Distintas maneras de atentar contra la vida privada de las personas a través de Internet

Luis Jiménez Guzmán*

Resumen

El uso de las nuevas tecnologías ha favorecido en muchos aspectos la vida del hombre, pero también han significado violaciones a derechos fundamentales como lo es la vida privada. Por lo tanto es importante el conocer los diferentes aspectos del uso de Internet donde nuestra intimidad es vulnerada y la manera en que se le ha legislado en el ámbito nacional e internacional.

The use of new technologies has favored many aspects of human civilization, although it has meant violations to fundamental rights as private life. Therefore, it is important to know the different aspects of the Internet use where our intimacy is damaged and the way in which this issue has been legislated national and internationally.

I. Introducción

Mark Lemley, destacado jurista norteamericano y catedrático de la Universidad de Stanford, California, no se equivocaba al argumentar en su obra *Software and Internet Law* que "la historia de la tecnología es también la historia de la invasión de la vida privada".[1] Y es que efectivamente, con la llegada de nuevos medios de comunicación como Internet, las posibilidades de conocer datos que consideramos personales y de que ellos sean conocidos sin nuestro consentimiento se han multiplicado. Aparte de ser la red una nueva alternativa para violar nuestro derecho a

*Secretario Particular del Magistrado Presidente del Tribunal Superior Agrario y Maestro Adjunto de la Cátedra de Títulos y Operaciones de Crédito en la Facultad de Derecho de la U.N.A.M.

[1] Lemley, Mark, *Software and Internet Law*, Aspen Publishers New York, NY, 2003, p. 111.

la vida íntima, también es una herramienta que permite facilitar métodos tradicionales para hacerlo.

Profundizando en este punto, el español Antonio Pérez Luño señalaba que: "En etapas anteriores el respeto a la vida privada podía realizarse mediante el uso de los sentidos tales como la vista y el oído. Se permanecía así dentro de los límites de las relaciones naturales. Los muros de una casa, la soledad de un lugar desierto, incluso el tono expresivo oral de un susurro, eran suficientes para asegurar la protección de la intimidad y para excluir el conocimiento y la difusión de las acciones y de las palabras de un individuo o de varias personas unidas entre sí por el vínculo de la confidencia. Hoy es posible observar y escuchar a distancia, sin límites de tiempo, de espacio o de modo; se pueden realizar fotografías en la noche, establecer comunicación simultánea de imagen y sonido con distintos lugares gracias a los circuitos televisivos, dejar involuntariamente el testimonio registrado de la propia imagen o de las conversaciones mantenidas e, incluso, se pueden confesar los propios pensamientos sin el uso de la tortura física y casi inadvertidamente".[2] De hecho, nadie puede tener certeza de la identidad de la persona o institución que está al otro lado de la computadora cuando navegamos por la red, y menos conocer sus intenciones.

Por ello, a continuación trataré de hacer una reflexión jurídica, acompañada de una breve descripción tecnológica acerca de los medios que la red ofrece para que se obtengan datos o informaciones propios de la vida privada de las personas. Sin embargo, los casos que se expondrán a continuación no tienen el carácter de taxativos, pero sí son las principales amenazas de nuestro objeto de estudio.

II. La violación al correo electrónico

Dentro de la esfera que comprende la vida privada de las personas, la correspondencia ha sido uno de sus principales componentes, y su inviolabilidad tiene reconocimiento constitucional en muchos ordenamientos jurídicos. Con la llegada de Internet, una nueva alternativa de correspondencia se ha popularizado alrededor del planeta: el llamado correo electrónico, o *email* (*electronic mail*).

Fue inventado en 1972 por Ray Tomlinson, un experto científico en informática que trabajaba para la consultora de ingeniería estadounidense Bolt, Beranek & Newman, que creó un sistema bastante simple por el

[2] Pérez Luño, Antonio, *Dilemas actuales de la protección de la intimidad*. Revista Ius et Praxis Universidad de Lima. Perú, 1992, Nº 21-22. p. 13.

cual se podía enviar un mensaje de una computadora a otra. Pero su uso masivo se disparó con la popularización de los servicios de Internet. En la actualidad se puede afirmar, sin temor a equivocarse, que el uso de la correspondencia digital es uno de los principales motivos a la hora de utilizar la red. Se dice que durante el año 2001, sólo en Estado Unidos más de 135 millones de personas tendrían una cuenta de correo electrónico, y se calcula que circulan diariamente por la red acerca de 500 millones de mensajes enviados (sólo en Norteamérica).[3] Según un reportaje de fecha 15 de mayo de 2006 del diario Reforma mexicano, circularían cerca de 60 mil millones de emails al día, y es un hecho que esta cifra aumenta cada día.[4]

Muchos han confundido al correo electrónico con el correo tradicional, pretendiendo de esta manera aplicar las mismas normas y los mismos principios entre uno y otro. La verdad es que eso es un error, ya que existen esenciales diferencias que hacen que el *email* sea un medio de comunicación con características totalmente particulares.

Cuando uno utiliza el correo tradicional, puede servirse de distintos métodos para darle mayor o menor seguridad a la carta o mensaje que se envía. Si se trata por ejemplo de una postal, uno descuida que se lea lo que ella contiene sabiendo que de por sí no tiene ninguna seguridad que la resguarde. Pero, si se trata de un mensaje que requiere mayor cuidado en cuanto a su contenido, se puede optar por enviarlo a través de un sobre sellado, por carta certificada, por un servicio de correo especial, exigir una entrega personal del mismo, etcétera. Tratándose de mensaje enviados a través del correo electrónico, no existe garantía alguna sobre la no violación de la correspondencia digital, ya que como se verá más adelante, antes que el mensaje llegue a su destino, pasa por distintas etapas en las cuales fácilmente puede revelarse su contenido.

Un correo electrónico puede duplicarse en forma infinita, ya que un mismo mensaje puede por ejemplo mandarse a uno o a varios destinatarios, todo ello en segundos, con la misma calidad y sin costo. Si a través del correo tradicional se quiere mandar un mensaje a varias personas, es necesario reproducirlo materialmente, y realizar la operación por separado para cada destinatario. Ello toma mucho tiempo y dinero. Además, no

[3] Good, Edgar, *An email Education. What You Don't Know About Email Can and Will Hurt You*, International Journal of Communications Law and Policy, Oxford University, U.K. 1999, pág. 12.

[4] El 15 de mayo de 2006, el diario nacional Reforma publicó un artículo titulado "Correo electrónico y abuso". Donde su autor cita la siguiente dato: "Según cifras proporcionadas por el Jefe Ejecutivo de Deutsche Telecom, Kai-Uwe Ricke, cada día son enviados 60 mil millones de correos electrónicos a través de Internet lo que, unido a la sofisticación cada vez mayor de los delitos cometidos por esta vía, significa un gran peligro para todos los usuarios". López, Eduardo, *Correo electrónico y abuso*, Sección Interfase, Diario Reforma, México, 15 de mayo de 2006.

existe garantía alguna respecto de las condiciones en que se va a recibir dicho mensaje.

El *email* es ubicuo, ya que no tiene un destino físicamente determinado, sino que puede ser recogido a través de cualquier computadora que se encuentre conectada a Internet en cualquier parte del mundo. El correo tradicional por su parte requiere de una casilla postal o de una dirección perfectamente determinada para llegar a su destino final.

El correo electrónico funciona a través de una página *web* que provee de este servicio a los usuarios, independientemente donde éstos se encuentren. Está página de acceso permite que el titular de la cuenta ingrese a su correo mediante la combinación de dos elementos: el nombre del usuario (en inglés *login*) y su contraseña (en inglés *password*). Según Giraldo Quintero, "el primero siempre se expresa en el idioma, código o signo identificable y legible; y el segundo se registra en caracteres ilegibles e identificables y es la llave personal con la que cuenta el usuario para impedir que terceros puedan identificarla y acceder a ella".[5] Incluso, la propia página de acceso a la cuenta de correo electrónico ofrece servicios en caso de que la clave de acceso haya sido olvidada. El correo tradicional funciona a través de un servicio postal bastante distinto.

Hechas las distinciones pertinentes, podemos entrar a dar una definición más concreta de correo electrónico, *email* o *electronic mail*: "aplicación mediante al cual un ordenador puede intercambiar un mensaje con otros usuarios de ordenadores (o grupos de usuarios) a través de la red. El correo electrónico es uno de los usos más populares de Internet. Dícese también de los mensajes enviados a través de este medio".[6]

La cuenta de correo electrónico, desde mi punto de vista, debe ser considerada como un dato de carácter personal y tener la protección de los datos considerados como tales, en los países donde este legislado. Esta protección ya ha sido reconocida, como lo señala Paloma Llaneza González, por el Consejo Europeo, que afirma que "la dirección de correo electrónico es un dato personal".[7] Esto confirma que la cuenta de correo electrónico y su contenido forman parte de la esfera íntima de las personas y, por consiguiente, merece la protección que se le ha reconocido y que se debe de reconocer en nuestro país.

---

[5] Giraldo Quintero, Argiro, *El Secreto en la Comunicación por Correo Electrónico*, Revista Electrónica de Derecho Informático, Número 025, agosto del 2000, http://www.alfa-redi.org/rdi-articulo.shtml?x=539 Consultada el 21 de octubre de 2007.

[6] Fernández Calvo, Rafael, *Glosario básico inglés-español para usuarios de Internet*, Asociación de Técnicos de Informática, http://www.ati.es/novatica/glosario/glosario_internet.html Consultada el 21 de octubre de 2007.

[7] Llaneza González, Paloma, *Internet y Comunicaciones Digitales*, Editorial Bosch, Barcelona, España 2000, pág. 271.

La intercepción de correos electrónicos es bastante más común de lo que los usuarios se imaginan. Ello se debe en gran medida al funcionamiento del sistema, que en muchos casos obliga a quienes lo prestan a cometer ente ilícito procurando que no pase como tal. Entidades que prestan el servicio de correo electrónico como *Hotmail* o *Yahoo*![8] reconocen que debe existir secreto en cuanto al contenido y uso que cada persona haga de su cuenta de correspondencia digital. Asimismo, cuando los usuarios contratan este servicio, se someten a un contrato de adhesión en el cual se determina como territorio jurisdiccional aquél en el cual se encuentra establecida la dirección comercial de la página *web*. Estos proveedores del servicio de correo electrónico generalmente justifican una intervención en la cuenta de los usuarios cuando se trata de cumplir con procedimientos legales o velar por el adecuado funcionamiento del sistema. Las palabras del norteamericano Barry Fraser ilustran estos de la siguiente manera: "Su mensaje electrónico puede ser manejado por muchos servicios digitales durante su envío. El operador de sistema de cada uno de esos sistemas puede ver el contenido del mensaje bajo alguna de las excepciones consagradas en el ECPA.[9] Adicionalmente, el mensaje puede ser interceptado si el remitente o el destinatario del mensaje consienten. En consecuencia, incluso si usted no ha consentido a tal intercepción o acceso, la persona a quien se envió el mensaje puede haber consentido a tales actividades".[10] Profundizando en las consecuencias de lo que esto puede traer, muchos han puesto en tela se duda las políticas que estos servidores ofrecen a sus usuarios, ya que muchas veces los intereses económicos pueden más que la protección de intereses legítimos.[11]

[8] Según lo señala el colombiano GERARLDO QUENTERO, Argiro "Hotmail empresa del potentado Microsoft consagra el secreto a la comunicación por correo electrónico así. "Es política de Microsoft respetar la privacidad de sus usuarios. Microsoft no supervisará, modificará o divulgará ninguna información de carácter personal acerca de usted o del uso que usted haga del Servicio. Incluidos sus contenidos, sin su previo consentimiento, a menos que Microsoft considere de buena fe que dicha actuación es necesaria para 1) cumplir las CDS, o 4) actuar para proteger los intereses de sus usuarios o terceros…". Yahoo! Igualmente expresa una política de privacidad así: "el usuario reconoce y acepta que Yahoo! No examinará lo contenidos con anterioridad a su puesta en disposición o transmisión, pero éste y sus representantes estarán facultados (pero no obligados) a rechazar o desplazar cualquier contenido que esté disponible en el Servicio. Sin perjuicio de lo anterior, Yahoo! Y sus representantes estarán plenamente facultados para suprimir cualquier Contenido que vulnere las Condiciones o que de algún modo sea inaceptable" *El Secreto en la Comunicación por Correo Electrónico*, Revista Electrónica de Derecho Informático, Número 025, agosto del 2000, http://www.alfa-redi.org/rdi-articulo.shtml?x=539 Consultada el 21 de octubre de 2007.

[9] *Electronic Comunications Privacy Act* de 1986.

[10] FRASER, Barry, *Rules of the Road Navigating the Information Superhighway*, Human Rights Magazine, Volume 26, No 1, 1999. http://www.abanet.org/irr/hr/winter99_fraser.html Consultada el día 21 de octubre de 2007.

[11] Al respecto, Pomeroy, Jeremy en *Online Anonymity can be Ilusory Under Current Law, ISP Policies* Multimedia & Web Strategist, Sept. 1998, pág.6, señalaba que "En cualquier caso, la protec-

Aparte de esto, la correspondencia digital también se ve amenazada por los llamados *hackers*, quienes a su vez buscan destruir los sistemas de seguridad que los proveedores del servicio tienen, para de esta manera poder acceder a las cuentas de correo de sus miembros. Esta práctica también es muy común alrededor del ciberespacio y su control no ha dado los suficientes frutos.[12]

Estamos concientes de que el uso de correos electrónicos personales por terceros es también una práctica muy común y de la que seguramente a lo mejor los afectados nunca se llegan a enterar. Por supuesto que las consecuencias de ello también afectan la vida privada de los dueños de las casillas electrónicas.

