

"Revolución Informática con Independencia del Individuo"

"SPAM" Y DERECHO. CONSIDERACIONES CRÍTICAS SOBRE LA REGULACIÓN DE LAS COMUNICACIONES COMERCIALES POR CORREO ELECTRÓNICO EN LAS LEYES 19.628 Y 19.946

Renato Jijena Leiva²⁶⁶

SUMARIO: I. *Introducción.* II. *Acerca del envío masivo de correos electrónicos masivos y no deseados o "spam". Consecuencias económicas y su visualización como un problema de conectividad.* III. *El spam desde la perspectiva de los emisores de correos electrónicos, de los receptores y de los intermediarios. Falta de eficacia de las propuestas de autorregulación para emisores, receptores e intermediarios.* IV. *Perú: un modelo legislativo sobre regulación del "spam".* V. *La validación legal del spam en el contexto de la ley sobre derechos de los consumidores (19.496).* VI. *La validación legal del spam en el contexto de la ley sobre tratamiento de datos personales (19.628).*

I. Introducción.

Resulta de interés jurídico el estudio de dos normas legales chilenas, a saber la N°19.496 sobre protección de los derechos de los consumidores y la N°19.628 sobre tratamiento de datos personales, que regulan el mal uso comercial que sistemáticamente se hace en Chile de las direcciones de correos electrónicos.

Esta práctica, en inglés denominada "*spam*" o correo basura, ha devenido en un gran problema de conectividad en el uso de la red Internet, y su origen primario es el tráfico de bases de datos personales con direcciones de correos electrónicos que permite el articulado de la ley 19.628, y en segundo lugar, la opción de enviarlos sin autorización previa del titular de la dirección de correo que permite el artículo 28 B de la ley 19.496.

Con este objetivo dogmático, primero es necesario entender el problema de los correos electrónicos masivos, abusivos y no deseados que se envían con fines de marketing o promoción comercial, denominados con el término inglés "*spam*" o correos basura. Ello, desde una perspectiva técnica y económica²⁶⁷, que permita visualizar las posibles responsabilidades para quienes los envían, para quienes los intermedian o transportan -los llamados proveedores de servicios de conectividad o "ISP" (de *Internet Service Provider*) y para quienes los reciban. Precisamente, el gran defecto de las normas

²⁶⁶ Profesor de Derecho Informático PUCV; Magister (c) Egob UTEM; Postgraduado en Derecho Informático por la Universidad de Zaragoza (España, 1990); Asesor Legal de la Subdirección de Informática del Servicio de Impuestos Internos de Chile.

²⁶⁷ En Chile ya se ha determinado que la práctica del envío indiscriminado de correos no solicitados genera enormes perjuicios a los receptores de dichos correos. La Cámara de Comercio de Santiago los ha cuantificado en aproximadamente 36 millones de dólares al año, y ellos derivan del tiempo necesario para eliminarlos y de los costos de conexión que asume y debe pagar el receptor. Téngase presente que para el emisor la práctica implica el único costo de tener un contrato de arriendo de casilla con un ISP o proveedor de conectividad a la red Internet.

"Revolución Informática con Independencia del Individuo"

citadas es que no consideran opciones que apunten a restringir legalmente el uso del dato personal dirección de correo electrónico y a establecer diversas obligaciones de cargo de los ISP que intermedian entre el emisor y el destinatario de un correo, mismas que en definitiva -y desde el punto de vista orgánico- debieran ser fiscalizadas en Chile por la Subsecretaría de Telecomunicaciones.

Revisadas las consecuencias económicas del *spam* y su visualización como un problema de conectividad, se debe tener presente que el servicio de acceso a Internet constituye un *servicio público de telecomunicaciones*; y que los servicios "*de intermediación*" en materia de conectividad -en general- y de envío y recepción de correos -en particular- que prestan las empresas proveedoras de conectividad o ISP son esenciales para el desarrollo futuro o para el estancamiento de la red Internet.

