otros dos restantes intitulados "Régimen Jurídico del Teletrabajo en Relación de Dependencia" (S-3498/10) y "Promoción y Difusión del Teletrabajo" (S-3499/10) ambos proyectos de los mismos autores: Adolfo Rodríguez Saá.; Roberto Basualdo; Arturo Vera.-Adriana Bortolozzi de Bogado; Graciela di Perna; Hilda González de Duhalde; Emilio Rached; Juan Romero y Liliana Negre de Alonso, estos dos últimos se alinearían dentro de la postura de regular al teletrabajo como estatutos especiales

A continuación haremos una breve consideración de los proyectos antes referenciados, conforme los clasificáramos con anterioridad en dos grupos.

Proyectos legislativos que regulan al teletrabajo como un capítulo de la Ley de Contrato de Trabajo (ley 20.744):

I) El proyecto de de la Diputada Olijela del Valle Rivas (25/9/2002), define la figura con las siguientes notas tipificantes: por la falta de presencia física del trabajador en la empresa, la utilización de las TIC y el contacto regular entre las partes.

Considera también, diversas formas de teletrabajar conforme al lugar en donde se preste –domicilio del trabajador, telecentros u oficinas satélites ofrecidas por la empresa, oficinas virtuales o móviles (distintos lugares sin fijación en uno) u otras opciones- siempre que se den los caracteres del teletrabajo. Prevé la posibilidad de que el trabajador opte por esta modalidad y viceversa, siempre que no entre en colisión con los arts. 64 y 65 de la LCT y la reglamentación que se establezca. A su vez fija condiciones igualitarias entre teletrabajadores y trabajadores presenciales de la empresa, siempre y cuando sean compatibles; la exigencia al empresario de proveer y financiar el mantenimiento de equipamientos y la prohibición de allanar el domicilio del trabajador por parte del empleador. El proyecto se delega su reglamentación e indica establecer requisitos de admisibilidad, porcentaje máximo de teletrabajadores y un registro de empleadores que implementen esta modalidad.

II) El del Diputado Lamberto (23/3/2006), preveía la incorporación a la LCT de un artículo 102 bis, que incluyera al teletrabajo a las modalidades contractuales, considerándolo como una forma de tra-



bajo en que el trabajador realiza tareas a través de una computadora, desde una ubicación remota de la sede de empleador.

III) El de la Senadora Bar (20/7/2007), define el teletrabajo como la realización de actos, ejecución de obras o prestación de servicios realizada total o parcialmente en el domicilio del trabajador o en lugares distintos del establecimiento del empleador, mediante la utilización de todo tipo de TIC. Podríamos señalar que es similar al primero expuesto, en cuanto a la caracterización del teletrabajo, conceptualización y denominación de los sujetos que lo integran, realizando también un enunciado no taxativo relacionado con las diversas formas y modalidades que puede presentar este contrato. Fija condiciones igualitarias de los teletrabajadores con los demás trabajadores que prestan igual actividad en la sede de la empresa; impone la obligación al empresario de facilitar el equipamiento y mantenimiento del mismo, siendo el trabajador responsable de su correcto uso y de la utilización por terceros no autorizados, en supuesto que las TIC sea facilitadas por el trabajador, los gastos en que este incurriera deberán ser compensados en su totalidad por el

empleador. También se resguarda la intimidad del trabajador y la privacidad de su domicilio; y al igual que el primer proyecto de esta línea se preveía su reglamentación sin fijar contenidos.

Proyectos legislativos que proponen al teletrabajo como una normativa especial:

I) En el seno del Ministerio de Trabajo, Empleo y Seguridad Social de la Nación, se conformó en septiembre de 2003, una Comisión de Teletrabajo (4) (interdisciplinaria), la que elaboró y elevó al P.E.N. en julio de 2007 un proyecto de ley (5) perdiendo estado legislativo.

El mencionado proyecto surge como una consecuencia necesaria de la ratificación por Ley N° 25.800 del Convenio de la OIT N° 177 sobre “Trabajo a Domicilio”, el que incluye en su normativa a todo tipo de modalidad de trabajo a distancia, entre ellas el “teletrabajo, a su vez consideró la necesidad de dotar a los actores sociales de reglas de juego claras que no descuiden los “derechos de los trabajadores” y su fácil implementación al mercado laboral por parte del empresariado.

El proyecto de 2007, mentado por la Dra. Viviana Laura Díaz, definía la figura en un sentido funcional, remarcando las condiciones que se deben prever para la operatividad de la normativa, concordando con la legislación general y con la internacional, en orden al trabajador dependiente y poniendo especial énfasis a la ajenidad del espacio de trabajo con respecto al poder de dirección y organización del empleador.

El proyecto referenciado tenía la intención de convertirse en un piso mínimo sobre el cual las partes, ya sea individual o colectivamente pacten condiciones específicas de teletrabajar.

II) El proyecto presentado por la Senadora Bortolozzi de Bogado (septiembre 2008) resulta similar

al anterior comentado, con particularidades tales como: extiende los beneficios al teletrabajador autónomo; incluye la compensación en los gastos de mantenimiento de equipos cuando el trabajador los aporte y el correcto uso si es el empleador el dador de los mismos; reconoce al teletrabajador el pleno ejercicio de los derechos intelectuales y patentes sobre toda invención fruto de su labor, salvo pacto en contrario, garantizando la inviolabilidad de dichos, descubrimientos científicos; aplicación directa del art. 23 de la LCT al teletrabajador; establece la obligación de adecuar las normas de higiene y seguridad, prevención y reparación de riesgos y accidentes del trabajo a esta modalidad; listado de enfermedades laborales específicas, prohíbe al empleador modificar unilateralmente la modalidad de teletrabajo a presencial, necesitando el consentimiento expreso del trabajador, como así también para su reversión.

III) El proyecto de los Senadores Rodríguez Saá, Basualdo, Bortolozzi de Bogado, di Perna., González de Duhalde, Rached, Romero y Negre de Alonso (octubre de 2010 -S-3498/10-), “Régimen Jurídico del Teletrabajo en Relación de Dependencia” (6), mantiene la misma línea del antiguo proyecto presentado por la “Comisión de Teletrabajo” del MTEySSN bajo el Expte. S-159/07 caduco el 28/02/09. Este se basó en aquel antecedente, al que se le introdujeron modificaciones sugeridas por especialistas en la materia y en orden a garantizar los derechos de los trabajadores.