Muchas propuestas en torno a cómo afrontar este problema han surgido por todo el mundo y de todos los tipos. Hay quienes ven una solución en la creación de un "organismo multinacional",[13] otros creen que la solución está en manos de los proveedores del servicio de Internet, más precisamente los operadores del sistema a cargo de manejo. Están los que creen que la solución es crear un sistema que torne imposible la identificación de la persona que envía los mensajes, con la obvia excepción del destinatario.[14]

---

ción ofrecida por los proveedores de Internet mediante sus "Políticas de privacidad", es típicamente sujeta a cambios. Los proveedores se reservan tradicionalmente el derecho de revisar y transforma los términos de dichas políticas sin previo aviso a los usuarios. En consecuencia, un usuario que confíe en un determinado nivel de protección conferido de acuerdo a una política de privacidad determinada, puede encontrarse de repente con que los detalles íntimos que, voluntaria o involuntariamente reveló a su proveedor, han sido puestos a disposición de terceras parte"

[12] En nota publicada por CNN online, se relata que el 24 de agosto de 1999 un cambio en la configuración del sistema dejó vulnerables los buzones de la totalidad de usuarios. *Hackers* descubrieron la falla, crearon un programa que permitía libre acceso a cuentas *Hotmail* y lo pusieron en libre uso en el Internet. Hasta el 30 de agosto, fecha en que el problema en el sistema fue corregido el único control posible fue la obstrucción de sitios que en todo el mundo aparecían con el script que permitía el acceso no autorizado. *New Hotmail breach reported*, 14 de septiembre de 1999, http://www.cnn.com/TECH/computing/9909/14/hotmail/index.html Consultada el 21 de octubre de 2007.

[13] Geraldo Quintero, Argino ha dicho que "La creación de un organismo multinacional, llámese gobierno ciber o organización internacional de regulación cibernética es necesaria para garantizar a todos los ciudadanos del mundo el secreto de sus comunicaciones por la red y los derechos a la intimidad, El desarrollo incalculable del servicio de Internet va unido el del correo electrónico, en 1999 solo Hotmail tenía 40 millones de usuarios, es pues urgente llamar la atención sobre unas regulaciones globales que permitan eficazmente garantizar los derechos fundamentales del hombre la tecnología y el temor de los estados a ser vulnerable por la criminalidad globalizada no puede acabar con las conquistas humanas en materia de derechos fundamentales." *El Secreto en la Comunicación por Correo Electrónico*, Revista de Derecho Informático, Número 025, agosto del 2000, http://www.alfaredi.org/rdi-articulo.shtml?x=539 Consultada el 21 de octubre de 2007.

[14] Barrera María Helena, se refiere a los inconvenientes de esta solución en el sentido de que: "Los problemas que conlleve esta solución son duales: En primer lugar anomimidad no puede ser sinónimo de privacidad, desde un punto de vista legal. Anonimidad es solo una de las posibilidades

Otros, como la prestigiada abogada ecuatoriana María Helena Barrera, creen que en la creación de un sistema de seguridad criptográfico está la solución más viable. Comparto esta postura, aunque sin embargo, al ser el correo electrónico una de las posibilidades de correspondencia más usadas del mundo, la existencia de una solución que combine armoniosamente aspectos técnicos y jurídicos se vuelve relevante, sobre todo en un mundo en que ya todos admiten que el ciberespacio no ofrece ninguna garantía segura y confiable en el ámbito de la correspondencia digital.

III. El correo no deseado

Antes de la llegada de Internet, el uso del teléfono y del fax en oficinas y lugares comerciales era vital a la hora de comunicarse con los demás. Durante los años en que este medio de comunicación tuvo su auge, surgieron quienes se dedicaban a enviar diariamente publicidad a través del fax, o quienes a través de grabadoras llamaban por teléfono promocionando algún producto. Esto seguramente le hizo pasar más de un mal rato a quien, por causa de esta publicidad no deseada, perdía tinta de su fax, tiempo y dinero. En países como Estados Unidos, este problema fue combatido a través de la promulgación de normas como la TCPA o Telephone Consumer Protection Act de 1991, que regularía la llamada publicidad no deseada a través del fax y del teléfono.[15]

Con el desarrollo y uso masivo del correo electrónico en el mundo, muchos también vieron en esta manera de comunicarse con las personas una excelente vía a la hora de hacer publicidad. De esta manera, es común entre quienes tienen una cuenta de correo electrónico recibir con muchísima frecuencia correo no solicitados o "correo basura" (junk mail).

Se ha clasificado al correo electrónico no deseado en *spam* o *junk mail* según si tiene o no intenciones comerciales. Es así que se define al *junk mail* como el "correo basura que, por lo general. No tiene carácter

que la privacidad brinda, uno de los componentes de un derecho mucho más vasto y global. En segundo legal, anonimidad puede ser destruida en cualquier momento, por regeneración legítima o ilegítima de la traza que conecta (incluso en los mejores instrumentos), el mensaje con su creador". *Correspondencia Digital: Recreando Privacidad en el Ciberespacio*, Revista de Derecho Informático, No.015, octubre de 1999, http://www.alfa-redi.org/rdi-articulo.shtml?x=345 Consultada el 21 de octubre de 2007.

[15] Ver, más sobre la Telephone Consumer Protection Act en texto de LEÓN LEÓN, Carlos Alfredo en *Consideraciones Legales Relativas al Envío de emails. Comerciales No Solicitados*, dicho texto publicado en Revista de Derecho Informático, Número 036, julio de 2001, http://www.alfa-redi.org/rdi-articulo.shtml?x=730 Consultada el 21 de octubre de 2007.

comercial y que suele provenir de direcciones no anónimas. Los casos más frecuentes son las pesadísimas cartas cadena (*chain letter*) sobre la buena o mala suerte, virus informáticos inexistentes, niños gravemente enfermos que desean recibir correos electrónicos de todos los confines de la tierra".[16] Desde un punto de vista más general, otros, lo han definido de la siguiente manera: "correo basura que por lo general no tiene carácter comercial, pero si es una "baratija" (la traducción literal de *junk* es baratija), es decir son mensajes que llenan el buzón incomodándolo."[17]

Cuando en el año 2000 escribí sobre el *junk mail* en específico señale: "¿de qué modo estos mensajes afectan la intimidad personal? ¿La vulneran o la violentan? Es claro que para poder recibir estos mensajes uno tiene que ser parte de una lista de direcciones electrónicas que aparecen en el header (cabecera) del mensaje. En los casos de usuarios más avanzados que utilizan estas herramientas, procuran colocar a los usuarios en bcc (*blind carbon copy*) de modo tal que no aparecen todas las direcciones a las cuales se ha enviado dicho "*junk mail*", mas esto es considerado una falta a las *nettiquets* y además una violación clara del espacio de la intimidad, pues en la mayoría de los casos estos mensajes no tienen más función que "llenar el buzón de correo".[18] De esto puedo obtener la diferencia clara entre *spam* y *junk*, el primero tiene fines comerciales y el segundo no necesariamente tienen que serlo, ya que pueden ser correos con bromas, chain *letters* o *hoax*,[19] pero a final de cuentas violentan nuestro espacio de privacidad.

El llamado *spam* o bombardeo publicitario se define tradicionalmente como "los mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas. Aunque se puede hacer por distintas

[16] Llaneza González , Paloma, *Internet y Comunicaciones Digitales*, Editorial Bosch, Barcelona, España, pág. 271

[17] Ferreyra, Gonzalo C, *Internet paso a paso: Hacia la autopista de la información*, Grupo Editor Alfaomega, México, 1996, pág. 35.

[18] Jiménez Guzmán, Luis, *Hacia una regulación del comercio electrónico en México*, Tesis Profesional, México, 1999, pág. 161.

[19] Un *hoax* (del inglés: engaño, burla) es un intento de hacer creer a un grupo de personas que algo falso es real. En el idioma español el término se popularizó principalmente al referirse a engaños masivos por medios electrónicos especialmente Internet. A diferencia del fraude el cual tiene usualmente una o unas cuantas víctimas y es cometido con propósitos delictivos y de lucro ilícito, el hoax tiene como objetivo el ser divulgado de manera masiva haciendo uso de los medios de comunicación, siendo el más popular de ellos en la actualidad Internet y no suelen tener fines lucrativos o no son su fin primario. Las personas que crean hoaxes tienen diversas motivaciones dentro de las que se encuentran el satisfacer la vanidad personal, la intención de hacer una broma para avergonzar o señalar a alguien o la pretensión de provocar un cambio social haciendo que la gente se sienta prevenida frente a algo o alguien, también suele ser característico dentro de los autores de hoax el querer mofarse y hacer evidente la credulidad de las personas y de los medios de comunicación. *Wikipedia*. La enciclopedia libre, http://es.wikipedia.org/wiki/Hoax . Consultada el 21 de octubre de 2007.

vías, la más utilizada entre el público en general es la basada en el correo electrónico".[20] Se trataría en este caso de publicidad que tiene intenciones comerciales. Según un estudio del *New York Times* 9 de cada 10 mensajes que se mandan a través de Internet constituyen correos electrónicos no deseados.[21]

La doctrina ha considerado que el correo electrónico no deseado produce dos efectos: el primero es que se incurre en un gran costo que tiene que ser afrontado tanto por el dueño de la cuenta de correo como por quien provee de acceso a Internet; y el segundo es que se trata de una manera más de atentar contra la esfera privada de las personas a través de este medio.

Se dice que la Comisión Europea ha calculado que unos 500 millones de "*spams*" se envían diariamente, y que ello representa una pérdida mundial de cerca de 9.300 millones de dólares al año.[22] Esto se traduciría por ejemplo en el tiempo en que uno se demora en leer y eliminar estos correos. Desde otra perspectiva, muchas páginas *web* que prestan el ser-

[20] Esta definición es la obtenida en *Wikipedia. La enciclopedia libre*, dentro de esta voz, encontramos un interesánte dato sobre el origen de la palabra *spam*: "Tiene raíces estadounidenses con unas curiosas derivaciones socio-culturales: La empresa chacinera estadounidense *Hormel Foods* lanzó en 1937 una carne en lata originalmente llamada *Hormel's Spiced Ham*. El gran éxito del invento lo convirtió con el tiempo en una marca genérica, tan conocida que hasta el mismo fabricante le recortó el nombre, dejándolo con solo cuatro letras: *Spam*. El *Spam* alimentó a los soldados soviéticos y británicos en la Segunda Guerra Mundial, y desde 1957 fue comercializado en todo el mundo. En los años 60 se hizo aun más popular gracias a su innovadora anilla de apertura automática, que ahorraba al consumidor el uso del abrelatas. Fue entonces cuando los *Monty Python* (grupo de comediantes ingleses) empezaron a hacer burla de la carne en lata. Su divertidísima costumbre de gritar la palabra spam en diversos tonos y volúmenes se trasladó metafóricamente al correo electrónico no solicitado, que perturba la comunicación normal en internet. En un famoso *sketch* de 1970 (*Flying Circus*) los comediantes británicos representaban a un grupo de hambrientos vikingos atendidos por solícitas camareras que les ofrecían "huevo y panceta; huevo, salchichas y panceta; huevo y *spam*; huevo, panceta, salchichas y *spam*; *spam*, panceta, salchichas y *spam*; *spam*, huevo, *spam*, *spam*, panceta y spam; salchichas, spam, spam, panceta, spam, tomate y *spam*, ...". La escena acababa con los vikingos cantando a coro "*Spam*, *spam*, *spam*, *spam*. ¡Rico spam! ¡Maravilloso *spam*! *Spam*, *spa-a-a-a-a-am, spa-a-a-a-a-a-am, spam*. ¡Rico spam! ¡Rico spam! ¡Rico spam! ¡Rico spam! ¡Rico *spam*! *Spam, spam, spam, spam*". Como la canción, el spam es una repetición sin fin de texto de muy poco valor o ninguno, que aplicado a los mensajes electrónicos, se refiere a los mensajes enviados de forma masiva y dirigidos a personas que, en principio, no desean recibirlos. http://es.wikipedia.org/wiki/Spam Consultada el 21 de octubre de 2007.

[21] Stone, Brad, *Spam Doubles, Finding New Ways to Deliver Itself* Según traducción textual: "En los últimos seis meses, el problema ha empeorado radicalmente. La cantidad de spam generado en todo el mundo se ha doblado desde el último año, de acuerdo con *Ironport*, una firma dedicada al filtrado de *spam*, y el correo basura alcanza ahora una proporción de 9 de cada 10 mensajes de email mandados por Internet" *New York Times*, 6 de diciembre de 2006.

[22] Citado por Roberto Sobrino, Waldo Augusto, *Las "Cookies" y el "Spam" (y la violación de la "Privacidad" y la "Intimidad")*.Revista de Derecho Informático No.035 de junio de 2001, http://www.alfa-redi.org/rdi-articulo.shtml?x=710 Consultado el 21 de octubre de 2007.

vicio de correo electrónico permiten que nuestras casillas ocupen una cierta cantidad de espacio. Por consiguiente, si nos vemos bombardeados de estos mensajes no deseados, se borrarán otras comunicaciones que sí pueden ser importantes para el usuario. Todo ello, a la larga trae pérdidas calculables en dinero, generando responsabilidades extracontractuales.