Desde la perspectiva de los emisores de correos electrónicos, de los receptores y de los intermediarios, llama la atención la falta de eficacia de las propuestas de "*autorregulación*" y existen, por el contrario, modelos de legislación comparada como el de Perú, que han de mostrado idoneidad jurídica y que confirman que el problema debe abordarse en sede del Derecho Positivo. No obstante este y otros modelos similares de normas extranjeras, la validación del *spam* en el contexto de la ley chilena sobre derechos de los consumidores mediante la incorporación el año 2004 de un artículo 28 B, y a pesar de la limitación de que la aplicación de la norma requiere la existencia de una relación entre un proveedor que ofrece comercialmente un producto o un servicio a un consumidor, ha generado la radicalización o un aumento progresivo del problema. Es que resulta, en el hecho, que este artículo 28 B posee una solución de fondo -en síntesis, permitir mandar los correos comerciales sin autorización del destinatario- que no logra hacerse cargo de la complejidad técnica ni de los intereses económicos involucrados.

II. Acerca del envío masivo de correos electrónicos masivos y no deseados o "*spam*". Consecuencias económicas y su visualización como un problema de conectividad²⁶⁸

Una de las prácticas masificada en la red Internet es el envío de correos o e-mails, remitidos sin la autorización del destinatario o receptor de la comunicación electrónica. No existe un concepto unánime del anglicismo "*spam*", pero a efectos de este informe se le concibe como "todo correo electrónico enviado de forma masiva, sin autorización del titular de la dirección o casilla electrónica, obteniéndose las direcciones de correos de fuentes no

²⁶⁸ La perspectiva de la conectividad nace de entender que Internet es una red telemática y un Servicio Público de Telecomunicaciones, que debe ser resguardado a instancias de la SUBTEL y que está amenazado por una serie de prácticas con consecuencias económicas y jurídicas que atentan contra la navegación o la conexión de los usuarios, problemas que, a la larga, pueden atentar contra elementos claves del desarrollo de Chile en materia de iniciativas de Gobierno Electrónico en el Sector Público o de transacciones comerciales tanto en el Sector Privado como en el Público. Tal es el caso de las prácticas de "*spam*", que en países como EE.UU. saturan servidores o sitios WEB y han llevado a desincentivar el uso de los correos electrónicos.

"Revolución Informática con Independencia del Individuo"

públicas de información, y que ocasiona perjuicios económicos al receptor de la comunicación, independientemente de que su contenido se relacione -o no- con una promoción comercial u oferta de servicios”.

El envío indiscriminado de correos electrónicos no solicitados, "*basura*" o "*chatarra*" y generalmente con promociones comerciales, los que saturan casillas de correos electrónicos, es un problema que en sus orígenes utiliza como materia prima -si se nos permite la expresión- el mayor número posible de listas, archivos, ficheros o bases de datos de direcciones de correo electrónico, un dato personal o nominativo *per se*. Eso justifica, creemos, el considerarlo dentro de los tópicos relacionados con la privacidad o intimidad desde la perspectiva de como se ve violentada de la mano de la conectividad a Internet. Lo realmente importante, para solucionar el problema de raíz, es evitar el tráfico de bases de datos personales con datos sobre direcciones de correo electrónico.

No es necesario contar con una definición detallada o unívoca de esta práctica. Tampoco es necesario profundizar en la descripción tecnológica o física de lo que son los correos electrónicos. En ese sentido, resulta obvio entender que se trata de sistemas de comunicación electrónica, informática y telemática y de servicios de mensajería de la misma naturaleza, en los que existe una comunicación diferida y no interactiva entre dos sistemas, uno que lo emite o envía y otro que lo recibe, y que mediante los correos pueden enviarse adjuntos textos, imágenes, datos o archivos con mensajes de voz. ¿A estas alturas del Siglo XXI, alguien podrá decir que no entiende lo que es un correo electrónico?; creemos que no. Lo que no debe hacerse es caer en la simpleza de definírseles como "*todo correo electrónico no deseado, no solicitado o no consentido*" y de creer que así se engloban sus principales características, de partida porque un correo que se envía por ejemplo una única vez no causa perjuicio alguno al destinatario, y porque en definiciones tan simples cabría por ejemplo el caso de que un alumno de derecho o un colega abogado le enviaran un correo a otro abogado para formalizar un contacto, sin que ambos supieran que el destinatario no lo deseaba y no lo consentía, y por cierto sin haberlo solicitado el receptor.