IV) El proyecto (7) firmado por los mismos senadores que el anterior referenciado (octubre de 2010 - S-3499/10) titulado “Promoción y Difusión del Teletrabajo”, incluiría a teletrabajadores en relación de dependencia como autónomos y al sector privado y público en todos sus niveles, nacional, provincial y municipal. A su vez, define al teletrabajo ampliamente (8).

Asimismo, establece que el P.E. deberá incentivar y facilitar la incorporación al teletrabajo de personas con discapacidad, población en situación de aislamiento geográfico o desplazamiento social, mayores de 45 años, jóvenes sin experiencia, mujeres con niños o mayores a cargo, acompañantes y cuidadores, y toda población vulnerable en general, quienes conservarán los beneficios que ya le hayan sido otorgados por otras leyes.

Instituye como autoridad de aplicación al MTEySSN de manera conjunta con el Ministerio de Acción Social de la Nación y el Ministerio de Educación de la Nación.

Sin perjuicio de los diferentes proyectos de ley que comentados con anterioridad, conforme afirmaciones vertidas en los diarios de publicación local y en sitios web, el Gobierno (desde el seno del MTEySSN) ultima los detalles para establecer, un nuevo proyecto de ley que fijen condiciones "de mínima" que marquen reglas claras, tanto para los dependientes como para las empresas. El principal punto, hará hincapié en la relación de igualdad entre el teletrabajador y aquel empleado que presta servicios de manera presencial (9).

Autora: Evangelina Checa

Bibliografía:

- De Virgiliis, M. A. - De Virgiliis, M. I. (2001) "El Teletrabajo. De la Chimenea a la Sociedad de la Información", Doctrina del Trabajo -B, pp. 1365 y ss.
- Díaz Aloy, V. (2009). "Consideraciones Acerca de los Enfoques Regulatorios del Teletrabajo". Colección Temas de Derecho Laboral. Errepar, pp. 27-41.
- Ledesma Iturbide, D. (2009) "Debates de Actualidad. La Regulación del Teletrabajo", Revista de Derecho Laboral. Actualidad. 2009-2, pp. 171-188.

Sitios Web:

- www.eclac.cl/socinfo/noticias/noticias/2/32222/GdT_eLAC_meta_5.pdf
- www.prensa.argentina.ar/.../11686-tomada-anuncio-que-se-enviara-un-proyecto-de-ley-para-regular-el-teletrabajo.php
- www.argentina.ar/_.../C3307-proyecto-de-ley-para-regular-el-teletrabajo.php
- www.argentina.ar/_.../C4701-proyecto-de-ley-para-regular-el-teletrabajo.php
- www.trabajo.gov.ar/.../teletrabajo/legislacion.htm

Referencias:

1- Unas de las empresas nacionales pioneras en implementar esta modalidad fue la petrolera YPF, la primera empresa adherente al Programa Piloto de Seguimiento y Promoción del Teletrabajo en Empresas Privadas (Propet) a partir de la firma del Convenio Marco con el Ministerio de Trabajo de la Nación. El mismo se puso en marcha a partir del 2 de mayo de 2008, donde 31 universitarios y 9 técnicos –con diferentes especialidades, grupo étnico y género-, durante 6 meses experimentaron dicho "sistema". "La firma destacó –en su oportunidad- que los 'empleados incluidos en el programa... gozarán de los mismos derechos y beneficios garantizados por la legislación vigente y convenios colectivos de trabajo que aquellos que prestan la mismas tareas en los establecimientos de la empresa, sin perjuicio de los... que se pacten en forma individual y colectiva, teniendo en cuenta las peculiaridades del trabajo..." a su vez "...se fijarán las condiciones referidas a la protección de los bienes e información, a salvaguardar la privacidad del dominio del trabajador y la adhesión a las normas de higiene y seguridad en el lugar del trabajo..." (la negrita nos pertenece). Pastorino, A. en Diario Comercio y Justicia del 24/04/08. www.ticordoba.com.ar/index.php?option=com_content&task=view&id=1516&Itemid=2.

2- En su Título III "De la promoción y defensa del empleo", Capítulo I "Medidas e incentivos para la generación de empleo", su artículo 22 prevé en el inciso e) "atender los efectos sobre el empleo de las políticas tecnológicas de modo que, a la par de buscar una mayor eficiencia económica en áreas prioritarias, preserve para otros sectores un balance más equilibrado en el uso de los recursos" y en su inciso g) "Desarrollar una asociación más estrecha entre la capacitación y formación de la fuerza laboral y el sistema productivo", en su artículo 23 prevé que la incorporación de tecnología constituye una condición para el crecimiento de la economía nacional. Es un derecho y una obligación del empresario que la ley reconoce, garantiza y estimula, y en la medida que afecta las condiciones de trabajo y empleo debe ser evaluada desde el punto de vista técnico, económico y social.

3- Sin perjuicio de ello, en mayo de 2010 en el MTEySSN firmó la "Declaración de lineamientos y compromisos en materia de teletrabajo, para la promoción de trabajo decente y como garantía de calidad laboral" "2010 - AÑO DEL BICENTENARIO DE LA REVOLUCION DE MAYO", www.trabajo.gov.ar y declaraciones del Ministro Carlos Tomada en www.prensa.argentina.ar/.../11686-tomada-anuncio-que-se-enviara-un-proyecto-de-ley-para-regular-el-teletrabajo.php

4- La Comisión de Teletrabajo fue creada en el mes de septiembre de 2003 El expediente de creación es el N° 1.079.053/03. www.trabajo.gov.ar/unidades/teletrabajo/antecedentes.

5- Régimen jurídico del teletrabajo en relación de dependencia, elevado al P.E.N el 02/07/2007, www.trabajo.gov.ar.

6- Consulta - www.teletrabajolegal.org.ar efectuada en marzo 2011.

7- Promoción y difusión del Teletrabajo en www.trabajolegal.org.ar, consulta efectuada en marzo 2011.

8- "(...) A los efectos de esta ley se entiende por teletrabajo a la modalidad de realización u organización del trabajo donde la prestación laboral al empleador o la prestación de servicios a terceros en forma autónoma se llevan a cabo mediante la utilización de las tecnologías de la información y de la comunicación fuera del ámbito físico donde está el contratante en forma total o parcial (...)"