Pero el tema que realmente nos interesa es el enfoque que debe dársele a este correo como atentatorio de nuestro derecho a la vida privada. Como se señalaba anteriormente, la casilla de correo forma parte de nuestra esfera íntima, y por consiguiente el acceso a ella y el uso que los demás pretendan otorgarle no tiene el carácter de libre y debe respetarse. A más del hecho de que los usuarios que tienen casilla electrónica se ven abrumados alevosamente de información que un dato personal, ha sido revelado sin su conocimiento.

En efecto, generalmente los correos no solicitados son enviados a una serie de personas al mismo tiempo, y ello responde al hecho de que, detrás de estos mensajes, existe una base de datos que contiene información de cada una de las personas que reciben esta correspondencia. Es casi seguro que aquella base de datos no cumpla con los requisitos que establecen leyes europeas, latinoamericanas o norteamericanas y por consiguiente se trate de bases de datos ilegales, obtenidas a través de métodos ilícitos y utilizados para fines contrarios a la ley. De todo ello se desprende que los correos no solicitados son ilegales y atentan contra nuestro derecho a no ser molestados, a que se respete aquella parte de nuestras vidas considerada como íntima.

En los Estados Unidos, este problema ya ha tenido que ser afrontado por los tribunales. Como lo señala Waldo Augusto Roberto Sobrino, "Entre las primeras Sentencias referentes a la cuestión del *spam*, es menester recordar *Cyber Promotions Inc, vs. América Online Inc.* y *América Online Inc. Vs Cyber Promotions Inc.*, tramitada en la Corte de Pennsylvania, el 4 de Noviembre de 1996, donde entre varias interesantes cuestiones, la empresa acusada de "spam", basada su defensa en al "Primera Enmienda" (*freedom speech rights*), e incluso se analizó la legalidad de *America Online* de enviar *email bombs*".[23] Como consecuencia de ello, se originó en el Congreso Norteamericano un proyecto de ley, la *Unsolicited Electronic Mail Act* del 2000 (H.R. 3113), durante esa legislatura (la 106) existieron 11 proyectos para regular el *spam*, de la legislatura 107 a la 109 existieron 20 proyectos de los cuales sólo uno fue aprobado.[24] La iniciativa en comen-

[23] *Ibidem*, refiriéndose a información obtenida en *Electronic Commerce & Law Report*, de fecha 1 de Diciembre de 1997.

[24] Información abundante sobre estos proyectos se encuentra en la página de *Spam Laws*, en www.spamlaws.com

to señala que: "Este proyecto establece que en un email comercial no solicitado que se encuentre marcado o rotulado como tal, se deben incluir en el mismo procedimientos para solicitar el retiro de las listas de distribución. Prohíbe asimismo que estos mensajes sean enviados utilizando las facilidades de proveedores (ISP) que hayan señalado expresamente que la prohibición de enviar estos mails utilizando sus servicios".[25] Cabe señalar que en el 2003 se aprobó por el Congreso Norteamericano la *Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003*', también conocida como CAN-SPAM *Act of 2003*[26] y más recientemente el 22 de diciembre de 2006 la *US Safe Web Act of 2006*.[27] Sin embargo, la promulgación de cualquier norma referente a Internet debe considerar el problema de la aterritorialidad de la red, ya que como veíamos anteriormente, la aplicación de una ley tiene cabida en un territorio jurisdiccional determinado, y en Internet el espacio físico no existe.

Muchos vieron una solución a través de los sistemas *Opt-in y Opt-out*. Mediante el primero, se establece que quien desee recibir algún tipo de correo electrónico no solicitado debe manifestarlo a través de su inscripción en una lista, vale decir, tiene que prestar su consentimiento para ello. El segundo sistema por su parte establece que es legítimo enviar este tipo de mensajes, salvo que el destinatario de éstos manifieste lo contrario. Dentro de estas dos posibilidades, el sistema *Opt-in* ha tenido mayor aceptación tanto en Estados Unidos (que lo adoptó en al *Telephone Consumer Protection Act*) como en Europa.[28] Al decir de Pedro Alberto de

[25] La información sobre este proyecto fue obtenida en la Librería del Congreso Norteamericano, *The Library of Congress. Thomas*, http://thomas.loc.gov/cgi-bin/query/z?c106:H.R.3113: Consultada el 21 de octubre de 2007.

[26] Para mayor información ver FILHO, Democrito. R, *Short commentaries on the CAN-SPAM Act*, Revista de Derecho Informático, No. 70, mayo del 2004, http://www.alfa-redi.org/rdi-articulo.shtml?x=1093 Consultada el 21 de octubre de 2007.

[27] Busca proteger a los consumidores frente al correo basura, el software espía y el fraude a través de Internet, permitiendo a la Comisión Federal de Comercio compartir información e investigar conjuntamente con sus interlocutores en otros países. La nueva Ley autoriza a la Comisión Federal de Comercio a proporcionar ayuda para la investigación a instituciones extranjeras que sean competentes para reprimir prácticas comerciales fraudulentas o engañosas, incluyendo la posibilidad de intercambiar temporalmente personal para colaborar en tales actuaciones. A estos efectos, la Comisión podrá negociar con sus contrapartes de otros países los acuerdos que formalicen la provisión de ayuda, materiales o información.

[28] Para apuntalar el comentario es importante señalar que el día 7 de diciembre de 2001, se publicó la siguiente noticia en el sitio de Internet Vlex en su sección Actualidad: *Los quince adoptan la opción opt-in dentro de la propuesta de la Directiva sobre el spam*, "El Consejo de Ministros de Telecomunicaciones de la UE ha aprobado la propuesta de Directiva sobre regulación del correo comercial no deseado (spam), optando por la opción '*optin*', que obligará a las empresas a obtener la autorización previa expresa del internauta para poder enviarle este tipo de correos electrónicos. La reunión de los encargados en materia de Telecomunicaciones en los Quince sirvió, además para la presentación por la Comisión del Séptimo Informe sobre la Implementación del paquete Legislativo sobre Telecomunicaciones, para la adaptación por parte de los representantes de los estados miem-

Miguel Ascencio,[29] el debate en la Unión Europea entre un régimen de listas de inclusión o de exclusión fue resuelto por el artículo 13 de la Directiva 2002/58/CE, sobre la privacidad y las comunicaciones electrónicas, que entendió con ciertas matizaciones a los mensajes de correo electrónico el restrictivo régimen previsto para el fax y los sistemas automáticos de llamada. El concepto de correo electrónico que no requiere la participación simultánea del remitente y del destinatario, como es el caso entre otros, de los mensajes SMS, MMS y de los mensajes dejados en contestadores automáticos. Obviamente que los partidarios del otro sistema, como las empresas de marketing, defenderán su derecho a hacer publicidad por este medio.

Otra solución presentada por los expertos en el sistema es la inclusión de filtros en los servidores, por medio de los cuales se detectaría y se imposibilitaría el ingreso de correos no solicitado. Se pretende que por medio de estos filtros, se detecte a estos mensajes que son enviados a través de ciertas palabras o expresiones, o de alguna dirección identificable. Sin embargo, aún cuando la solución puede ser buena, se debe considerar la posibilidad de que quienes envían esta correspondencia tratarán de "disfrazar" estos mensajes, de tal manera que no sean detectados por estos filtros y puedan llegar a su destino. Hay quienes creen que la autorregulación todavía puede ser una alternativa, pero son los que menos, ya que está demostrado que en un mundo donde los intereses valen más que la buena fe, este tipo de soluciones se vuelven un tanto utópicas.

La situación en nuestro país al decir de la doctrina existente,[30] es la de contar con un sistema de listas de exclusión (*opt-out*) según lo señala el artículo 18 de la Ley Federal de Protección al Consumidor, que se refiere a que la Procuraduría Federal de Protección al Consumidor pueda llevar un registro público que será gratuito, de consumidores que no deseen que su información sea utilizada con fines publicitarios, quienes podrían comunicar a la PROFECO su solicitud de inscripción en este registro, ade-

bros de la propuesta de Directiva de la Comisión sobre regulación del denominado '*spam*'. Finalmente, los Quince han optado por la opción '*optin*' por la que las empresas que deseen remitir correos comerciales a internautas deberán contar con el consentimiento expreso previo de los destinatarios, con la excepción de que ya exista una relación contractual comercial entre ambas partes. Los ministros europeos también han aprobado el refuerzo de la protección del ciudadano en la Red a través de la introducción de ciertas condiciones para el uso de las denominadas 'cookies', de forma que los internautas tengan la opción de rechazar el uso de las mismas en sus conexiones a la Red." http://premium.vlex.com/actualidad/Actualidad-vLex/Los-Quince-adoptan-opcion-%27opt-in%27-dentro-propuesta-Directiva-%27spam%27/2100-118803,busqueda_3613951,01.html Consultada el 21 de octubre de 2007.

[29] De Miguel Asencio Pedro Alberto, *Derecho del Comercio Electrónico*, Editorial Porrúa, México, 2005, p. 213.

[30] Ver a Ramírez Chelala, Yesín y Vera Prendes, Luis o a De Miguel Asencio, Pedro Alberto.

más el artículo 18 *bis* del mismo ordenamiento prohíbe a los proveedores y empresas el envió de publicidad a los consumidores que expresamente les hayan manifestado su voluntad de no recibirla o que estén inscritos en el registro del artículo 18. Cabe destacar que antes de la reforma de 2004 se fijó la precisión de los artículos mencionados ya que con anterioridad sólo contaba con el artículo 76 *bis* cuya fracción VI se limita a establecer que el proveedor debe respetar la decisión del consumidor de no recibir avisos comerciales, pero sin incluir reglas específicas sobre el envío de mensajes de correo electrónico ni disposiciones sobre la puesta a disposición de los consumidores de vías para manifestar su oposición a la recepción de esos envíos. Así con la reforma el artículo 17 quedó como sigue:

> ARTÍCULO 17.- En la publicidad que se envíe a los consumidores se deberá indicar el nombre, domicilio, teléfono y, en su defecto, la dirección electrónica del proveedor; de la empresa que, en su caso, envíe la publicidad a nombre del proveedor, y de la Procuraduría.
> *Párrafo reformado DOF 04-02-2004*
> El consumidor podrá exigir directamente a proveedores específicos y a empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios, no ser molestado en su domicilio, lugar de trabajo, dirección electrónica o por cualquier otro medio, para ofrecerle bienes, productos o servicios, y que no le envíen publicidad. Asimismo, el consumidor podrá exigir en todo momento a proveedores y a empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios, que la información relativa a él mismo no sea cedida o transmitida a terceros, salvo que dicha cesión o transmisión sea determinada por una autoridad judicial.
> *Párrafo adicionado DOF 04-02-2004*

Se transcribe el numeral porque es importante señalar que se habla por primera vez en una legislación nacional de la dirección electrónica de un proveedor y el segundo párrafo señala que el consumidor puede exigir no ser molestado en su dirección electrónica para que les ofrezcan bienes de consumo, afirmando así la exclusión.

IV. Las cookies o galletas

Se definen tradicionalmente como cookie (espía, cukie, caqui, fisgón, galleta) a “los ficheros de datos guardados en un directorio específico del ordenador del usuario”. Se crean por los servidores web con el objeto de ser enviados a los programas navegadores del usuario, y así recoger la información de que dicho fichero ha reunido. Por lo tanto son considerados

como datos personales".[31] Otros han preferido definirlas como "un fragmento de información que se almacena en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página. Esta información puede ser luego recuperada por el servidor en posteriores visitas. Las inventó Lou Montulli, un antiguo empleado de *Netscape Communications*. Al ser el protocolo HTTP incapaz de mantener información por sí mismo, para que se pueda conservar información entre una página vista y otra (como *login* de usuario, preferencias de colores, etc), ésta debe ser almacenada, ya sea en la URL de la página, en el propio servidor, o en una *cookie* en el ordenador del visitante."[32]

Para empezar, lo que se deja el disco duro del usuario es un inofensivo fichero de texto (con extensión ".txt") y no fichero ejecutable (".exe", ".com", ".com", ".bat" etc.), por lo que no existe posibilidad alguna de que una "*cookie*" sea en realidad un virus informático.

- Las "*cookies*" no pueden "ver" ningún dato del disco duro del usuario, ni puede determinar la dirección de *e-mail* o la identidad del usuario los facilitan de una manera voluntaria.
- Un sitio web sólo puede recoger las "*cookies*" que dejó el mismo, es decir, no puede recoger las "cookies" provenientes de otros sitios."[33]
- Para su aplicación, muchos servidores utilizan el sistema *Opt-in*, es decir la instalación de las *cookies*. Sin embargo, no siempre esta política ha sido respetada.