No resulta novedoso además, el afirmar que es con los datos personales que se registran al solicitarse el uso de una casilla o cuenta de correo electrónico como elaborarse un perfil del titular de la dirección (*nombre, domicilio, números de teléfono, profesión, gustos, familia, estudios, etcétera*), lo que se agrava porque además de no haber autorización previa, expresa e informada de la persona individualizada al cederse la información se violenta la privacidad del titular propietario de los datos.

Tampoco resulta original afirmar que "*el dato dirección de correo electrónico*" puede dar a conocer nombres y apellidos de una persona, quizás la zona geográfica de residencia u origen (*pero no necesariamente, porque uno puede usar cuentas de extensión ".cl" sin estar en Chile*), o la empresa o servicio público donde trabaja. Lo que si es totalmente inexacto es afirmar -como se ha hecho- que un dato "*dirección de e-mail*" puede evidenciar o reflejar aspectos delicados de una persona como su inclinación política, religiosa o sexual, salvo que expresamente quien envía el correo mediante una cuenta de por ejemplo un partido político determinado quisiera ser reconocido o asociado

"Revolución Informática con Independencia del Individuo"

a la militancia de ese partido político, lo cual ya no es una fidelización furtiva o clandestina del dato que realiza sin autorización quien recopila las direcciones de correo.

El problema crece -entrando al análisis económico- cuando los costos son financiados por el destinatario que paga por mantener su casilla y asume los gastos de la conexión para recibirlos, lo que ocasiona perjuicios económicos (y no como ocurre en la mayoría de las prestaciones de servicios de telecomunicaciones donde los costos los paga el que inicia la comunicación.); cuando son enviados al amparo del falso argumento de existir una convención internacional que lo permite si se ofrece la posibilidad de eliminarse del listado de destinatarios; y cuando el contestarlos es un mecanismo usado por las empresas -generalmente anónimas- para verificar que las direcciones de correo estén activas, sin que se concrete la remoción ofrecida.

Abordar la regulación de los llamados "spam" se dificulta porque existen diversos actores relacionados, a saber: generalmente un comerciante o prestador de servicios que quiere promocionar sus productos; una empresa emisora que ofrece externalizado el servicio de comercialización on line a los proveedores, y que "trafica" anónimamente y sin estar registrada en parte alguna listas fidelizadas de direcciones de e-mail; un ISP, "*Internet Service Provider*" o proveedor de servicios de conectividad a Internet que intermedia y almacena los correos en las casillas de sus clientes, tanto de emisores como de receptores, sin filtrarlos, sin bloquearlos o sin negarse a distribuirlos; y un titular de una dirección de correo electrónico que lo recibe sin haberlo nunca solicitado.

Las posibles opciones de solución -que normativamente siempre se han considerado en el Derecho Comparado- son dos: o se exige a los emisores que obtengan autorización previa, expresa y para fines específicos del receptor y titular de una casilla de correo electrónico, o se permite su envío obligando a que sea éste último quien soporte los costos de la transmisión y la carga de, posteriormente, manifestar que no desea recibirlos o solicitar su eliminación de la base de datos de quien lo envía.

Los temas de la autorización previa y del uso del dato personal "*dirección de correo electrónico*" para los fines con que el titular ha contratado el servicio con un proveedor de conectividad, no son menores. En Francia, por ejemplo, desviar la finalidad con que se recopiló un dato nominativo como "la dirección de correo electrónico" es delito penal -sancionado con privación de libertad-, y en Chile en cambio, se cree erradamente que publicitar una dirección de e-mail con fines académicos y/o profesionales conlleva una autorización tácita para ser destinatario de promociones comerciales.

Internet no es sino un conjunto mundial de servidores y redes computacionales entrelazados gracias a los llamados "*proveedores de acceso o conectividad*" -que son múltiples- y al uso de un único protocolo de comunicaciones, también conocido como "*la telaraña de la información*". La red permite el intercambio de datos entre los cinco continentes, posibilitando el acceso a todo tipo de contenidos con independencia de la ubicación físico-geográfica de dichos proveedores y sus usuarios. Internet no es una empresa o una organización determinada: se trata más bien de un recurso o medio tecnológico que comparten tanto los proveedores de acceso como los proveedores de aplicaciones específicas (e-mail, diseño de páginas WEB, *e-commerce*, etc.).