9- www.argentina.ar/_.../C3307-proyecto-de-ley-para-regular-el-teletrabajo.php, consulta marzo 2011.

EVIDENCIA DIGITAL: ADMISIBILIDAD Y VALORACIÓN EN EL DERECHO PROCESAL CIVIL Y PENAL DE LA PROVINCIA DE MENDOZA (ARG) - PARTE 2

IV. EVIDENCIA DIGITAL EN EL PROCESO CIVIL

“ART. 181 - MEDIOS DE PRUEBA – Son medios de prueba: Los documentos, la confesión, el dictamen e informe de peritos y expertos, la declaración de testigos, el examen judicial, reproducciones y experiencias y cualquier otro no prohibido por la ley en general o para casos particulares, que sea idóneo y pertinente...”

Si bien el Código de Procedimiento no contiene disposiciones específicas respecto del uso de medios electrónicos, se entiende que, dado el marco legal general que habilita el uso de documentos electrónicos, la presentación de evidencia digital está admitida.

En este artículo se consagra el principio de libertad de medios de prueba, el cual implica la posibilidad que tanto las partes como el juez, puedan introducir en el proceso las pruebas necesarias para acreditar los hechos invocados, incluyendo aquella que consta en formato digital, siempre que cumpla con las condiciones de admisibilidad, esto es, que sea una prueba:

- **Idónea:** es decir, que es apta para producir en el juez convicción o convencimiento respecto del hecho en cuestión.

- **Pertinente:** tiene que estar referida a hechos cuyo conocimiento sea relevante para el proceso.



*Dra. Bárbara Peñaloza – Abogada –
Cursando el Posgrado en Especialización en Derecho Informático de
EIDerechoInformatico.com – Argentina*

- No debe estar prohibida por la ley en general o para casos particulares.

“ART. 206 - OTROS MEDIOS DE PRUEBA – Cuando se ofreciere un medio de prueba idóneo y pertinente, no previsto por la ley, el tribunal establecerá la manera de diligenciarlo, aplicando en lo posible, por analogía, el procedimiento formado para otras pruebas.”

“ART. 207 - APRECIACION DE LA PRUEBA – Todas y cada una de las pruebas serán apreciadas según las reglas de la Sana Crítica, salvo disposición expresa en contrario.”

El principio de libertad de prueba permite que el Juez pondere otros medios de prueba no contemplados específicamente en la normativa procesal. En efecto, el Juez dispone de la facultad de admitir, ordenar, valorar e interpretar distintos elementos de prueba, que le permitan formar su convicción respecto de los hechos alegados por las partes.

El principio de libertad probatoria es relevante al considerar el tema de evidencia digital. Como los medios de prueba electrónicos no están expresamente contemplados en el Código Procesal, la validez de la prueba digital se fundamenta en el sistema de libertad probatoria y en la amplia potestad del juez para su interpretación.

En conclusión, considero que una adecuada práctica consistiría en presentar la prueba obtenida por medios electrónicos junto con la prueba Documental (por ejemplo, presentar en soporte papel la cadena de mails que prueban la existencia de un contrato), es decir, al momento de interponer la demanda (Arts. 165 y 212 CPC Mendoza), haciendo expresa reserva de apoyar dicha prueba, en el momento procesal oportuno, con informes técnico – jurídicos que brinden elementos para formar la convicción del Juez, esto es, explicar los métodos que se han aplicado para la obtención de la prueba, su resguardo y conservación segura, su eventual modificación de formato, los mecanismos de autenticación que se han utilizado, y la certificación de copias respectiva.

Se admite la participación de expertos para la realización de pericias e informes técnicos. La prueba pericial debe ofrecerse, en los procesos ordinarios, cuando se abra la causa a prueba, y en los procedimientos sumarios y sumarísimos, junto con la demanda.

Los peritos pueden ser presentados por las partes o, si estas no designan uno, son nombrados de oficio, luego de realizar un sorteo entre los que se encuentran inscriptos en las listas oficiales. Pueden intervenir entre uno y tres peritos en un mismo proceso, dependiendo de la complejidad del asunto. Los informes y pericias son elementos de prueba expresamente contemplados en las normas procesales. En Mendoza se exige que el informe de-



talle los principios científicos o prácticos, las operaciones experimentales o técnicas en las cuales se funde y las conclusiones, respecto a cada punto sometido.

El perito es un auxiliar del juez, el Código Procesal establece los requisitos profesionales para acreditar la idoneidad del mismo. El Artículo 19 dispone que para aquellos casos en los cuales la profesión estuviese reglamentada, el perito deberá tener título habilitante en la ciencia, arte, industria o actividad técnica especializada a que pertenezcan las cuestiones acerca de las cuales deba expedirse. En caso contrario, o cuando no hubiere en el lugar del proceso perito con título habilitante, podrá ser nombrada cualquier persona con conocimientos en la materia.

Respecto de los expertos informáticos, se pueden inscribir en las listas del Poder Judicial de Mendoza, dentro de la categoría de "Ciencias Informáticas", para lo que deberán presentar, entre otras cosas, Diploma Original debidamente legalizado por el Ministerio de Educación de la Nación, por lo que se puede deducir que se exige título habilitante, ya sea en Ingeniería o alguna Licenciatura.

Considero que el perito informático debe tener conocimientos técnicos en Arquitectura de Computadoras, Tecnología Informática, Redes de computadoras, Transmisión de Datos, Programación, Diseño de Sistemas, Modelización y Bases de datos. Así como también debe tener conocimiento del Marco Legal y la Práctica procesal.

Dado que el tema de la pericia informática no está expresamente regulado en las normas de procedimiento, no existen criterios, políticas ni manuales para la obtención, producción, conservación y presentación de pruebas electrónicas. Tampoco reglas y obligaciones específicas para dichos peritos. Se aplican las generales de la ley respecto de estos colaboradores de la Justicia.

- Medidas Precautorias

En muchas oportunidades, antes de iniciar la demanda o después de iniciada esta, es posible que sea conveniente, a los fines de asegurar la evidencia solicitar, por ejemplo, el secuestro de la notebook donde se encuentran los archivos que acreditan la existencia de un contrato, de un celular o de Smartphone, de una cámara de fotos, etc.

Para estos casos, se deberá solicitar al juez, alguna de las medidas precautorias previstas en el CPC Mendoza o alguna medida que, no estando prevista, sea idónea para asegurar provisoriamente un derecho (Art. 115 CPC Mendoza).