Como señalaba la definición de Wikipedia, fue creado por la empresa Netscape en 1995 para uso de la versión 2.0 de su navegador. Tiene como función original el hacer que se recuerde y reconozca a un usuario cada vez que ingrese a una página web. Ello en teoría buscaba también que la navegación por Internet sea más personal y conveniente. En realidad se trata de una información valiosa, producto de las huellas que dejan los usuarios durante su navegación, creando un perfil exacto y minucioso respecto de las preferencias de éstos dentro de la red, sus hábitos de consumo, el tiempo destinado a navegar, sus intereses comerciales, sus posibilidades económicas, entre otros aspectos, esto es posible ya que cada

[31] Definición propia. *Hacia una regulación del comercio electrónico en México*, Tesis profesional, México 1999, pág.157

[32] Definición de *Wikipedia. La enciclopedia libre*. Mas información sobre el tema en: http://es.wikipedia.org/wiki/Cookie Consultada el 21 de octubre de 2007.

[33] S Elias, Miguel, *Situación Legal de los Datos de Carácter Personal frente a las Nuevas Tecnologías*, Revista de Derecho Informático, No. 032, marzo de 2001, http://www.alfa-redi.org/rdi-articulo.shtml?x=638 Consultada el 21 de octubre de 2007.

usuario que visita una página web deja un rastro o número IP (*Internet Protocol*), que es lo que permite identificar los pasos que éste efectuó mientras navegaba, y las *cookies* por sí solas no pueden identificar a quien navega en la red, a través de la lectura de su IP esto se vuelve posible. Puede demostrarse de esta manera su ilegalidad ya que se atenta contra un derecho fundamental de las personas, cual es su vida privada, que se ve desnudada con los datos de carácter personal que este sistema arbitrariamente transmite. Aún cuando existen mecanismos para desactivar la lectura y escritura de las *cookies*, la posibilidad de habilitarlas sin nuestro consentimiento no es tarea difícil.

Esta información de carácter personal constituye un bien extremadamente cotizado por empresas que se dedican al marketing directo, ya que se trata de bases de datos que revelan las preferencias de los usuarios en la red. Un ejemplo que ilustra perfectamente la amenaza que representa este sistema fue el estudio que hizo la *Federal Trade Comisión* (FTC) por encargo del aquel entonces vicepresidente de Estados Unidos, Al Gore en 1998. De ello se desprendieron los siguientes resultados: de 1400 *websites* comerciales visitados, un 85% recogía y almacenaban datos personales de los visitantes. Sólo un 14% daban algunas indicaciones acerca de intimidad de la información recogida y sólo un 2% ofrecía una política a favor de los usuarios con sentido.[34]

En los Estados Unidos existen ya demandas al respecto, y uno de los casos más sonados es el de la empresa *Double Click Company* que tiene como razón social el diseñar estrategias de marketing por Internet a través del estudio del comportamiento de los usuarios mientras navegan. Esta empresa posee cerca de 1.500 sitios de Internet afiliados en todo el mundo, desde los cuales se monitorea a los navegantes. De ello se desprenden, mediante el uso de *cookies*, verdaderos perfiles de los usuarios. Se crean así bases de datos obtenidas sin el consentimiento de quienes las forman, y que son muy cotizadas en el mercado. Ello condujo a que en el año 2001, el Centro de Información sobre Privacidad Electrónica denuncie públicamente a esta empresa sobre estas prácticas ilegales. Los demandados se defendieron argumentando que "la promoción es un servicio a todos los consumidores", que "usan las *cookies* únicamente para asegurar que un usuario no vea el mismo aviso demasiada veces" y que "esta metodología cuestionada les permite suministrar a sus empresas afiliadas, información precisa para que luego estas sugieren correctamente ciertos productos a los clientes". Este caso fue planteado ante la *Federal*

[34] Información en Cascuberta, David, *La privacidad en los nuevos medios electrónicos. Aspectos éticos y sociales*, Revista de Derecho Informático. No. 011, junio de 1999, http://www.alfa-redi.org/rdi-articulo.shtml?x=276

Trade Comisión que fue resuelto por la Suprema Corte de los Estados Unidos favorable a *Doubleclick*,[35] así la jurisprudencia norteamericana determinó que el uso de *cookies* con fines de publicidad no viola la privacidad ni las normas sobre comunicaciones electrónicas (ECPA), a pesar de lo que la doctrina ha sostenido. Pero en un nuevo litigio contra *Pharmatrack*[36] la Corte revirtió su criterio y determinó que si es ilegal y va en contra de la ECPA el uso de *cookies* con fines de publicidad y recolección de datos apegándose así a lo dicho en la doctrina.

Consideremos el caso de que se vendiera esta información o se analizara de forma incorrecta, ya que podría causar serios problemas. Debido al incalculable alcance de este tipo de empresas y a la difusión que haga de nuestros datos a sus "clientes" se podrían dar hechos inimaginables como el ser rechazados en nuestro trabajo por haber visitado una página *web* que aboga por la legalización del aborto, o ser vigilados minuciosamente después de hojear información "en línea" acerca de cómo fabricar bombas caseras, o tener que pagar más nuestro seguro después de visitar un sitio con información para pacientes con SIDA.[37]

En la actualidad, hay quienes creen que las cookies pueden convertirse en un mecanismo que no atenta contra el derecho a la vida de las personas a través de un sistema como el del *Opt-in*, y que se ajuste a las exigencias de los ordenamientos jurídicos. Sin embargo, aún cuando exista una aparente buena fe por parte de quienes proponen este sistema, se ha demostrado ya que las llamadas galletitas pueden ser colocadas sin que el usuarios se percate, y ello debe considerarse en la actualidad donde la tecnología ha podido más que las buenas intenciones.

[35] In re *Doubleclick Inc. Privacy litigation, 2001 U.S. Dist. LEXIS 3498* (2001). Este criterio fue revertido por un reciente fallo en el caso "Pharmatrack". Consultado el 21 de octubre de 2007.

[36] In Re *Pharmatrak, Inc. Privacy Litigation*, 329 F 3d 9 (Ist Cir. May 9, 2003).

[37] Al decir de Ramírez Ramírez, Agustín, "toda la información contenida en el expediente clínico se encuadra en el concepto de "datos personales", de tal suerte que las instituciones públicas prestadoras de servicios médicos cuentan, entre sus archivos, con información de los datos de salud —tanto físicos como mentales— de la mayor parte de la población de nuestro país. Lo anterior no pasaría de ser un dato estadísticamente trascendente, si no fuera por las implicaciones que puede tener este criterio en la relación médico-paciente y en la forma de ejercer la medicina pública", nuestra preocupación va más a la parte de las instituciones médicas privadas que no tienen a la fecha algún control sobre esos expedientes que contienen datos personales, porque después de leer lo dicho por Ramírez en la parte pública estamos de una u otra forma cubiertos. RAMÍREZ RAMÍREZ, Agustín, Tratamiento jurídico de los datos clínicos en México (Información y limites de acceso) en CIENFUEGOS SALGADO, David y MACÍAS VÁZQUEZ, Maria Carmen, *Estudios en homenaje a Marcia Muñoz de Alba Medrano Bioderecho, tecnología, salud y derecho genómico*, Instituto de Investigaciones Jurídicas, UNAM, México, 2006, p. 338.

V. El derecho a la vida privada y los Proveedores del Servicio de Internet (ISP)

Cada vez que nos conectamos a la red, requerimos de un servicio que nos permite conectarnos al ciberespacio. Este servicio lo prestan los llamados *Internet Service Providers* (ISP) o Proveedores del Servicio de Internet (PSI). Tradicionalmente se les ha definido como la "organización, habitualmente con ánimo de lucro, que además de dar acceso a Internet a personas físicas y/o jurídicas, les ofrece una serie de servicios (por ejemplo, hospedaje de página web, consultoría de diseño e implantación de *webs* e Internet, etc.,)".[38] Resultan interesantes además mencionar que en nuestra legislación no se habla directamente de Proveedores de Servicio de Internet, pero una interpretación al artículo 3 fracción XII, de la Ley Federal de Telecomunicaciones nos da una idea al señalar que es el "servicio que presta un usuario de la red concesionada o red pública de telecomunicaciones, cuya actividad tiene efecto en el formato, contenido, código, protocolo, almacenaje o aspectos similares de la información transmitida".

Algunas teorías se han tejido en torno al grado de participación y responsabilidad que tienen los ISP cuando por ejemplo, derechos como el de la vida privada de las personas han sido quebrantados. De ello, a mi parecer, deben hacerse ciertas observaciones.

Dentro de quienes proveen del servicio de Internet a los usuarios, están aquellos que lo hacen de manera gratuita. Se ha dado el caso de que, para acceder a este servicio sin costo ofrecido por los ISP, ha sido necesario llenar una serie de datos. De ello se forman grandes bases de datos y se instalan *cookies* que permiten seguirle la pista a los cibernautas. El negocio de estos ISP es vender esa información, obtenida de manera ilegal y arbitraria, a terceros. Eso sin duda es atentar contra nuestra vida íntima y es condenable por la justicia. Para ilustrar lo antes expuesto es interesante mencionar por ejemplo la cláusula sexta del contrato que deben firmar quienes acceden a los servicios gratuitos que ofrece el servidor español Laflecha.net, y que literalmente dice que:

> Marqueze garantiza la confidencialidad de sus datos al incorporarlos a un fichero de nivel de seguridad alto, inscrito en la Agencia de Protección de Datos, con la finalidad de gestionar la prestación del servicio y permitir poner en contacto a los usuarios entre sí y a su vez con la empresa Marqueze Telecom, S.A, a través de las distintas plataformas desde las que sea accesible el servicio, tales como Internet, Televisión, prensa o cualquier otro apto para la prestación del servicio,

[38] Definición obtenida del glosario de Términos Informáticos en http:// www.ati.es/novatica/glosario/glosario_internet.html Consultado el 21 de octubre de 2007.

> y la remisión por parte de esta compañía, destinataria de los datos, de información sobre productos y servicios, propios o de terceras personas, que pudieran ser de su interés, para lo cual usted presta su consentimiento. Dado que entre sus datos pueden encontrarse algunos especialmente protegidos como los de orientación sexual, se le informa de su derecho a no proporcionar estos datos. Asimismo usted presta el consentimiento para dicho tratamiento.
> El usuario presta su consentimiento expreso e inequívoco que para el tratamiento de los datos recogidos con la finalidad prevista en el párrafo anterior se efectúe a través de un servidor ubicado en un datacenter, situado en Madrid, España, mediante Comvive Servidores S.L cuyas prestación del servicio se encuentra en http://www.comvive.es/ [39]

Un caso distinto es el de los proveedores de servicios que presentan sitios en los que se ofrecen o se cometen actos contrarios al derecho. Común ha sido el caso de proveedores de servicios de Internet, donde a través de los sitios que funcionan por los servicios que éstos prestan, se ha injuriado a personas, atentando de esta manera contra su honor y su vida privada. Un caso de estas características se produjo en marzo del año 2000 en Inglaterra, donde el proveedor de servicios *Demon Inc*. fue obligado a pagar, por concepto de indemnizaciones por los daños causados, producto de las injurias transmitidas en un foro de discusión alojado en sus servidores, la suma de 15.000 libras esterlinas. El afectado apuntó la querella contra la empresa proveedora de la conectividad en calidad de responsabilidad de los contenidos injuriosos.[40]

Como un ejemplo, al no existir en nuestro país un solo caso de interpretación judicial en este sentido debemos ilustrar el ocurrido en la jurisprudencia chilena donde existe un caso de similares características al ya narrado y que merece ser visto con detalle. Se produjo en Concepción, donde el 31 de julio de 1999, a causa de un aviso que apareció en la sección "Productos y Servicios" que ofrece ENTEL Chile a través de su proveedor de servicios de Internet www.entelchile.net. Dentro de estos "servicios Gratuitos" se encuentra la sección de Avisos Clasificados, ubicada en el

[39] Consultar condiciones de privacidad de www.laflecha.net

[40] La información de este caso fue obtenida del informe de JIJENA LEIVA, Renato en *Responsabilidad de los ISP por la difusión de contenidos online*, pp. 7 y 8. el mismo autor también se refiere a la resolución del Consejo de Telecomunicaciones de la Unión Europea, que el 27 de septiembre de 1996 resolvía que debe impedirse la difusión de contenidos ilícitos en Internet, argumentado que "lo que es ilícito fuera de línea también lo es en línea", enfocando el fallo principalmente a que los Estados Miembros "adopten normas que regulen los nuevos servicios de Internet, en particular la actividad y la responsabilidad de los proveedores de conectividad o suministros de servicios de Internet". Revista Electrónica de Derecho Informático, No. 15, octubre de 1999, http://premium.vlex. com/doctrina/REDI-Revista-Electronica-Derecho-Informatico/Informe-legal-improcedencia-censurar-legalmente-contenidos-Internet-Analisis-Boletin-N%B02395-19/2100-107405,01.html Consultado el 21 de octubre de 2007.

sitio web http://www.tribu.cl, administrada por la empresa externa Grupo web, la que a su vez tiene varias subdirecciones como computación empleos, diversión, espectáculos, etcétera, entre ellas se publicó un anuncio de ofrecimientos sexuales en el que figuraba una adolescente de 17 años como remitente y donde se indicaba como teléfono de contacto el de su teléfono privado. Esto dio lugar a desagradables episodios que produjeron, entre otras cosas, una profunda crisis emocional en la afectada por el mal causado contra su honor y su vida privada. Producto de ello, el padre de la menor decidió interponer un Recurso de Protección contra el ISP, en este caso contra la Empresa Nacional de Telecomunicaciones ENTEL S.A. Se trata del primer caso en que los tribunales chilenos resolvieron sobre un atentado contra el derecho de la vida privada cometido a través de Internet. De este polémico fallo se concluyó, en resumen, lo siguiente:

> Considerando 19° Que en un sitio web pueden publicarse y divulgarse contenidos ilícitos o nocivos, sea mensajes, avisos o bienes protegidos por propiedad intelectual que no cuenten con autorización cuya utilización cause daño a la honra y bienes de terceros, invadiendo su vida privada e intimidad vulnerando su honra o atentando contra su patrimonio o, incluso, tales avisos o mensajes pueden llegar a ser contrarios a la ley, el orden público, a la seguridad nacional o a la moral o a las buenas costumbres.
> En la delimitación de las responsabilidades, son actores en Internet: el proveedor de acceso a la red, el proveedor de sitio o de almacenamiento, el proveedor de contenido y los usuarios o destinatarios finales del servicio.
> El proveedor de acceso permite que un determinado usuario de conecte con la red Internet, que de no existir ese acceso haría imposible la comisión del ilícito; el proveedor de sitio o almacenamientos, en la medida que permita que un determinado sitio web en el que se cometan actos ilícitos permanezcan almacenados en su propio servidor, que de no contar con este dispositivo técnico haría imposible la existencia o permanencia de ese sitio web en Internet; y el proveedor de contenido, por ser el que directamente incorpora contenidos ilícitos bajo su tuición en un determinado sitio *web*".[41]

Para efectos de este caso, y según lo señala el propio considerando 20° de este fallo, ENTEL S.A. tiene a su vez la calidad de proveedor de acceso y de proveedor de alojamiento del sitio www.tribu.grupoweb.cl. La calidad de proveedor de contenido la tiene por su parte la empresa "Grupo web". De acuerdo al considerando 21°, donde se expone la opinión del Profesor de Propiedad Intelectual de la Facultad de Derecho de la Universidad de Chile y Director General de la Sociedad Chilena del Derecho de

[41] Considerando 19° del Recurso de Protección N° 243-1999 contra ENTEL Chile, en el Archivo de Gaceta Jurídica, N° 239, pág. 229, edición de Mayo del 2000. Santiago, Chile.

Autor, Santiago Schuster Vergara, la responsabilidad recae directamente en el usuario proveedor de contenido en la red. Puede además extenderse a aquellos que son incorporados directamente por los destinatarios finales del servicio Internet, cuando el proveedor del sitio ha creado un fondo de información como los foros que en él se encuentran, y no ha tomado las providencias mínimas necesarias para la adecuada identificación de los usuarios que allí participan. Asimismo, se determinan que también cabe responsabilidad al proveedor de acceso y al proveedor de alojamiento de la página web respectiva, cuando, a sabiendas de la actividad ilícita que se realiza por los abonados a su servicio, éstos no se han evitado por miedo que su acceso se vuelva imposible o que se remueva la información allí contenida. Como lo señala Humberto Carrasco Blanc refiriéndose a este considerando, esta sería la posición que han adoptado algunos países europeos,[42] donde la responsabilidad recaería en los ISP "cuando pueda

[42] Resulta sumamente interesante conocer la posición de la Directiva de la Unión Europea que efectivamente parece haber dado las directrices en este fallo. De la mano de la obra de VALLEPUGA GONZÁLEZ, Paula se describe a continuación, la posición de los europeos, quienes refiriéndose a la responsabilidad de los ISP, han manifestado que: " Esta Directiva, en principio no impone una obligación de supervisión general; pero para excluirles de responsabilidad regula una serie de imposiciones en función del servicio de la información que presten. La exclusión de obligación general de supervisión se recoge en el artículo 15: "1. los Estados miembros no impondrán una obligación general de supervisar los datos que transmitan o almacenen, ni una obligación general de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas, respecto de los servicios contemplados en los artículos 12, 13 y 14 . 2. Los Estados miembros podrán establecer obligaciones tendentes a que los prestadores de servicios de la sociedad de la información comuniquen con prontitud a las autoridades públicas competentes los presuntos datos ilícitos o las actividades ilícitas llevadas a cabo por destinatarios de su servicio o la obligación de comunicar a las autoridades competentes, a solicitud de éstas, información que les permita identificar a los destinatarios de su servicio con los que hayan celebrado acuerdos de almacenamiento." La responsabilidad de los distintos prestadores de servicios intermediarios se recoge en los artículos 12, 13 y 14. la Directiva distingue tres tipos de servicios: 1. servicio de mera transmisión: consiste en transmitir por una red de telecomunicaciones, datos facilitados por el destinatario del servicio o en facilitar acceso a una red comunicaciones. Estos servicios de mera transmisión engloban el almacenamiento sirva exclusivamente para ejecutar la transmisión de datos a través de una red de comunicaciones cuando el almacenamiento de la información es automático, provisional y temporal, realizado además con la única finalidad de hacer más eficaz la transmisión ulterior de esa información a otros destinatarios del servicio a petición de éstos. 3. alojamiento de datos: consiste en almacenar datos facilitados por el destinatario del servicio. Esta clasificación coinciden con la realizada por el Anteproyecto de Ley de Comercio Electrónico español, que ha sido aprobado el 7 de febrero de 2000. El Anteproyecto los denomina, respectivamente, operadores de acceso, prestadores de servicios de almacenamiento de datos y prestadores de servicios de alojamiento de datos. A) Servicios de mera transmisión: los PSIs que ofrezcan este servicio no serán responsables, siempre que: no hayan originado ellos mismos la transmisión; el prestador de servicios cumpla las condiciones de acceso a la información; cumpla las normas relativas a la actualización de la información, especificadas de manera ampliamente reconocida y utilizada por el sector; no interfiera en la utilización lícita de la tecnología ampliamente reconocida y utilizada por el sector, con el fin de obtener datos sobre la utilización de la información; y actúe rápidamente efectivo de que: la información ha sido retirada del lugar de la red en que se encontraba inicialmente; de que se ha imposibilitado el acceso a ese información; o de que un tribunal o autoridad administrativa ha ordenado reti-

esperarse razonablemente que son conscientes de que aquél es *prima facie* ilegal, no han tomado medidas razonables para eliminar dicho contenido una vez que el mismo ha traído claramente su atención."[43]

Sin embargo y a pesar de lo anteriormente expuesto cabe preguntarse si efectivamente los grados de responsabilidad han sido o no correctamente repartidos. Más concretamente, sobre si en realidad en estos caso específicos, los ISP son o no responsables por los actos cometidos contra la vida privada de las personas. A ello ha salido al paso la doctrina, entre ellos Jijena, Carrasco y Llaneza González, quienes argumentan que las exigencias de tomar las "providencias mínimas" como identificar al usuario o extraer contenidos contrarios al orden público, las buenas costumbres o la moral de la red se vuelven técnica y económicamente imposibles de ejecutar por parte de los ISP. Además, no les confiere responsabilidad alguna por su rol de intermediarios. Como lo señala Jijena, "Analógicamente, tal posición sería equivalente al absurdo de sancionar a las compañías de teléfono por permitir a sus usuarios que se conecten con líneas de conversaciones eróticas o pornográficas".[44] En lo personal, comparto las posturas antes mencionadas, ya que por las características de la red en estos casos específicos, la responsabilidad recaería en quien comete específicamente el ilícito, a saber el usuario (obviamente siempre que el ISP esté legalmente establecido y no sea éste el responsable de incitar a la comisión de estos ilícitos). El proveedor de Servicio de Internet no sería sino el "vehículo" que se presta para acceder al ciberespacio, por lo cual de la misma manera que está exenta de responsabilidad una empresa que alquila sin complicidad un vehículo en el cual se comete un crimen, el ISP también debería estar fuera de toda responsabilidad por los ilícitos cometidos en al red. Ello no es impedimento para que, desde mi punto de vista, se imponga a los ISP la obligación de realizar revisiones periódicas respecto de los contenidos que se encuentran en su servidor para que esto no se convierta en cuna de delitos cometidos a través del ciberespacio.

---

rarla o impedir su acceso a ella, Alojamiento de datos: el prestador de servicios no tendrá responsabilidad por los datos almacenados siempre que: no tenga conocimiento de lo dispuesto en el párrafo anterior, el PSI actué con prontitud para retirar los datos o hacer que el acceso a ellos sea imposible. Por tanto, según este artículo, a los servidores que tengan alojadas páginas web no se les obliga a hacer una revisión periódica de su contenido, pero si por cualquier circunstancias conocen que una actividad o información es ilícita deberá o bien retirarla, o bien impedir el acceso a la misma." *Responsabilidad de los Prestadores de Servicio en la Sociedad de la Información*, Revista de Derecho Informático, No. 030, enero de 2001, http://www.alfa-redi.org/rdi-articulo.shtml?x=615 Consultado el 21 de octubre de 2007.

[43] Carrasco Blanc, Humberto, *Algunos Aspectos de la Responsabilidad de los Proveedores de Servicios y Contenidos de Internet. El caso "ENTEL"*, Revista de Derecho Informático, No. 26, septiembre de 2000, http://www.alfa-redi.org/rdi-articulo.shtml?x=554 Consultado el 21 de octubre de 2007.

[44] Jijena Leiva, Renato, *Op. cit*.

La legislación española, a través de la Ley de Servicios de la Información y del Comercio Electrónico, más conocida como LSSICE, regula la presencia de contenidos ilícitos en red, responsabilizando a los ISP en caso de que, al estar al tanto de que su servidor posee algún contenido ilícito, no lo hayan comunicado a la Administración.[45] Es así que dicha ley, en su exposición de motivos en el punto tercero segundo párrafo dice:

> "La ley establece, así mismo, las obligaciones y responsabilidades de los prestadores de servicios que realicen actividades de intermediación como las de transmisión, copia, alojamiento y localización de datos en la red. En general, éstas imponen a dichos prestadores un deber de colaboración para impedir que determinados servicios o contenidos ilícitos se sigan divulgando. Las responsabilidades que puedan derivar del incumplimiento de estas normas no son sólo de orden administrativa, sino de tipo civil o penal, según los bienes jurídicos afectados y las normas que resulten aplicables".[46]

En todo caso, hay quienes creen que la solución está en que los proveedores de servicio de Internet instalen programa filtro en la red que impida el acceso a sitios web ilegales. Otros creen que la solución más factible es la autorregulación o la firma de Tratados Internacionales que legislen sobre el tema.

VI. ¿Las páginas web protegen efectivamente nuestro derecho a la intimidad?

Además de analizar el rol que juegan los Proveedores de Servicio de Internet, es prudente estudiar qué tan efectivas son las políticas de seguridad que los sitios web ofrecen y cómo éstos atentan muchas veces contra el derecho a la vida privada de las personas sin que siquiera nos percatemos de ello. De hecho, aún cuando existen aparentes garantías frente a la información que uno entrega a estos sitios web, más de uno se ha llevado una sorpresa a la vuelta de la esquina. Para no ir muy lejos,

[45] Esta información se obtuvo de una entrevista realizada a la exministra de Ciencia y Tecnología española Anna Birulés, publicada en la revista *Cuenta y Razón del pensamiento actua*l, Entrevista con Anna Birulés, Ministra de Ciencia y Tecnología, No. 117, La Rioja, España, pág. 141-143.

[46] Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico, o LSSICE, punto tercero, párrafo segundo de la exposición de motivos. Fue aprobado por el Consejo de Ministros con fecha 8 de febrero de 2002, y en la actualidad ha sido muy cuestionado, sobre todo por grupos que defienden la libertad de expresión. Se puede visitar en la página: "La ley de Internet fácil" del Ministerio de Industria, Turismo y Comercio de España: http://www.lssi.es/Secciones/Normativa/ Consultada el 21 de octubre de 2007.

basta con recordar lo polémico que puede ser entregar el número de nuestra tarjeta de crédito, que es un dato de carácter personal, a un ente que está al otro lado de la conexión y que no tenemos la menor idea de que efectivamente se trate de quien dice ser. A causa de estos, las estafas en Internet han sido cuantiosas. A ello debe agregársele el hecho de que muchos de estos sitios web también juegan con información que les hemos entregado, comercializándola ilegalmente y sin nuestro consentimiento.

Resulta también curioso que incluso páginas web como *Hotmail* (que no solamente ofrecen un servicio de correo electrónico gratuito, sino que tienen una amplia gama de servicios), han transferido datos de sus suscriptores, valiosa información, a un directorio público en Internet.[47] Todavía más polémico es el caso del famoso sitio Terra, que fue multado por la Agencia de Protección de Datos española con la suma de 20 millones de pesetas por haber permitido la fuga de datos personales de sus clientes en agosto del año 2000.[48]

En nuestro país los casos más importantes fueron en el sector público. En mayo de 2003 se puso al descubierto que la empresa *Choice Point* vendió al gobierno de Estados Unidos bases de datos de uso privativo del Estado mexicano desde 18 meses atrás, las investigaciones permitieron conocer que en 2001, la empresa Soluciones Mercadológicas en Bases de Datos vendió en 335 mil dólares a *Choice Point* la base de datos del padrón electoral del Instituto Federal Electoral, en el que se incluía información de 58 millones de votantes mexicanos.[49]

Asimismo, la *American Civil Liberties Union* (ACLU) habría solicitado en junio de 2002 a la *Federal Trade Comisión* (FTC) sancionar a una empresa gigante de productos farmacéuticos, llamada Eli Lilly, por haber divulgado la lista de personas que consumían su antidepresivo Prozac. Este hecho ha sido considerado como atentatorio contra el derecho a la vida privada de las personas, pudiendo como consecuencia de ello traer discriminaciones o rechazos contra quienes consumen el fármaco.[50]

---

[47] Información publicada en el diario español "El País" *Passport almacena los datos de 150 millones de usuarios*, 25 de octubre de 2000.