"Revolución Informática con Independencia del Individuo"

Internet existe en la medida que las empresas proveedoras de servicios de conectividad permiten el acceso a los múltiples servidores que comparten información. Estas empresas, que en su mayoría son las mismas que prestan servicios de telecomunicaciones de otra naturaleza, actúan comercialmente en un régimen de libre competencia. En cuanto a los servicios que prestan, si bien es cierto no son tan esenciales a esta fecha como los de agua, luz, gas o teléfono, la disminución de la brecha digital mediante la penetración y masificación de la red y a la luz de desarrollos en curso como los de la *Telefonía IP*²⁶⁹ o de VOLP -por sus siglas en inglés, voz sobre protocolo de Internet- harán que pasen a ser esenciales en muy corto tiempo.

A esta fecha no cabe cuestionar, por la naturaleza de la red Internet y la forma en que las empresas prestan los servicios de acceso a la misma, la viabilidad de incluir a los servicios de acceso a la red dentro de la definición que la ley N°18.168 contempla para los servicios públicos de telecomunicaciones. Nada obsta a este enfoque el que por la naturaleza "*de interconexión de hecho*" de la red Internet (un ISP puede conectarse a ella, o no, y si lo hace e interconecta servidores habrá Internet) no sea susceptible de ser concesionado legal y administrativamente como ocurre con la telefonía o los espectros radioeléctricos²⁷⁰.

El artículo 3º señala que "*para los efectos de esta Ley los servicios de telecomunicaciones se clasificarán en la siguiente forma*", y en la letra b) determina que existen los "*Servicios públicos de telecomunicaciones, destinados a satisfacer las necesidades de telecomunicaciones de la comunidad en general*", los que "*deberán estar diseñados para interconectarse con otros servicios públicos de telecomunicaciones*".

Debe tenerse presente que el servicio de acceso a Internet constituye un servicio público de telecomunicaciones; y debe considerarse que los servicios "de intermediación" en materia de conectividad en general y de envío y recepción de correos en particular que prestan las empresas proveedoras de conectividad o ISP son claves en el desarrollo o en el estancamiento de la red Internet. Por lo mismo, no pueden quedar sólo entregados a las

²⁶⁹ En Chile "*la Subsecretaría de Telecomunicaciones ha resuelto regular*" (técnica y administrativamente "*la Telefonía IP, esto es, aquella que permite la transmisión de voz por las mismas redes que utiliza Internet y en la que confluyen los últimos avances en telecomunicaciones e informática. En tanto permite la transmisión de voz, la tecnología IP aparece como una atractiva alternativa al servicio telefónico tradicional, basado en redes físicas, destacando una notoria reducción de los costos asociados a las comunicaciones, por cuanto la duración de la llamada y la distancia de la misma, esenciales para establecer el valor del servicio tradicional, son en este sistema irrelevantes*". El sistema operará mediante una concesión de servicio público de telecomunicaciones de voz sobre banda ancha (SPTVBA), introduciéndose una nueva categoría de concesión y de servicio público de telecomunicaciones diversa de la que se aplica a las concesiones de servicio público telefónico.

²⁷⁰ En este contexto se entienden las normas técnicas administrativas que -para posibilitar el uso eficiente y adecuado de la red y aientar la conectividad a Internet- ha dictado la SUBTEL a esta fecha, las que, salvo error u omisión serían: 1) la Resolución Exenta 1.483, de 22 de octubre de 1999, para fijar el procedimiento y plazo para establecer, publicitar y aceptar interconexiones entre ISP²⁷⁰; 2) la Resolución exenta 669 de 1 de junio de 2001, modificada por la Resolución exenta 1.493 exenta de 12 de noviembre de 2001, que fija indicadores de calidad de servicio de acceso a Internet y sistema de publicidad de los mismos; y 3) la resolución 698 de 30 de junio de 2000, que fija los indicadores de calidad de los enlaces de conexión para cursar el tráfico nacional de Internet y sistema de publicidad de los mismos.

"Revolución Informática con Independencia del Individuo"

reglas del mercado si se constata que la falta de normas legales -generales, permanentes, obligatorias y no discriminatorias- que les asignen derechos y obligaciones específicas a los ISP -esencialmente de filtrado y bloqueo de correos- atenta contra la conectividad y el acceso a la red Internet.