Entre las medidas enumeradas (de modo no taxativo), podría solicitarse el secuestro de bienes determinados o el depósito de cosas.

V. EVIDENCIA DIGITAL EN EL PROCESO PENAL

El nuevo Código Procesal Penal de la Provincia de Mendoza fue dictado en 1999 por Ley 6730. Si bien es un código nuevo, no hace mención alguna a

la evidencia digital, debiendo adaptarse también las normas generales sobre prueba y aplicarlas para el caso de que se esté en presencia de evidencias contenidas en soportes electrónicos.

En términos generales, el proceso penal consta de dos etapas, en las cuales intervienen dos instancias judiciales diferentes. La primera etapa, de instrucción, corre a cargo del Juez de Garantías, el Fiscal de Instrucción y las fuerzas policiales y de seguridad. La segunda etapa, de sentencia, está a cargo de un tribunal oral de sentencia, el cual recibe la prueba y alegatos de las partes, es decir, del ministerio público fiscal en representación del Estado, y de la defensa en representación del procesado.

Las medidas preparatorias, primera etapa del juicio penal o etapa de instrucción, son ordenadas por el Juez de Garantías, solicitadas u ordenadas por el Agente Fiscal de Instrucción, o realizadas por la Policía o Fuerzas de Seguridad.

- Potestades. Conducción de la investigación.

Las medidas preparatorias son desarrolladas por el Fiscal de Instrucción o la Policía Judicial.

El Artículo 333 establece las funciones de la policía Judicial. Faculta a dichas fuerzas a investigar, por iniciativa propia, en virtud de denuncia o por orden de autoridad competente, los delitos de acción pública, impedir que los hechos cometidos sean llevados a consecuencias ulteriores, individualizar a los culpables y reunir las pruebas para dar base a la acusación.

Si el delito fuera de acción pública dependiente de instancia privada, sólo deberá proceder cuando reciba la denuncia del particular damnificado.

El Artículo 336 enumera las atribuciones de los funcionarios de la policía judicial.

Art. 336 - Atribuciones. La Policía Judicial tendrá las siguientes atribuciones:

1) Recibir denuncias.

2) Cuidar que el cuerpo, instrumentos, efectos y rastros del delito sean conservados, mediante los resguardos correspondientes, hasta que llegue al lugar el Fiscal de Instrucción.

3) Si hubiere peligro de que cualquier demora comprometa el éxito de la investigación, hacer constar el estado de las personas, cosas y lugares, mediante inspecciones, planos, fotografías, exámenes técnicos y demás operaciones que aconseje la policía científica.

4) Proceder a los allanamientos, a las requisas urgentes y a los secuestros impostergables.

5) Si fuera indispensable, ordenar la clausura del local en que se suponga, por vehementes indicios, que se ha cometido un delito grave.

6) Interrogar sumariamente a los testigos presumiblemente útiles para descubrir la verdad.

7) Citar y aprehender al presunto culpable en los casos y forma que este Código autoriza.

8) Recibir declaración al imputado, sólo si éste lo pidiera, en las formas y con las garantías que establece el Código.

9) Usar de la fuerza pública en la medida de la necesidad.

El Artículo 337 del citado Código prohíbe a los funcionarios de la policía y fuerzas de seguridad abrir la correspondencia que secuestren, debiendo ser remitida intacta a la autoridad judicial competente. Tampoco podrán difundir a los medios de prensa los nombres y fotografías de las personas investigadas como participantes de un hecho.

Respecto de la investigación relacionada con elementos tecnológicos, la Policía Federal cuenta con una unidad especial, la Policía Científica, que presta apoyo en estos temas. Sin embargo, aún no se dispone de Manuales de Procedimientos ni de Guías para la obtención de evidencia digital, conservación, preservación y presentación en juicio. La policía provincial, está aún más desprovista de elementos.

El Fiscal por su parte, está facultado para proponer y producir prueba. El código autoriza al fiscal para citar a testigos, requerir informes, disponer las medidas que considere necesarias y practicar las inspecciones de lugares y cosas con la debida orden judicial de allanamiento en caso de ser necesario.

El Código autoriza a las partes a proponer actos procesales o la obtención de medios de prueba en cualquier momento de la investigación, quedando facultado el fiscal para decidir sobre su pertinencia.

En la etapa de juicio, el Código prevé que se presenten las pruebas producidas en la etapa de instrucción, admitiendo también la posibilidad de instrucción suplementaria para realizar las medidas que hubieren sido omitidas o denegadas en su oportunidad. Asimismo, el tribunal tiene facultades para ordenar nuevas medidas de prueba.

- U.D.A.P.I.F: Unidad De Apoyo Para la Investigación Fiscal

En el Art. 3 del Pacto Social se acordó que el Gobierno de la Provincia de Mendoza debía aportar a la U.D.A.P.I.F. toda la información disponible en las distintas bases de datos de la Provincia.

Por otra parte, se firmaron Convenios Particulares de Cooperación con cada uno de los Organismos que han autorizado:

- El acceso directo vía Web Service o
- La Comunicación vía correo electrónico con Firma Electrónica

Así, se firmaron acuerdos de cooperación con la DGR, la Dirección General del Registro Civil, la D.N.R.P.A., el CodeMe (Clearing de Créditos del Comercio de Mendoza), entre otros, que permiten la colaboración de estos organismos para la prevención y el pronto esclarecimiento de delitos con el Ministerio Público Fiscal, permitiendo el fácil acceso del mismo a consultar los datos disponibles en sus bases de datos informáticas, ya sea (según se dijo anteriormente) por el acceso directo vía Web Service, con un usuario y contraseña, o mediante correos electrónicos emitidos por estos organismos al Ministerio Fiscal, rubricados con Firma Electrónica.

- Prueba

El Código establece el principio de libertad de la prueba:

Art. 205 - Libertad Probatoria. Todos los hechos y circunstancias relacionados con el objeto del proceso pueden ser acreditados por cualquier medio de prueba, salvo las excepciones previstas por las leyes.

Art. 206 - Valoración. Las pruebas obtenidas durante el proceso serán valoradas con arreglo a la sana crítica.

Art. 207 - Exclusiones Probatorias. Carecen de toda eficacia probatoria los actos que vulneran garantías constitucionales. La ineficacia se extiende a todas aquellas pruebas que, con arreglo a las circunstancias del caso, no hubieren podido ser obtenidas sin su violación y fueran consecuencia necesaria de ella.