[48] Información publicada en el diario español "Elmundo.es" *La agencia de protección de datos multa a Terra*, 28 de marzo de 2001.

[49] Información obtenida del diario "El Universal", *Multa millonaria a vendedores del padrón electoral*, en su edición del día, sábado 16 de diciembre de 2006. http://www.eluniversal.com.mx/notas/394453.html

[50] Esta noticia se publico en la página web de Newsbytes.com, para ver más detalle de esta información, remitirse a http://www.newsbytes.com

El caso más alarmante desde mi punto de vista es aquel que se refiere a sitios web que se dedican a entregar información sobre nosotros, vale decir datos de carácter personal e incluso datos sensibles como nombre, dirección, teléfono, CURP, IFE, cédula profesional, estado civil, etcétera. A pesar de que este tipo de páginas no es muy popular en México, en Europa y Estados Unidos son una práctica frecuente. He querido presentar un caso concreto con las siguientes páginas de Internet que prestan sus servicios en Argentina y Estados Unidos respectivamente. La primera nos permite acceder a correspondencia electrónica de terceros, para de esta manera poder conocer qué mensajes le han llegado al destinatario, cuándo los ha leído, desde qué número IP lo ha hecho, así como otros datos sensibles. El reporte se actualiza en tiempo real, y además va informando lo que el destinatario hace. Si al mensaje enviado se le agregan links, el sistema avisa si el destinatario da *click* en los mismos

Como consecuencia de la indiscriminada transferencia de datos de carácter personal que se efectúan a través de Internet, ya algunos ordenamientos jurídicos están tomando cartas en el asunto. Resulta interesante mencionar un pronunciamiento de la Unión Europea, donde en diciembre del 2001 se manifestaba en Bruselas que: "El Consejo de Ministros de Telecomunicaciones de la Unión Europea ha alcanzando un acuerdo sobre la Directiva referente a la privacidad en las comunicaciones electrónicas, norma que compromete a organismos públicos y privados a destruir o hacer anónimos los datos personales que obtengan a través de sus comunicaciones en Internet, excepto si consideran que éstos afectan a la seguridad pública o del Estado". Uno de los grandes aportes de este hecho constituye el reconocimiento que la Directiva establece al principio universal de la "destrucción inmediata" de los datos personales. Es así que se permite almacenar tales datos si el usuario ha sido informado. Sin embargo, esta destrucción no se llevará a cabo "si fuera necesario para la protección de la seguridad pública, la Defensa, la seguridad del Estado, incluido el bienestar económico, o la aplicación del ordenamiento penal".

Se dice que esta norma no altera el equilibrio actual que las legislaciones nacionales mantienen entre le derecho a la intimidad y la protección de la seguridad. Esta legislación, que tiene como objeto mantener el nivel de protección de la vida privada ante la irrupción de nuevas tecnologías de la comunicación, fue aprobada después de que los ministros resolviesen lo últimos puntos de fricción de la propuesta original, en especial, el referido al correo electrónico publicitario con fines de venta, que, como general, no podrá ser enviado sin autorización previa del receptor.[51]

[51] Esta noticia puede leerse con detalle en artículo publicado por el diario español "Edmundo.es" de fecha 7 de diciembre de 2001, "*Decisión de los ministros de telecomunicaciones. La*

A nivel América latina, no hay todavía nada concreto en cuanto a afrontar este problema. Pero debemos sin lugar a dudas servirnos el día de mañana de la experiencia legislativa de otros países que en la actualidad ya se encuentran luchando contra los peligros que traen consigo las nuevas tecnologías.

VII. Internet como medio de control de empleador sobre el trabajador

Es difícil que en estos días una empresa de tamaño mediano a grande no se encuentre incorporada a los servicios que le ofrece Internet. De hecho, es de todos conocido que con la llegada del ciberespacio, el mundo laboral sufrió grandes transformaciones, ya que esa necesidad imperiosa de contactarse con gente, conocer otros mercados, sobrepasar fronteras, ofrecer sus productos a nivel nacional e internacional, palpar las tendencias de la economía, transar en las bolsas de cualquier parte de la Tierra, por nombrar algunas ventajas, se volvió una realidad para muchos sin necesidad de ser grandes potentados económicos. Internet abrió las puertas del mercado al mundo. Sin embargo, quienes en la actualidad se han dedicado a estudiar el fenómeno de la red respecto del impacto que produce en la vida privada de las personas están especialmente preocupados por la amenaza que se ha vuelto este medio de comunicación a la hora de controlar a los empleados. Es por ello que hemos querido tratar este caso que, si bien tiene similitud con puntos analizados anteriormente, merece ser estudiado por el alcance que está logrando a nivel mundial. Se trata pues nuevamente de dos derechos constitucionales en conflicto. El primero de ellos, el derecho a la libertad de trabajo y protección, la libertad de empresa y la libertad de información; y el segundo, el derecho a la vida privada de las personas. Este aparente conflicto se traduce en la vida cotidiana en distintas circunstancias.

Al momento de contratarse a personal, se suele hacer un proceso de selección, legítimo en los casos en que éste se vea fundado en capacidades, aptitudes y condiciones laborales del postulante. Para ello se utilizan distintos mecanismos como currículos, entrevistas, pruebas e incluso la contratación de empresas que se encargan de esto. Sin embargo, en este proceso de búsqueda de información del potencial trabajador, se puede llegar a la averiguación de datos que se consideren personales e incluso

UE respetará la privacidad de datos en Internet salvo cuando afecten a la seguridad", para acceder directamente a este artículo, remitirse a http://www.elmundo.es/navegante/2001/12/07/seguridad/1007715325.hml Consultada el 21 de octubre de 2007.

sensibles, y que pueden amenazar la vida privada del postulante, como por ejemplo su tendencia política, su religión, su estado de salud, por nombrar algunos ejemplos. Sin embargo, si ésta se obtiene a través de medios ilícitos como la transferencia de datos de carácter personal a través de Internet sobre una persona, sin que existiera previamente la prestación de su consentimiento, obviamente que se trata de un acto de discriminación ilegítimo.[52]

Pero uno de los casos que más ha llamado la atención es el uso de la red como medio de control del empleador sobre el trabajador. Se discute básicamente si Internet es una herramienta lícita para inspeccionar a los subordinados o si en realidad se está atentando contra la intimidad de éstos. El problema se da básicamente a la hora de determinar si es legal que el empleador revise, por ejemplo, la correspondencia electrónica de sus empleados, y por consiguiente examine también hechos pertenecientes a la vida privada de éstos. ¿Se puede despedir al trabajador por concepto de la información que se obtuvo al examinar su correo electrónico?[53]

Uno de los casos de mayor impacto al respecto se produjo a finales del año 1999 en España, donde un empleado del Deutsche Bank fue despedido luego de que se demostrara que usaba el correo electrónico que le otorgara la empresa para fines distintos a los que se le había asignado. La defensa de Gregorio Jiménez Román, el empleado despedido, tuvo sus fundamentos en que se violó su correspondencia y por consiguiente se atentó contra su vida íntima al habérsele revisado su casilla de correo electrónico. Por su parte, el banco legitimó su defensa en el hecho de que el ex empleado utilizaba el correo de la empresa en forma improcedente y masiva para enviar mensaje a través de Internet, muchos de ellos con contenido pornográfico. El afectado recurrió ante el juzgado de Instrucción Segundo de Barcelona, y posteriormente ante el Tribunal Superior de Justicia de Cataluña, que a su vez legitimó el proceder del Deutsche Bank, argumentando que:

> "concurre así un acreditado incumplimiento laboral del trabajador sancionado, ya que su actitud supone la pérdida de tiempo de trabajo efectivo, tanto del trabajador al confeccionar y enviar los mensajes como de sus compañeros al recibirlos y leerlos". [54]

[52] Para ver con más detalle este tema, remitirse a la obra de CUERVO, José, *La Intimidación Informática del Trabajador*, Revista de Derecho Informático, No. 003, octubre de 1998, http://www.alfa-redi.org/rdi-articulo.shtml?x=158 Consultada el 21 de octubre de 2007.

[53] Para mayor información ver la obra de RUBIO DE MEDINA, Maria Dolores, *El despido por utilización personal del correo electrónico*, Editorial Bosch, España, 2003.

[54] Sentencia dictada por la Sala de Social del T.S.J. de Catalunya de fecha 14/11/2000, conocida también como "*La sentencia de los emails*", pág. 11. http://www.abog.net/documentos/documentos_emails_1.asp Consultada el 21 de octubre de 2007.

El informe de la Fiscalía de Cataluña sentenciaba que: "el derecho a la intimidad es aplicable al ámbito de las relaciones laborales pero en dicho ámbito debe tenerse en cuenta que el poder de dirección, imprescindible para la buena marcha de la organización productiva, atribuye al empresario, entre otras facultades, la de adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones laborales". El único límite que pone la fiscal a ese control es que el empresario debe ejercer esas facultades "dentro del debido respeto a la dignidad del trabajador". Según los abogados del banco, la empresa había advertido a sus empleados de la naturaleza exclusivamente profesional que debía tener el uso del correo electrónico.[55]

Otro caso de similares características se produjo también en España, en diciembre del 2001, luego de que una empresa, Productos Eaton Livia, instalara un programa informático en los ordenadores de los trabajadores para controlar tanto sus actividades como su rendimiento laboral. Producto de ello, se despidió a un empleado que había estado jugando solitario desde su puesto de trabajo. En primera instancia, un Juzgado Social de Barcelona había dado la razón al trabajador. Sin embargo, el Tribunal Superior de Justicia de Cataluña revocó el fallo, alegando que "el ordenador es un instrumento de trabajo que pertenece a la empresa y un medio al servicio de los fines económicos y mercantiles de la misma y que el empresario tiene todo el derecho a supervisar la actividad de sus empleados". La compañía, según la sentencia, instaló los programas de control de forma que no pudieron ser detectados por el usuario y lo hizo sin entrar en el PC del trabajador por lo que, según destaca el tribunal, no violó su *password* (código de acceso), y que se trataría de un programa que se activaba de forma automática cuando se ponía en marcha el ordenador. Asimismo, el veredicto indicaba que de acuerdo con el control de la empresa, el empleado se pasó un día jugando menos de una hora, durante otros seis días estuvo entre una hora y dos, durante otros 24 días estuvo entre dos y tres horas y dos días más jugó más de tres horas. El "programa espía" tenía la particularidad de identificar los programas y ventanas de Windows que se activaban en cada momento sin invadir los contenidos, ni siquiera el PC. En conclusión, para el Tribunal Superior de Justicia de Cataluña, la medida de control informático de la empresa era "justificada (ya que existían razonables sospechas de la comisión por parte del empleado de grave irregularidades en su puesto de trabajo."[56]

[55] La información de este caso de obtuvo del diario español "Elmundo.es" la nota se titula "*La Fiscalía entiende que no es delito que los jefes controlen los emails de sus empleados*" http://www.elmundo.es/navegante/2001/11/26/esociedad/1006801495.html de fecha 26 de noviembre de 2001. Consultada el 21 de octubre de 2007.

[56] *Sentencia del T.S.J. de Cataluña de 23 de octubre de 2000* (AS. 2000/4.536), por la que se declara de oficio la nulidad de la Sentencia del Juzgado de lo Social núm. 1 de los de Barcelona en

Frente a los dos casos recién expuestos, es preciso reflexionar acerca de la legalidad de los métodos utilizados por el empleador a la hora de controlar a sus trabajadores. En lo personal, creo que las personas tenemos vida privada donde quiera que nos encontramos, ya sea en nuestra casa, en nuestro trabajo, en nuestro automóvil o mientras estamos de vacaciones. Por consiguiente, nuestra correspondencia, que forma parte de nuestra esfera íntima, debe ser respetada igualmente. Sin embargo, creo que debemos ser consientes de que la computadora, así como por ejemplo el fax o el teléfono son bienes que le pertenecen a la empresa y que tienen asignada una función determinada para su uso, el cual es el funcionamiento de ésta, por lo que su uso indebido por parte del trabajador constituyen causales de incumplimiento de los deberes laborales. Veo razonable que, dentro de las cláusulas del contrato de trabajo, se especifique que por ejemplo el correo electrónico que la empresa otorga a sus trabajadores no es de uso personal, sino profesional, y por consiguiente sea perfectamente posible que el empleador lo examine siempre que crea necesario. Además, compartiendo la postura de gran parte de la doctrina sobre este asunto,[57] de requerirse la inspección del mismo, éste debería llevarse a cabo previa notificación al trabajador, indicándole el motivo de la inspección y qué se va a inspeccionar (obviamente todo ello debe practicarse con fines puramente profesionales). Dicha notificación no necesariamente debe significar avisar con tiempo de la inspección que se va a realizar (ya que en este caso se corre el riesgo de que puedan cometer fraude los trabajadores), sino que la notificación debería interpretarse más como el hecho de efectuar tal revisión de la casilla en presencia del trabajador.