III. El *spam* desde la perspectiva de los emisores de correos electrónicos, de los receptores y de los intermediarios. Falta de eficacia de las propuestas de "autorregulación" para emisores, receptores e intermediarios.

Anticipamos que al abordar la regulación de los llamados "spam" se distinguían diversos actores relacionados, a saber: generalmente un comerciante o prestador de servicios que quiere promocionar sus productos; una empresa emisora que ofrece externalizado el servicio de comercialización on line a los proveedores, y que "trafica" anónimamente y sin estar registrada en parte alguna listas fidelizadas de direcciones de e-mail; un ISP que intermedia y almacena los correos en las casillas de sus clientes, tanto emisores como receptores, sin filtrarlos; y un titular de una dirección de correo electrónico que lo recibe sin haberlo solicitado.

Los principales actores involucrados son el emisor o remitente del correo; el receptor o destinatario; y el ISP o proveedor de conectividad que intermedia y donde están las casillas receptoras de los correos. El emisor puede actuar personalmente (el propio proveedor) o, habiéndose contratado el servicio, operar por encargo de otro. Y el receptor puede querer o no recibir el correo. Y respectivamente ellos pueden reclamar el reconocimiento de su "*derecho de enviar*", de su "*derecho de no recibir*" y de su "*derecho de no distribuir*".

Desde otra perspectiva más amplia o general, se ha consignado que de acuerdo con la regulación efectuada por la SUBTEL sería posible distinguir en Internet la participación de las siguientes entidades: 1) la compañía de telecomunicaciones, que es el concesionario de servicio público telefónico o de servicio intermedio propietario de los medios de transmisión, pudiéndose prestar a través de ellas un servicio de Internet conmutado, o de banda ancha por medios alámbricos o inalámbricos; 2) el ISP o proveedor de acceso a Internet, que es la persona natural o jurídica que presta el servicio de acceso a Internet; 3) el proveedor de contenidos, que es la persona natural o jurídica que pone a disposición de los usuarios contenidos y/o aplicaciones en Internet a través de medios propios o de terceros; y, 4) el usuario, que es la persona natural o jurídica que a través de los servicios de un ISP que intermedia accede a la red de Internet, *en este caso, para enviar o recibir correos electrónicos no solicitados*.

El problema del *spam* suele abordarse sólo desde la perspectiva de la relación entre emisores y receptores, y la discusión suele remitirse a si los primeros requieren o no autorización previa de los segundos para el envío de los correos no solicitados, y si los

"Revolución Informática con Independencia del Individuo"

segundos pueden oponerse en base a un derecho a no recibirlos²⁷¹. Pero esta visión es sesgada y no idónea para solucionar los problemas de conectividad que se generan ni para acotar debidamente esta práctica. Esta es, por cierto, una de las deficiencias de las normas aprobadas en Julio del 2004 en la ley chilena sobre derechos de los consumidores.

Por lo mismo, no pueden quedar sólo entregados a las reglas del mercado si se constata que la falta de normas legales que les asignen derechos -por ejemplo de bloqueo de emisores o de no distribución de correos electrónicos, sean los de sus propios usuarios-clientes o no- y que establezcan responsabilidades y obligaciones específicas -por ejemplo de oferta y uso de sistemas de filtrado- a los ISP atenta contra la conectividad y el acceso a la red Internet.

La "autorregulación" promovida por la SUBTEL y por la entidad gremial que agrupa a los proveedores de Internet -la API- el año 2002 ha resultado ineficaz, debido, fundamentalmente, a que se trata de simples sugerencias o recomendaciones que nadie está obligado a cumplir. Ello es insuficiente frente a los grandes negocios que, a través de este medio, pueden gestarse.

Conceptualmente se trató de indicaciones idóneas, que distinguían también entre los roles de los emisores, de los ISP intermediarios y de los usuarios. Y "culturalmente" están siendo difundidas por la API, la que señala que consisten en una serie de recomendaciones de buenas prácticas para el envío de mensajes publicitarios por correo electrónico, así como para los ISP y los destinatarios, siguiendo lo que estaría siendo la tendencia mundial en el área, y las que ofrece la opción de autorizar a utilizar un sello distintivo a quienes cumplan con las recomendaciones de buenas prácticas.