Entre las pruebas enumeradas encontramos:

- Inspección y Reconstrucción,
- Registro y Requisa (que debe ordenarse por decreto fundado, bajo pena de nulidad),
- Allanamiento de la morada (siempre que se cumpla con las formalidades pertinentes, por orden dictada por decreto fundado de juez competente)
- Secuestro, y en este capítulo hay algunos artículos interesantes:

Art. 225 - Documentos Excluidos. No podrán secuestrarse, bajo pena de nulidad, las cartas, documentos, grabaciones o elementos soportes de medios electrónicos que se envíen o entreguen a los defensores para el desempeño de su cargo.

Art. 226 - Custodia o depósito. Los efectos secuestrados serán inventariados y puestos bajo segura custodia. (...) Se podrá disponer la obtención de copias o reproducciones de las cosas secuestradas cuando éstas puedan desaparecer, alterarse, sean de difícil custodia o convenga así a la investigación penal preparatoria. Las cosas secuestradas serán aseguradas con el sello del Tribunal o Fiscalía de Instrucción que intervenga y con la Firma del Juez o del Fiscal, según corresponda, y del Secretario, debiéndose firmar los documentos en cada una de sus hojas. (...)

Art. 227 - Intercepción de Correspondencia. Siempre que lo considere útil para la averiguación de la verdad, el Tribunal podrá ordenar por decreto fundado, bajo pena de nulidad, la interceptación o el secuestro de la correspondencia postal, telegráfica, electrónica o de todo efecto remitido por el imputado o destinado al mismo, aunque sea bajo nombre supuesto.

- Testigos
- Peritos

Art. 245 - Calidad Habilitante. Los peritos deberán tener título habilitante en la materia a que pertenezca el punto sobre el que han de expedirse, siempre que la profesión, arte o técnica estén reglamentados. En caso contrario, o cuando no existan peritos diplomados, deberán designarse a personas de conocimiento o práctica reconocidos.

Art. 249 - Nombramiento y Notificación. Se designará un perito, salvo que se estimare indispensable que sean más (...)

Art. 250 - Peritos de Control. (...) cada parte podrá proponer a su costa otro perito legalmente habilitado (...)

VI. CONCLUSIONES

Se advierte que en la legislación argentina hay ciertos avances, así, ya existe un marco legal sustantivo que otorga valor legal al documento electrónico, se considera que un elemento de prueba en formato digital es jurídicamente un documento electrónico válido en virtud de la Ley 25.506, y ya hay bastante jurisprudencia que acepta a la evidencia en formato digital como prueba válida.

Sin embargo, existen pocas normas procesales modernas que contemplen el tema de evidencia digital (en Mendoza no hay ninguna, a pesar de que el Código Procesal Penal es muy reciente) y existe disparidad de criterios judiciales para interpretar un elemento de prueba electrónico presentado en juicio.

Por otro lado, en Mendoza, los procedimientos se sustancian en soporte papel, aunque paulatinamente se va logrando la digitalización de los documentos que se ofrecen como prueba. Sin embargo, los tribunales deben hacer copia de estos documentos para agregarlos en soporte papel al expediente,

por lo que aún no existe el “expediente digital”. Por otro lado, se advierte cierto avance, pues ya están en funcionamiento las notificaciones electrónicas y de consulta del estado del expediente en forma remota por Internet, y funcionan satisfactoriamente, lo que significa una importante disminución de costes y una aceleración en los procedimientos.

También se advierte la inexistencia de oficinas específicas de conservación de evidencia digital y de manuales de procedimientos para la obtención, preservación y presentación en juicio de evidencia digital.

Por lo tanto, creo que es indispensable comenzar a incorporar el uso de las nuevas tecnologías en la administración de justicia, para la gestión electrónica de expedientes, las notificaciones y la admisión de evidencia digital, y complementar el uso de la tecnología con leyes específicas de administración electrónica que doten a los magistrados, funcionarios y auxiliares de la Justicia, como la policía y las fuerzas de seguridad, del marco normativo adecuado para una gestión acorde al siglo XXI, en el que impera la tecnología y las telecomunicaciones, las que evolucionan a pasos agigantados.

Autora: Dra. Bárbara Virginia Peñaloza

SELLOS DE CONFIANZA: INCREMENTANDO LA SEGURIDAD EN EL COMERCIO ELECTRÓNICO

¿A la falta de regulación y control del sector gobierno de las empresas que ofertan y venden sus productos por medios de Internet, es posible incrementar la confianza de los ciudadanos?

¿Confiar o no confiar?... ¡Esa es la cuestión! Esta simple pregunta representa la principal disyuntiva que tiene que resolver una persona para decidir si compra o no un artículo por Internet.

Adquirir un producto en una Tienda Electrónica tiene múltiples beneficios, tales como: total disponibilidad (debido a que se puede tener acceso las 24 horas todos los días de la semana), adquisición de bienes y/o servicios fuera del lugar de residencia, inclusive fuera del territorio nacional, comparar precios, investigar funcionalidades de los productos; y sólo contando con una computadora personal y acceso a Internet; sin embargo,

Siendo tal la cantidad de ventajas ¿Qué circunstancias se suscitan para que merme la confianza de los usuarios?

En México contamos con un marco jurídico (1) suficiente que regula el desarrollo del Comercio Electrónico, sin embargo éste no ha sido un factor determinante para incrementar la confianza. Un estudio realizado por la Asociación Mexicana de Internet AMIPCI (2) revela que existen dos grandes factores que disminuyen la confianza. Por una parte los compradores potenciales se sienten inseguros al momento de realizar el pago, sobre todo con el uso que puedan hacer con la información de su tarjeta de crédito, y por otra existe un gran temor para proporcionar datos personales a través de la red.



José Luis Chávez Sánchez, Lic. en Derecho, egresado de la UNAM, labora desde hace 10 años en la misma UNAM, en la DGETIC, experto en el manejo de temas a fines al derecho informático.

Estos factores son los principales problemas que enfrenta el Comercio Electrónico, por tal razón la industria ha buscado la manera de fortalecer la seguridad y certeza en los usuarios, la pregunta a resolver en ese momento fue: ¿Bajo que procedimientos se podría incrementar tan ansiada confianza? Es al final de la década de los 90's cuando "a iniciativa del Canadian Institute of Chartered Accountants (CICA) y del American Institute of Chartered Public Accountants (AICPA)"(3), surgen los "sellos de confianza" (SysTrust o WebTrust), éste fue el detonante para que otras empresas del sector privado empresarial (principalmente) apoyaran este tipo de prácticas, generándose una gran gama de sellos, con mayores o menores beneficios.