Resulta interesante la opinión del juez norteamericano James M. Rosenbaum, quien en una entrevista concedida al diario argentino Clarín[58] en diciembre del 2001 señalaba que: “Ha surgido un nuevo “principio legal”. Si una corporación, empresa u organismo del Estado posee una computadora y un empleado pone en ella cosas personales, el autor no tiene derecho sobre el material almacenado ni puede esperar privacidad”. Según el magistrado, los estadounidenses sienten una profunda repulsión

demanda de despido disciplinario contra la empresa “PRODUCTOS EATON LIVIA S.A.” formulada por el actor con antigüedad superior a 30 años, que era Jefe de Métodos y con salario mensual de 680.488 ptas.

[57] Una detallada exposición de este tema está en la publicación de Herrera Bravo, Rodolfo y Hernández Rubio, Montserrat, *La Legitimidad del Control Tecnológico del Empleador sobre el Trabajador*, Revista de Derecho Informático, No. 035, junio de 2001, http://www.alfa-redi.org/rdi-articulo.shtml?x=709 Consultada el 21 de octubre de 2007.

[58] Esta información se obtuvo de la Columna de Opinión del diario argentino *Clarín* de fecha de diciembre de 2001, en entrevista al Juez del estado de Minnesota, James M. ROSENBAUM, en un artículo titulado ”Ante todo, privacidad”.

por las "inspecciones generalizadas".[59] Continua el Juez argumentando que "si no se le da el debido aviso al trabajador de que se va a llevar a cabo una inspección, el empleador debería perder todo derecho a tomar cualquier medida laboral adversa al trabajador".

En nuestro país no existe una regulación específica ni precedente alguno en jurisprudencia sobre el uso del correo electrónico e Internet en las relaciones laborales, la única disposición que existe es el artículo 135 de la Ley Federal del Trabajo que en su fracción IX, señala que el trabajador tiene la obligación de utilizar las herramientas de trabajo únicamente para el objeto para el que le fueron destinadas, por lo que se puede concluir que actuar en contra de lo que señala este numeral puede significar una causa de rescisión de contrato de trabajo sin responsabilidad alguna para el empleador. Al decir de Yesín Ramírez Chelala: "por lo que toca a la Ley Federal del Trabajo, si bien es cierto que por analogía se le podría dar el carecer de herramienta de trabajo al correo electrónico e Internet, sería idóneo para efectos procesales, que en la misma Ley se adoptara dicha disposición, a fin de proteger a los patrones del uso indebido de las TICS por parte de los trabajadores, con el objeto de disminuir riesgos y responsabilidades que su uso indebido pueda conllevar".[60] Se puede decir que si el trabajador ocupa parte de su tiempo laboral en el uso de correo electrónico o consulta de Internet para fines personales desatendiendo sus labores pone en riesgo el patrimonio de la empresa actuando en contra de la fracción IV del numeral 134 del mismo ordenamiento legal que establece que el trabajador deberá ejecutar el trabajo con la intensidad, cuidado y esmero apropiados y en la forma, tiempo y lugar convenidos.

Ahora bien, el respeto a la vida privada de los trabajadores también tiene que ser garantizado, ya que Internet se puede convertir en medio de

[59] El precedente del tema que se trata en esta entrevista es el siguiente: "Hace unos meses, el tema se planteó en las oficinas de una importante editorial neoyorquina. Un gerente de la oficina comercial de la empresa recibió un sobre que contenía material fotocopiado. Cualquiera que fuera el contenido, al gerente le resultó claramente ofensivo. La empresa reaccionó con una búsqueda clandestina en la división "infectada" revisando el contenido del disco rígido de todas las computadoras, sin avisar a los empleados y pese a que el material ofensivo había sido fotocopiado y no generado por una computadora. Según parece, la búsqueda descubrió una serie de elementos irritantes que iban desde chistes hasta pornografía, todos dentro de computadoras de la empresa. La consecuencia: alrededor del 10 por ciento de los empleados del departamento fueron despedidos". La información de este caso se obtuvo de la misma entrevista efectuada por el diario *Clarín* de fecha 5 de diciembre de 2001 al juez Rosenbaum, cuyo texto fue extraído de la Columna de Opinión del mencionado rotativo.

[60] Ramírez Chelala, Yesín y Vera Prendes, Luis, *Aspectos Laborales de la sociedad de la información* en Navarro Isla, Jorge, (coord) *Tecnologías de la Información y de las comunicaciones aspectos legales*, Editorial Porrúa, México, 2005, p. 345.

control de los trabajadores, como dijera Rocio Ovilla Bueno[61] "es necesario hacer respetar las reglas relativas a la protección de la vida privada y el secreto de correspondencias. El empresario o patrón no tiene el derecho de interceptar el correo electrónico de sus trabajadores, ya que puede tener una responsabilidad penal por abrir este coreo de sus trabajadores", se refiere a la violación de correspondencia señalada expresamente en el artículo 16 de la Constitución Política,[62] pero como ya lo estudiamos es difícil hacer una analogía entre el correo convencional y el correo electrónico. Nuestro máximo tribunal, la Suprema Corte de Justicia de la Nación, nos da luz en el tema y en un criterio establece lo siguiente:

> VIOLACIÓN DE CORRESPONDENCIA, CONCEPTO DE CORRESPONDENCIA EN EL DELITO DE. Para la configuración del delito de violación de correspondencia es irrelevante que haya sido un sobre que contenía un giro telegráfico el que abrió indebidamente el inculpado, al no estar dirigido a él, toda vez que debe considerarse como correspondencia una comunicación escrita, entendiéndose por tal, una carta o comunicación con el sobrescrito cerrado o con la plica cerrada y sellada, un pliego igualmente guardado en el sobrescrito o la plica, un despacho telegráfico o telefónico con igual protección y cualquier *otra comunicación escrita análoga*.[63]

En este orden de ideas solamente podrían ser revisadas dichas comunicaciones con el consentimiento del expreso del trabajador, ya que si no es de esta forma carecen de valor probatorio y son constitutivas de delito.

Desde mi punto de vista, debe preciarse que si es la empresa la que provee de computadoras a los trabajadores y si ésta además les entrega una dirección de correo electrónico que incluso lleve dentro de la dirección el nombre de dicha entidad (ejemplo:jimenezgl@unistudios.com), es precisamente la empresa la dueña de la casilla. Se trata de un bien que ésta entrega a sus miembros para el desarrollo de las actividades para las cuales han sido contratados. En este caso, el trabajador no es más que un usuario de un bien que le pertenece a la persona jurídica, de la misma manera que el vehículo que por ejemplo determinados empleadores les facilitan a sus trabajadores para el desarrollo de sus actividades laborales.

---

[61] *La protección de los datos personales en México*, Editorial Porrúa, Colección Breviarios Jurídicos No. 28, pág. 50.

[62] Artículo 16 constitucional párrafo decimosegundo: "La correspondencia que bajo cubierta circule por las estafetas estará libre de todo registro y su violación será penada por la ley". A su vez el Código Penal Federal en su artículo 173 sanciona al que abra indebidamente una comunicación escrita que no esté dirigida a él.

[63] Tesis aislada, *Semanario Judicial de la Federación* y su *Gaceta*, t. VIII, junio de 1991, Octava Época, tribunales colegiados de circuito, p. 459.

Se vuelve además indispensable, creo yo, para evitar posibles arbitrariedades, que dentro del contrato de trabajo se especifique con toda claridad cuales son los márgenes dentro de los que deben manejarse los trabajadores al hacer uso de los bienes que le pertenecen a la empresa, en este caso específico, el correo electrónico que ésta les facilita. Dentro de la doctrina, José Joaquín Ugarte Godoy comparte también esta postura. De lo anteriormente expuesto, se puede además deducir que se trata de otro argumento legítimo que tiene el empleador, que apegado a las normas de derecho, le podría permitir inspeccionar las casillas de correo electrónico de sus subordinados.

Además de lo anterior, comparto la postura de Rocío Ovilla Bueno, en el sentido de que el empresario realice una cláusula en el contrato de trabajo donde se precise claramente cuáles son las posibilidades para que el trabajador utilice la mensajería electrónica de la empresa, así como los derechos que tiene el empresario para leer este tipo de correo profesional.

VIII. Internet y los Órganos Gubernamentales

Muchos entes policiales e investigativos utilizan Internet, conscientes de que es una poderosa herramienta al momento de realizar sus labores. Para los servicios de inteligencia, se trata de un medio sumamente útil y necesario para transmitir y recabar información. De esta manera, una nueva función de la red ha ido tomando forma, es lo que muchos expertos han llamado el ciberespionaje.[64] Y es que efectivamente, la red muchas veces ha sido utilizada como medio para la comisión de ilícitos como pornografía infantil, narcotráfico, e incluso actos terroristas. Sin ir muy lejos, recordemos que mucha información para cometer los atentados del 11 de septiembre fue transmitida a través de páginas de Internet, donde por medio de ciertos sitios, se revelaba información para cometer estos actos, como por ejemplo los planos de un avión, indicaciones precisas del actuar de los terroristas, etcétera. Ello ha motivado a que órganos gubernamentales, para contrarrestar este tipo de actos, utilicen a su vez la red para rastrear el uso que los particulares hacen de ella.

[64] La palabra cyber o ciber se define como un "Prefijo utilizado ampliamente en la comunidad Internet para denominar conceptos relacionados con las redes (ciberespacio, cibernauta, etc,) su origen es la palabra griega kibernao, que significa pilotear una nave". *Glosario básico inglés – español para usuarios de Internet*, Asociación de Técnicos de Informática de España, de esta raíz es que se ha formado el término ciberespionaje. http://www.ati.es/novatica/glosario/glosario_internet.html#indice Consultada el 21 de febrero de 2007.

Con el fin de ilustrar esto, he querido reproducir un extracto de una noticia que señalaba que: "*Carnivore*, la controvertida herramienta de vigilancia de mensajes de correo electrónico desarrollada por el FBI puede tener acceso a todo tipo de comunicaciones enviadas a través de Internet, según pruebas recientes. Un oficial del FIB que participó en las pruebas señaló que aunque *Carnivore* tiene la habilidad de grabar una gran cantidad de mensajes de correo electrónico y otro tipo de comunicaciones vía web, su uso está restringido por las leyes y las órdenes específicas de los tribunales.

Por su parte, Marcus Thomas, jefe de la sección de cybertecnología del FBI, declaró que en una situación real, la herramienta no podría poner a los filtros para que hagan nada. Pero nuestros procedimientos son muy detallados, solamente hacemos lo que nos está permitido por la orden de la corte", añadió Thomas."[65] Sin embargo, aún cuando en teoría estos mecanismos de rastreo debieran poder instalarse solamente previa autorización por parte de autoridad competente, en la práctica esto no sucede y es de todos sabido.

Países como Estados Unidos han propuesto la creación de una ciberpolicía, que como lo explica el español Sánchez Almeida, se trataría de "un cuerpo de intervención rápida que pudiese actuar en cualquier país del mundo sin autorización judicial, a fin de perseguir el cibercrimen allí donde ocurra". Agrega que "La prensa ha explicado que los países europeos lo han evitado, vendiendo la imagen de que Europa es más respetuosa con los derechos fundamentales. Tal información es tendenciosa".[66] Efectivamente, el control de la red es una tarea muy difícil de lograr, por no decir imposible. Aún cuando existen entes como el famoso ECHELON (conocido también por las siglas UKUSA, y que es un sistema de escuchas y filtrado de conversaciones a través del teléfono o de Internet),[67] los

[65] *Desastre 11-S. Como afectará este ataque el futuro de Internet*, página de noticias informáticas, Micro Tecnologías, el 12 de septiembre de 2001. http://www. microteknologias.cl/rep_carnivore.html Consultada el 20 de octubre de 2007.

[66] Sánchez Almeida, Carlos, *Intimidad: Un derecho en Crisis. La Erosión de la Privacidad*, Revista de Derecho Informático, No. 024, julio del 2000, http://www.alfa-redi.org/rdi-articulo.shtml?x=504 Consultada el 21 de octubre de 2007.