Dentro de las principales recomendaciones para el buen uso del correo electrónico figura aquella que señala que no se enviarán mensajes publicitarios a destinatarios que no lo hayan autorizado; los destinatarios ya inscritos podrán solicitar, a través de un procedimiento sencillo, ser eliminados de la lista, y que aquellos proveedores de contenidos, productos y servicios que contraten los servicios de una empresa para el envío de correos electrónicos publicitarios, deberán asegurarse que dichas empresas cumplan con las recomendaciones de buenas prácticas.

Reflejando una percepción que con este estudio se busca cambiar, es sintomático que para las recomendaciones de buenas prácticas a las empresas proveedoras de acceso a Internet se contemplen sólo un par de afirmaciones generales, no obstante

²⁷¹ PALAZZI comenta (en la revista *Jurisprudencia Argentina*, tomo 2004, vol II, paginas 1346-1355) que en Estados Unidos la doctrina ha planteado numerosas teorías para fundar el derecho a no recibir correos electrónicos. *"Esta teorías van desde la invasión de privacidad receptada por el common law, hasta la aplicación analógica de la ley destinada a evitar llamados telefónicos molestos. También se han sugerido -sin éxito- reformas legislativas a nivel federal, pero a nivel estatal existen numerosas leyes que prohíben o regulan el spam"*.

"Revolución Informática con Independencia del Individuo"

tenerse en cuenta los graves perjuicios que a ellas les ocasiona el spam²⁷². Una, en cuanto a que los ISP deberán cautelar por la correcta instalación y funcionamiento de los servidores de correo de sus clientes, para evitar el llamdo "open-relay". Otra, para que pongan a disposición de sus clientes, en sus respectivos sitios web o en cualquier otro medio, las condiciones particulares de uso del servicio de correo electrónico que presta cada ISP.

La actuación de los ISP y el rol que ellos asuman, en su calidad de intermediarios entre emisores y receptores de correos electrónicos, es la clave para frenar la penetración y el desarrollo del spam. Creemos que a estas empresas prestadoras de servicios, intermediadoras y distribuidoras de los correos electrónicos cabe exigirles -en el marco de los contratos vigentes- que se adopten concretas medidas de filtrado y bloqueo de las direcciones usadas por emisores de "spam", en el contexto mayor de las obligaciones de seguridad e idónea prestación de servicios que subyacen en la celebración de un contrato de arriendo de una casilla o cuenta de correo electrónico²⁷³.

V. Perú: un modelo legislativo idóneo sobre regulación del "spam"

El día 12 de abril del año 2005 fue publicada en Perú la Ley 28.493, que en apenas 10 artículos *"regula el uso del correo electrónico comercial no solicitado (SPAM)"*, ley que parece tutelar el derecho a decidir qué correos electrónicos comerciales se deben recibir y cuáles rechazar, y que busca diferenciar lo permisible y lo no permisible en la recepción de correos electrónicos no solicitados. De esta manera, el Perú ha definido acciones concretas en la regulación a nivel nacional del *spam*, a través de un cuerpo legislativo específico^{274, 275}.

²⁷² Se indican: 1) aumento del tráfico de correo y por ende mayor utilización de Ancho de Banda (BW), lo cual afecta a los clientes por medio de un acceso más lento (menor ancho de banda disponible) y obligaría al ISP a contratar más Ancho de Banda; 2) aumento de la utilización de recursos en plataforma de correos; 3) aumento del encolamiento de correos, lo cual impacta en la capacidad de procesamiento (CPU), Discos y Memoria de Servidores; 4) aumento de conexiones concurrentes, lo cual impacta en la capacidad de procesamiento (CPU), Memoria y Ancho de Banda (BW); 5) bloqueo de direcciones IP por parte de organismos internacionales, tanto para los servicios del ISP como para los clientes, por medio de las llamadas "listas negras", lo que implica aumentar los esfuerzos de supervisión y operación; 6) aumento de los reclamos por Spam, lo cual impacta en el costo y operación del personal de Call Center, operaciones y/o soporte; etcétera.