Y a todo esto, ¿Qué son los sellos de confianza? Como su nombre lo sugiere son marcas (distintivos) electrónicas, las cuales son otorgadas casi siempre por alguna entidad privada, son publicados en las páginas Web e indican que la empresa: cumple con las leyes, códigos éticos y de buenas prácticas; brinda una mayor seguridad tecnológica y procedimental antes, durante y después de la transacción (Sobre todo en el tratamiento de la información recabada de datos personales y tarjetas de crédito); indican mecanismos para resolver controversias entre comprador y vendedor.

En pocas palabras estos distintivos pretenden “aumentar la confianza de los consumidores sobre la seguridad, privacidad, transparencia y funcionalidad de las empresas que los obtienen, al cumplir con los requisitos establecidos. (4)”

En México surgen los sellos de confianza, impulsado por la Asociación Mexicana de Internet (AMIPCI), teniendo como peculiaridad el apoyo del Gobierno Federal a través de la Secretaría de Economía y la Procuraduría General del Consumidor.

La AMIPCI revisa que la empresa o Institución que cuenta con un sitio Web en operación y que solicita el sello, cumpla con cuatro aspectos, y mediante un pago otorga el sello de confianza en un documento electrónico con un certificado digital, bajo la figura de una licencia de marca de certificación.

Los elementos que la AMIPCI vigila que cumplan las empresas e Instituciones son:

1.Cumplir con el marco legal aplicable a cada sector:

a)En lo que concierne al sector privado deben ajustarse a lo señalado por la Ley Federal de Protección al Consumidor en sus artículos 16, 17, 18 bis, 76 bis (Proporcionar en el Sitio Web números telefónicos, dirección y demás información de la organización que permitan al comprador realizar aclaraciones o reclamaciones; usar la información recabada sólo para los fines solicitados garantizando la confidencialidad de la misma y no ceder dicha información a terceros; evitar prácticas de envío spam (5), así como eliminar las prácticas comerciales engañosas.)

a)En lo que concierne al sector público deben cumplir con lo señalado en Ley Federal de Transparencia y acceso a la información Pública y los Lineamientos de Protección de Datos Personales.

2.Sujeción al Marco sobre privacidad de la Cooperación Económica del Asia-Pacífico (APEC por sus siglas en Inglés) a través de avisos de privacidad y sus respectivos resúmenes.

3.Observancia del Código de Ética de la AMIPCI.

4.Cumplimiento de los términos y condiciones establecidos en el contrato celebrado entre la AMIPCI y los titulares del sello.

De esta manera, al cumplir con estos cuatro puntos se otorga el sello de confianza, y con ello se reconoce a las empresas o instituciones (sectores público y privado) que promueven el cumplimiento de la privacidad de la información y están legítimamente establecidas.

Es de resaltar que la AMIPCI también ofrece un procedimiento entre las partes para resolver las controversias que pudieran suscitarse con los consumidores de los titulares del sello.

Los sellos de confianza es una solución importante que busca generar confianza en los internautas que día con día navegan por la red y con ello darle un impulso más al desarrollo del Comercio Electrónico, sólo el tiempo nos dirá la aceptación e impacto de éstos en el comercio electrónico y sus usuarios.

Autor: Jose Luis Chávez Sanchez

Referencias:

1- Código de Comercio, La Ley Federal de Protección al Consumidor, Código Civil Federal, Código Federal de Procedimientos Civiles.

2- "Estudio realizado" www.amipci.org.mx/temp/ResumenEjecutivoEstudioAMIPCI2005-0315079001138390784OB.pdf

3 - http://www.amipci.org.mx/en_los_medios.php?mcmvme=266

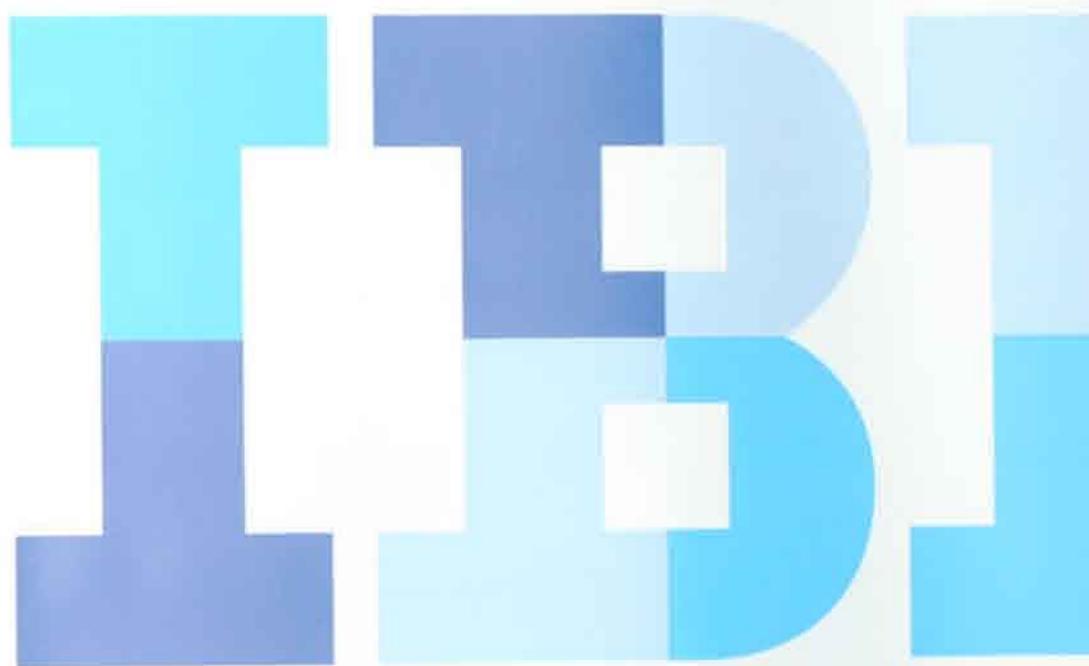
4- "Libro Blanco sobre los Sistemas de Autorregulación, los Sellos y Marcas de Confianza en Mercados Digitales y Códigos de Buenas Prácticas para el comercio electrónico", Dr. Miguel Ángel Martínez, http://www.e-global.es/confianza/libro_blanco_sellos.zip

5- Son mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas, ya sea por correo electrónico u otros medios.