[67] *ECHELON* es la mayor red de espionaje y análisis para interceptar comunicaciones electrónicas de la historia. Controlada por la comunidad UKUSA (Estados Unidos, Canadá, Gran Bretaña, Australia, Irlanda del Norte y Nueva Zelanda), *ECHELON* puede capturar comunicaciones por radio y satélite, llamadas de teléfono, *faxes* y *emails* en casi todo el mundo e incluye análisis automático y clasificación de las interceptaciones. Se estima que *ECHELON* intercepta más de tres mil millones de comunicaciones cada día. A pesar de haber sido presuntamente construida con el fin de controlar las comunicaciones militares y diplomáticas de la Unión Soviética y sus aliados, se sospecha que en la actualidad *ECHELON* es utilizado también para encontrar pistas sobre tramas terroristas, planes del narcotráfico e inteligencia política y diplomática. Sus críticos afirman que el sistema es utilizado tam-

gobiernos no van a dar su brazo a torcer en este campo. Sánchez Almeida, refiriéndose a estos órganos argumentaba que "Mucho se hablado sobre ECHELON: gracias a los descubrimientos del periodista Duncan Campbell, fue objeto de un debate reciente en el Parlamento Europeo. Curiosamente, ese mismo Parlamento aprobó el 7 de mayo de 1999 el proyecto ENFOPOL, un sistema que pretendía que la Red pudiese ser transparente a la investigación policial. En las bases técnicas de Enfopol se habla de que todas las comunicaciones, origen, destino, contenido de los mensajes, puedan disponerse en tiempo real por la "autoridad competente". Afortunadamente, y espero no equivocarme, las sucesivas movilizaciones de grupos de defensa de derecho civiles van teniendo efecto, y el proyecto se está convirtiendo en un acuerdo de colaboración en el ámbito estrictamente judicial, que requerirá en cualquier caso autorización de los tribunales para cualquier tipo de escucha. Con todo, habrá que mantener la guardia".[68]

Es nuestro país para garantizar la presencia de la autoridad en la supercarretera de la información, la Policía Federal Preventiva desarrolló en México la primera Unidad de Policía Cibernética,[69] que además de las

bién para el espionaje económico y la invasión de privacidad en gran escala. Los miembros de esta alianza de habla inglesa son parte de la alianza de inteligencia UKUSA, que lleva reuniendo inteligencia desde la Segunda Guerra Mundial. La existencia de *ECHELON* fue hecha pública en 1976 por Winslow Peck. Varias fuentes afirman que estos estados han ubicado estaciones de intercepción electrónica y satélites espaciales para capturar gran parte de las comunicaciones establecidas por radio, satélite, microondas, celulares y fibra óptica. Las señales capturadas son luego procesadas por una serie de supercomputadoras, conocidas como diccionarios, las cuales han sido programadas para buscar patrones específicos en cada comunicación, ya sean direcciones, palabras, frases o incluso voces específicas. El sistema está bajo la administración de la NSA (*National Security Agency*). Esta organización cuenta con 100.000 empleados tan sólo en Maryland (Estados Unidos) (otras fuentes hablan de 38.000 empleados a escala mundial), por lo que es probablemente la mayor organización de espionaje del mundo. A cada estado dentro de la alianza UKUSA le es asignado una responsabilidad sobre el control de distintas áreas del planeta. La tarea principal de Canadá solía ser el control del área meridional de la antigua Unión Soviética. Durante el periodo de la guerra fría se puso mayor énfasis en el control de comunicaciones por satélite y radio en Centro y Sudamérica, principalmente como medida para localizar tráfico de drogas y secuaces en la región. Los Estados Unidos, con su gran cadena de satélites espías y puertos de escucha controlan gran parte de Latinoamérica, Asia, Rusia asiática y el norte de China. Gran Bretaña intercepta comunicaciones en Europa, Rusia y África. Australia examina las comunicaciones de Indochina, Indonesia y el sur de China, mientras que Nueva Zelanda barre el Pacífico occidental. Según algunas fuentes el sistema dispone de 120 estaciones fijas y satélites geoestacionarios. Estos podrían filtrar más del 90 % del tráfico de Internet. Las antenas de Echelon pueden captar ondas electromagnéticas y trasmitirlas a un lugar central para su procesamiento. Se recogen los mensajes aleatoriamente y se procesan mediante los diversos filtros buscando palabras clave. Este procedimiento se denomina "Control estratégico de las telecomunicaciones". *Wikipedia. La enciclopedia libre*, http://es.wikipedia.org/wiki/ECHELON Consultada el 21 de octubre de 2007.

[68] Sánchez Almeida, Carlos, *op cit.*

[69] Entre sus principales funciones están: "Identificación y desarticulación de organizaciones dedicadas al robo, lenocinio, tráfico y corrupción de menores, así como a la elaboración, distribución

acciones preventivas en materia de delitos cometidos en Internet y usando medios informáticos, cuenta con un área específica en materia de prevención y atención de denuncias de delitos contra menores, como existen en los países desarrollados.

Los crímenes cometidos en agravio de menores a través de una computadora y otros medios han tenido un incremento sin precedentes, tanto en México como en el mundo, derivado de la velocidad del desarrollo tecnológico y con las crecientes oportunidades de acceso a Internet. La red ha sido utilizada por organizaciones criminales de pedófilos que promueven y transmiten pornografía infantil; también, se sabe de las operaciones de bandas internacionales de prostitución, que utilizan sistemas informáticos como medio de promoción y sobre todo de reclutamiento. Otro tipo de crímenes que se han incrementado de manera considerable son el fraude cibernético, la piratería de software, la intrusión a sistemas de cómputo, el hackeo, la venta de armas y drogas por Internet y el ciberterrorismo que en los últimos años ha cobrado mayor importancia y es un tema aparte que requiere de un estudio minucioso; sólo por dar un ejemplo debemos citar una amplia investigación que realizó el diario nacional "El Centro"[70] en su edición de lanzamiento, donde se señala que "un informe del Departamento de Justicia de EU, fechado el 5 de septiembre de 2006 confirma que el FBI opera una oficina especial de investigación y lucha antiterrorista desde los atentados de Nueva York, en 2001. El gobierno de México siempre lo ha negado." Pero esto no es lo más alarmante si no la posibilidad que tienen de violar la vida privada de las personas simplemente por creer que tienen alguna relación terrorista, así continúa la nota: "el gobierno mexicano ha permitido a *Verint Technology Incorporation*[71] realizar acciones de espionaje en el territorio nacional,

y promoción de pornografía infantil, por cualquier medio. Localización y puesta a disposición ante autoridades ministeriales de personas dedicadas a cometer delitos informáticos. Realización de operaciones de patrullaje anti hacker, utilizando Internet como instrumento para detectar a delincuentes que cometen fraudes, intrusiones y organizan sus actividades delictivas en la red. Análisis y desarrollo de investigaciones en el campo sobre las actividades de organizaciones locales e internacionales de pedofilia, así como de redes de prostitución infantil". Información de la página de la Secretaria de Seguridad Pública: http://www.ssp.gob.mx/portalWebApp/appmanager/pcibernetica/desk?_nfpb=true&_pageLabel=pcibernetica_page_3&docName=¿Quiénes%20somos?&nodeId=/BEA%20Repository/99424//archivo&pathImg=/BEA%20Repository/import/Policia%20Federal%20Preventiva/Policía%20Cibernética/Conoce%20a%20la%20Policía%20Cibernética/¿Quiénes%20somos?

[70] Hernández, Luis Guillermo, *El vigilante que todo lo ve y lo oye*, "El Centro"; México, lunes 5 de marzo de 2007, pp. 2 y 3.

[71] *Verint Technology Inc*, subsidiaria de *Verint Systems Inc*, es una empresa fundada en 1994 con capital privado en la que participan como accionistas funcionarios y ex funcionarios de Washington, de acuerdo con un reportaje de Robert O´Harrow Jr, del Centro de Reporteros de Investigación de Estados Unidos.

mediante la intervención de líneas telefónicas, lectura de correos electrónicos, navegación en todas las páginas web e intervención en llamadas a celulares en todo el país —cuando el FBI y la Procuraduría General de la República consideren que hay riesgo para la seguridad de Estados Unidos y Canadá".[72] Como podemos observar, la creación de estas policías es benéfica en algunos aspectos pero en otros menoscaba los derechos fundamentales de los ciudadanos, en concreto el derecho a la vida privada Sin embargo, el problema está en que la información que éstos perciben muchas veces ha sobrepasado los límites puramente investigativos y se vuelven verdaderos sistema de persecución que atentan contra el derecho que todo ser humano tiene para no ser perturbado y para que no se conozcan aspectos de su vida que se consideren como íntimos. Es prudente que los Estados, que legítimamente pueden crear órganos para combatir delitos que se cometan con o sin participación de medios de comunicación como Internet, alcancen al momento de desempeñar sus funciones, un equilibrio armonioso entre el legítimo derecho a investigar este tipo de crímenes y el derecho a no intervenir en la vida privada de las personas. Pero en la práctica, estas expectativas parecen poco alentadoras.

A través de los casos recientemente expuestos, surge de pronto una controversia entre algunos derechos constitucionales, vale decir el derecho a la protección de la vida privada y otras garantías como el derecho a desarrollar actividades económicas o el derecho a la propiedad privada, y que se encuentran básicamente arraigadas en quienes desarrollan actividades económicas al parecer lícitas. Ya a finales del siglo XIX, los connotados Warren y Brandeis se habían manifestado respecto de las controversias que tales derechos acarreaban, producto de que muchas veces se falló dando prioridad más a la propiedad que a la privacidad. Por eso es que daban como ejemplo el hecho de que "el principio que protege los escritos personales y toda otra producción personal, no contra el robo o la apropiación física, sino contra toda forma de publicación, no es en realidad el principio de la propiedad privada, sino el de una inviolable personalidad".[73] Pero en la actualidad, el problema ha tenido tanto defensores como detractores.

Dentro de quienes defienden a la vida privada como un bien económico que todos tenemos conjuntamente con otros, está el profesor de la Universidad de Chicago Richard Posner. Para este autor, estos dos bienes no son entendidos como fines en sí mismo, sino como bienes intermedios para lograr otros fines. Desde esta perspectiva, el chileno Hernán

[72] Hernández, Luis Guillermo, *También husmea el FBI*, "El Centro", México, martes 6 de marzo de 2007, pp. 2 y 3.

[73] Posner, Richard, *The Right of Privacy, en Georgia Law Review*, 12(3), 1978, p. 394.

Corral la ha descrito así: "la "demanda por información privada" es comprensible cuando una relación actual o potencial, sea comercial o personal, crea oportunidades de ganar para el demandante, lo que es obvio para el inspector del Servicio de Impuestos, para el novio, para el conviviente, acreedor y competidor, entre otros buscadores de información. Incluso estima comprensible la curiosidad casual por las vidas de amigos y colegas, ya que ella nos permite formarnos una imagen más adecuada de aquellos, y el conocimiento así obtenido es útil en nuestro trato social"[74]

La postura de Posner se sintetiza, básicamente enfocando al derecho a la vida privada sustentado en la eficiencia económica (donde la gente se vendería a sí misma tanto como a sus bienes), y según los siguientes principios: "I) otorgar protección a los secretos de negocios o comerciales por los cuales los hombres de empresas explotan su superior conocimiento o habilidades; 2) no conceder, en general, esa protección a los hechos personales de la gente como mala salud, mal carácter, sobre los cuales no podrá otorgarse un derecho de exclusividad, aunque sí para prevenir su descubrimiento mediante métodos indudablemente intrusivos; 3) limitar, tanto como sea posible, las escuchas comunicacionales y otras formas de vigilancia intrusiva a la vigilancia de actividades ilegales".[75]

Dentro de los detractores de esta postura está Edward Bloustein, quien ha manifestado que el hecho de que el secreto incentive la inversión en la producción de una información socialmente valiosa, se sale del campo meramente económico para expresar un juicio de valor. Así, el estudio de Posner no lograría capturar el significado de la privacidad como un valor final, y no como un instrumento meramente económico:" el mercado nos dice algo sobre la realidad social, pero está lejos de decírnoslo todo, y frecuentemente, está lejos de decirnos lo suficiente".[76]

---

[74] Corral Talciani, Hernán, en *Configuración Jurídica del Derecho a la Privacidad II*, Revista Chilena de Derecho, Vol. 27 No.2, pág.72, Sección Estudios. Dentro de esta postura están incluso aquellos que sostienen que aquella información basada en chismes típica de la prensa sensacionalista tiene también su justificación. "Hay aparentemente muy poca privacidad en las sociedades pobres, donde, consecuentemente, la gente puede fácilmente observar de primera mano la intimidad de la vida de los otros. La vigilancia personal es un lujo en las sociedades ricas, porque la gente vive en condiciones que les proporcionan altas cuotas de privacidad. De tal observación y porque el valor (y por tanto el costo de oportunidad) del tiempo es demasiado grande para merecer una asignación de tiempo para mirar a los vecinos, la gente de las sociedades ricas vio un método alternativo de informarse sobre cómo viven los demás y la prensa lo proveyó. Una función legítima e importante de la prensa es proveer especialización de la curiosidad en las sociedades donde los costos de obtener información han llegado a ser demasiado altos para el fisgón."

[75] Posner, Richard, *The Right of Privacy*, en Georgia Law Review, 12(3), 1978, pp. 399.

[76] *Ibidem*, refiriéndose básicamente a la obra de Bloustein, Edward, *Privacy es dear at any price: a response to profesor Posner' s Economic Theory*, en Georgia Law Review 12, 1978, pág. 440.

Considero prudente, a modo de reflexión, tomar las palabras de Corral, quien como conclusión ha manifestado que "La información personal no puede ser objeto de propiedad en la medida en que no se trata de un objeto ni tangible ni intelectual, y porque su grado de proximidad a la persona misma le otorgan una calidad personalísima que la extrae de las categorías de la comercialidad y del tráfico del mercado".[77] Soy partidario de la postura recién manifestada, ya que no se puede, desde mi punto de vista, poner en riesgo bajo ninguna perspectiva una garantía esencial del hombre por dar cabida a intereses que no se equiparan ni en importancia ni en prioridad respecto de la esencia misma del hombre. Es a raíz de esto que se ha desarrollado en la actualidad justamente una fundamentación postmoderna, inclinada por sobre todo a la defensa de la dignidad humana frente a la amenaza que representan los intereses económicos en este campo. Bien ha dicho Bloustein que "la autoestima que aflora del derecho a la vida privada es un valor único y no susceptible de cambio".[78]

[77] Corral Talciani, Hernán, en *Configuración Jurídica del Derecho a la Privacidad II*, Revista Chilena de Derecho, Vol. 27 No.2, p. 72.

[78] *Ibídem*, p.73.