²⁷³ Si ellos son partícipes coadyuvantes del cumplimiento de las nuevas normas que tutelen el dato personal "dirección de correo electrónico"; si ellos son obligados a ofrecer sistemas de filtrado a sus usuarios o clientes; si ellos implementan dichos sistemas en sus servidores o donde se alojan las casillas de emisores y receptores; si ellos son facultados para dar de baja a usuarios que generan spam y a spammers encubiertos; y si se agrupan bajo un código de conducta que con la obligatoriedad de una norma legal -no en sede de "autorregulación"- los lleve a estar constantemente intercambiando información sobre quienes actúen como spammers, el problema podría controlarse o al menos minimizarse. En este ámbito, por cierto, no existen las soluciones definitivas.

²⁷⁴ Véase en la URL <http://www.habeasdata.org/Peru-multa-por-spam?PHPSESSID=26c1cfaed4daf2095e6ac8529d4725c4> como esta normativa ya ha sido eficazmente aplicada. El año 2007 se aplicó la primera multa a un *spammer* en ese país, luego de un proceso que duró 6 meses la cabo del cual el "INDECOPI" emitió una resolución sancionadora. La decisión final de la comisión

"Revolución Informática con Independencia del Individuo"

El artículo 1° establece que el objeto de la ley es regular el envío de comunicaciones comerciales publicitarias o promocionales no solicitadas, realizadas por correo electrónico, pero *"sin perjuicio de la aplicación de las disposiciones vigentes en materia comercial sobre publicidad y protección al consumidor"*.

El artículo 2° contiene cuatro definiciones, a saber, correo electrónico²⁷⁶, correo electrónico comercial²⁷⁷, proveedor del servicio de correo electrónico²⁷⁸, y dirección de correo electrónico²⁷⁹.

El artículo 3° establece tres *derechos de los usuarios*, a saber: (i) rechazar o no la recepción de correos electrónicos comerciales; (ii) revocar la autorización de recepción, salvo cuando dicha autorización sea una condición esencial para la provisión del servicio de correo electrónico; y, (iii) que su proveedor de servicio de correo electrónico cuente con sistemas o programas que filtren los correos electrónicos no solicitados (materia que en Argentina, por ley, también es obligatorio que sea proveído para el caso del filtrado de contenidos no deseados).

El cuarto artículo, a consecuencia del anterior, alude a una *obligación expresa de cargo del proveedor* que esté domiciliado en el Perú, concretamente, contar con sistemas o programas de bloqueo y/o filtro para la recepción o la transmisión que se efectúe a través de su servidor de los correos electrónicos no solicitados por el usuario.

El artículo 5° definió los tres *requisitos que debe contener todo correo electrónico comercial, promocional o publicitario no solicitado, originado en el Perú*: (i) la palabra "publicidad", en el campo del asunto o *subject* del mensaje; (ii) el nombre o denominación social, domicilio completo y dirección de correo electrónico de la persona natural o jurídica que emite o envía el mensaje; y, (iii) la inclusión de una dirección de correo electrónico válido y activo de respuesta para que el receptor pueda enviar un mensaje para notificar su voluntad de no recibir más correos no solicitados o la inclusión de otros mecanismos

que aplicó una multa de 5 Unidades Impositivas Tributarias (app. 5,400 dólares americanos), se fundó en la infracción tanto a la ley que regula el uso del correo electrónico comercial no solicitado como a la Ley de Protección al Consumidor; le ordenó de oficio, como medida correctiva, que cumpliera con abstenerse de enviar correos electrónicos comerciales a la dirección de correo del denunciante; y, ordenó que se cumpliera con la adecuación del envío de sus correos electrónicos comerciales a las normas vigentes en materia de regulación de correos electrónicos comerciales no solicitados.

²⁷⁵ Llama la atención que el artículo 9° de la ley determinó que la "Autoridad Competente" para conocer las infracciones sería el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual o INDECOPI, actuando a través de una "Comisión de Protección al Consumidor y de la Comisión de Represión de la Competencia Desleal".

²⁷⁶ *Todo mensaje, s se considera correo electrónico la información contenida en forma de remisión o anexo accesible mediante enlace electrónico directo contenido dentro del correo electrónico.*

²⁷⁷ *Todo correo electrónico que contenga información comercial publicitaria o promocional de bienes y servicios de una empresa, organización, persona o cualquier otra con fines lucrativos.*

²⁷⁸ *Toda persona natural o jurídica que provea el servicio de correo electrónico y que actúa como intermediario en el envío o recepción del mismo*

²⁷⁹ *Serie de caracteres utilizados para identificar el origen o el destino de un correo electrónico.*

"Revolución Informática con Independencia del Individuo"

basados en Internet que permita al receptor manifestar su voluntad de no recibir mensajes adicionales.