“

LA ESTRELLA DEL MUNDO IT CONTINÚAN SIENDO LOS SERVICIOS. EL SERVICIO DE NUBES ES EL SEGMENTO QUE SE LLEVA LA MAYOR INVERSIÓN EN AMÉRICA LATINA. EL SERVICIO DE NUBES REPRESENTA LA PRINCIPAL FUENTE DE INGRESOS PARA LAS EMPRESAS DE IBM.

Jorge Goulu es Ingeniero Industrial del ITBA (Instituto Tecnológico de Buenos Aires). Comenzó su carrera en IBM en 1987. En sus más de 20 años de experiencia en IBM, ha ocupado cargos de liderazgo como Director de Canales para Sudamérica y América Latina, Gerente de Ventas para Argentina, Paraguay y Uruguay, Gerente de áreas de Marketing y el Sector Industrial. Actualmente es el Presidente y Gerente General de IBM en Argentina.



[ibm.com/](https://www.ibm.com/)

CIOS. NO SOLO ES EL
A LATINA SINO QUE
MPAÑÍAS.”

*carrera en IBM Argentina en el año
ctor de SMB para SSA, Director de
uay, y ha trabajado también en las
Argentina.*



*Jorge Goulou
Presidente y Gerente General de IBM Argentina*

1 - Cómo se llega a ser CEO de IBM?

Cuando estudiaba en el ITBA se hablaba de las empresas grandes y yo tenía ganas de trabajar en una empresa así. Entre las compañías que sonaban, estaba IBM. En mi caminata diaria de Retiro al ITBA, entré en IBM y dejé un curriculum. Me llamaron para entrar como becado en el año 1986. Comencé a trabajar en el sector industrial. Me asignaron inmediatamente a un proyecto para Acindar, que estaba automatizando sus hornos. IBM le ofrecía un programa que tomaba datos de la producción y generaba gráficamente un flujo de alimentación del horno, se conectaba con los laboratorios y el programa dosificaba los componentes que iban a volcarse en el horno. Para mí era ciencia ficción lo que estaba haciendo. El cliente en ese momento era una de las empresas más grandes de la Argentina y estábamos trabajando en el corazón de su negocio, con lo cual el nivel de exigencia era muy alto. Gracias a mis jefes, aprendí mucho el significado del trabajo en equipo. En momentos críticos, se reunía todo el equipo, no importa cuál era el nivel, con el único objetivo de ir para adelante. Me resultó una experiencia extraordinaria y no me la voy a olvidar más.

Durante más de 20 años de experiencia en IBM, he ocupado cargos de liderazgo como Director de SMB para SSA, Director de Canales para Sudamérica y América Latina, Gerente de Ventas para Argentina, Paraguay y Uruguay y he trabajado también en las áreas de Marketing y el Sector Industrial. Antes de ser CEO, me desempeñaba como Vicepresidente de General Business de IBM Latinoamérica, era responsable por los negocios de una gran parte de los clientes de toda la región. Asimismo, llevé adelante la estrategia de Expansión Geográfica para la región.

2 - Que opinión le merecen las redes sociales desde el punto de vista de la interacción con las empresas tech?

Para nosotros en IBM es muy importante generar un diálogo abierto con los diferentes públicos de la compañía, integrar e incentivar las conversaciones. La calidad, tratamiento, presentación y utilidad del contenido que presentamos nos permite brindar valor agregado en nuestras charlas online. Queremos seguir creciendo en este sentido, mejorar aún más el feedback y afianzar los vínculos establecidos hasta el momento.

Este año desarrollamos Blue Point (www.ibmbluepoint.com) una plataforma abierta y pública donde todos los profesionales de IBM pueden compartir y conversar sobre experiencias, creencias, valores y conocimientos de su trabajo diario en la compañía. Blue Point es una iniciativa de apertura única en la región que busca dar a conocer y transformar en referentes para el mercado a los especialistas de IBM en distintos temas como Mundo Inteligente, Infraestructura, Trabajo Inteligente, Gestión de la Información e Industrias. Está basado en los usuarios de twitter de nuestros empleados.

La comunicación con diferentes actores siempre formó parte de nuestra estrategia. Consideramos que las nuevas tecnologías mejoran las herramientas de interacción y creemos que una estrategia de redes sociales transforma y optimiza la cultura de la compañía. Sobre esta base comenzamos a desarrollar nuestro perfil social.

La información que compartimos refleja los valores, visión y misión de la compañía y está alineada con nuestras estrategias de negocio.

3 - Que perspectivas tiene IBM respecto de los próximos años en materia de desarrollo de tecnología en América Latina.

La estrella del mundo IT continúan siendo los servicios. No solo es el segmento que se lleva la mayor inversión en América Latina sino que representa la principal fuente de ingresos para las compañías. De hecho, para IDC crecerán un 3,9% más rápido que en los mercados desarrollados. Este año arrancó muy bien para la compañía y los resultados superaron todas nuestras expectativas.

Actualmente IBM crece en todos los sectores, con los segmentos de hardware y software avanzando en forma pareja, al igual que sucede con toda la industria.

Los negocios se orientan cada vez más a las soluciones que a los productos lo que también representa una de las tendencias de cambio constante para la industria. Según las proyecciones de IDC, las soluciones de negocios alcanzarán un 8,2% de crecimiento en 2011 y es en ese sentido que las compañías siguen avanzando y adaptándose.

Asimismo, veo en Latinoamérica un fuerte impulso al uso de tecnología para hacer que las ciudades funcionen de manera más inteligente. IBM se encuentra trabajando junto a los gobiernos brindando soluciones relacionadas con seguridad pública, salud, energía y otras áreas donde la tecnología puede jugar un papel clave para mejorar el desarrollo de las ciudades y la experiencia del ciudadano.



4 - Un libro que recomienda? y porque?

Recomiendo "Capitán de Mar y Guerra" de Patrick O'Brian porque está relacionado con uno de mis principales hobbies, la navegación. Además la historia refleja similitudes con la vida diaria en una empresa, sobre las decisiones que debemos tomar y las situaciones que enfrentamos.

5 - Un CEO de IBM tiene pasatiempos que no están relacionados con la tecnología?

Sin dudas: navegación, golf, tenis y fútbol.

6 - Que idea de crecimiento ve IBM a la empresa en América Latina?

Vemos una fuerte oportunidad de crecimiento para las pequeñas y medianas empresas. Y estamos trabajando en conjunto con ellas y con nuestros asociados de negocio para acercarle a este segmento soluciones y servicios especialmente diseñados para ellas.

IBM Argentina está desarrollando una serie de programas relacionados con el crecimiento de las empresas del país, especialmente aquellas ubicadas en las regiones de Cuyo, Centro, Litoral, Patagonia e Interior de Buenos Aires.

La inversión está inmersa dentro de una iniciativa de presencia regional consolidada, con mayor cantidad de recursos asignados y un muy fuerte foco en el desarrollo de canales locales que permitan a las empresas de la región contar con una IBM mucho más cercana.

El foco de IBM Argentina en el interior está relacionado con la contribución a la optimización de los procesos de negocio de las PYMEs, el crecimiento de las economías regionales y la colaboración con asociados de negocio en cada lugar donde la compañía tiene presencia.

7 - Qué opinión le merece las nuevas fuentes de energía? IBM analiza la implementación dentro de sus productos?

Desde IBM buscamos diseñar productos que minimicen el impacto ambiental a través de su ciclo de vida. La reducción, re-utilización y reciclaje continúan siendo el mejor método para contribuir a la sustentabilidad ambiental. Por eso, la empresa trabaja para incrementar cada vez más la eficiencia energética de sus productos. La compañía ha reutilizado y reciclado más de 94% del volumen total procesado de sus productos, reduciendo notablemente desde el año 1995 a hoy el porcentaje de desperdicio llevado a rellenos de seguridad o a incineración. Los datos muestran que en 2008 el ratio de desperdicios fue menor al 1%.

Nuevas tecnologías en disipación de calor y consumo de energía generan menos impacto ecológico. Se procesa más información con menor consumo. Los servidores de IBM consumen hasta un 30% menos de energía que los de la competencia. En 2008, IBM y sus proveedores adquirieron más de 400 toneladas de plástico reciclado para usar en productos IBM, lo cual representa más de 10% de todo el plástico adquirido por IBM.

8 - Cual es la fórmula que ha utilizado IBM para mantenerse vigente tantos años en un mercado tan cambiante?

Si analizamos la historia de IBM en el mundo entendemos claramente que la palabra "progreso" es la que mejor define estos 100 años. IBM se caracteriza por su capacidad para transformarse y adaptarse a las diferentes épocas y coyuntura del mundo moderno. Pasaron tormentas económicas, cambios en el panorama político, desastres naturales y burbujas tecnológicas y la compañía sigue trabajando para hacer que el mundo funcione mejor.

El proceso de transformación de la compañía fue paulatino. IBM se enfocó en promover el cambio en el modelo de negocio y se comprometió a transformar la compañía en una empresa globalmente integrada que incrementó su productividad y participación en los mercados de más alto desarrollo en el mundo. Esto requirió una inversión sustancial y continúa generando un crecimiento significativo.

IBM ha pasado de ser una compañía básicamente dedicada al hardware a transformarse en una organización que brinda servicios de valor agregado a sus clientes a través de la consultoría, los servicios de tecnología, el software y hardware. Esto hace que IBM vaya más allá de las áreas de tecnología de sus clientes, transformándose en un socio estratégico para generar ventajas competitivas en todo tipo de empresas.

Realizamos desinversiones y adquisiciones para liderar el modelo de computación emergente. Hicimos cambios operativos para mejorar nuestra capacidad de integrar para los clientes. Se adquirieron más de 80 compañías para complementar la cartera de productos, particularmente en software de integración y transformación de negocios. En 2002 compramos PriceWaterhouseCoopers y creamos una nueva unidad de consultoría de negocios, así nos convertimos en la Empresa de Servicios de Negocio y IT más grande del mundo. En 2004 vendimos la división de PCs a la empresa Lenovo, ese fue el paso definitivo para salir del negocio de la comoditización para estar en el negocio de la innovación y dar valor agregado a sus clientes.

Todos estos cambios demuestran cómo IBM ha innovado y transformó sus operaciones hacia el mercado de servicios de negocio y tecnológicos. Anticiparnos a las necesidades de nuestros clientes nos permite ser la única empresa a nivel mundial con la capacidad de atender los requerimientos de

todas las empresas, sin importar su tamaño, aportamos valor y generamos una estructura que posibilita el crecimiento cuidando su inversión.

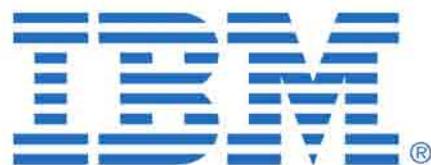
9 - Hacia donde va IBM como proveedora de productos y servicios? cual es la meta a 10 años?

IBM brinda servicios en muchos rubros, siempre de la mano de la tecnología y con el objetivo de ayudar a crear un mundo más inteligente y sustentable. IBM quiere utilizar toda su experiencia para ayudar a la sociedad, a empresas privadas y al sector público a enfrentar sus desafíos actuales y futuros. Creemos que a través de nuestra visión Smarter Planet es posible una nueva forma de encarar el negocio y llevar a un nuevo nivel de inteligencia la forma de trabajo del mundo. Esta estrategia está basada en cuatro pilares: nueva inteligencia, infraestructura dinámica, trabajo inteligente y cuidado del medio ambiente. IBM posee el conocimiento, hardware y software para manejar sistemas más inteligentes que hagan que el mundo sea más inteligente.

10 - Para finalizar que recomendaciones le daría a una empresa si tiene que adquirir tecnología y servicios?

Le recomendaría que busque un socio tecnológico que lo asesore haciendo una evaluación de sus propias necesidades, buscando las soluciones que se adecúen a éstas. Hay una solución a la medida de cada empresa y contar con expertos que asesoren a la hora de tomar decisiones es clave.

Agradecemos a Jorge Goulu por la gentileza.



Dejamos huellas.

Seguínos.

[twitter](#) @elderechoinf



RED IBEROAMERICANA

ELDERECHO Informático.com

LA COMUNIDAD DE DERECHO INFORMÁTICO MÁS GRANDE DE IBEROAMÉRICA