El *artículo 6°* establece cuatro presunciones legales (admiten prueba en contrario, por ende) de *casos en los cuales el correo electrónico comercial no solicitado será considerado ilegal*: (i) cuando no cumpla con alguno de los requisitos establecidos en el artículo 5° de la ley; (ii) cuando contenga un nombre falso o información falsa que se oriente a no identificar a la persona natural o jurídica que envía el mensaje; (iii) cuando contenga información falsa o engañosa en el campo del asunto o *subject*, y que no coincida con el contenido del mensaje; y, (iv) cuando se envíe a un receptor que haya formulado el pedido para que no se envíe dicha publicidad, luego del plazo de dos días.

Otras presunciones, relacionadas con la infracción del artículo 6°, son establecidas por el *artículo 7°*. La norma citada señala que se considerarán responsables de las infracciones, y que deberán compensar al receptor de la comunicación (i) todas las personas que envíen correos electrónicos no solicitados conteniendo publicidad comercial; (ii) las empresas o personas beneficiadas de manera directa con la publicidad difundida; y, (iii) los intermediarios de correos electrónicos no solicitados, tales como los proveedores de servicios de correos electrónicos.

La norma peruana, por último, establece expresamente en el *artículo 8°* un *derecho a compensación pecuniaria* para el receptor de un correo electrónico ilegal, que puede accionar por la vía del proceso sumarísimo contra la persona que lo haya enviado. Esa compensación pecuniaria será equivalente al uno por ciento de la *Unidad Impositiva Tributaria* por cada uno de los mensajes de correo electrónico transmitidos en contravención de la presente ley, con un máximo de dos *Unidades Impositivas Tributarias*.

V. La validación legal previa del spam en el contexto de la ley chilena sobre derechos de los consumidores. Errada opción de fondo y limitantes derivadas del ámbito de aplicación de la ley

No es suficiente abordar el problema en el contexto de la ley de derechos de los consumidores, como se ha propuesto y aprobado a esta fecha en Chile mediante la ley 19.955 de Julio del año 2004, modificatoria de la ley 19.496, toda vez que suele no darse entre el emisor del correo electrónico no deseado, invasivo y perjudicial y el receptor del mismo, una relación de aquellas generadas entre proveedores y consumidores que se regulan en el contexto del derecho de los consumidores.

Dicho de otra forma, los e-mails que saturan las casillas o buzones de correo electrónico pueden no contener ofertas, promociones comerciales o publicidad engañosa y no ser emitidos por proveedores que ofertan un bien a cambio de un precio.

La nueva ley chilena sobre derechos de los consumidores contempla el siguiente artículo 28 B, inciso primero:

"Toda comunicación promocional o publicitaria enviada por correo electrónico deberá indicar la materia o asunto sobre el que versa, la identidad del remitente y

"Revolución Informática con Independencia del Individuo"

contener una dirección válida a la que el destinatario pueda solicitar la suspensión de los envíos, que quedarán desde entonces prohibidos".

Al optarse por esta regulación se omitió considerar detalles prácticos, como el hecho frecuente de que si uno solicita ser removido no se hace sino comprobar al emisor que el receptor tiene la casilla activa, al solicitar ser removido aparece una dirección que lleva a registrarse en una base de datos de un país extranjero en donde ninguna posibilidad tiene de ser aplicada la ley chilena.

Este criterio obedeció además a consideraciones económicas ajenas al problema del "spam" (a saber, permitir la promoción comercial por esta vía de las pequeñas y medianas empresas), y puede resumirse en que se ha permitido por ley que se generen cientos de "primeros envíos" de ofertas de distintos productos y desde direcciones diversas, con la posibilidad sólo teórica de ofrecer una posibilidad de removerse que siempre es ineficaz.

No obstante el marketing que sobre las bondades de la norma que acoge el *optout* realiza el propio SERNAC²⁸⁰, se trata de una declaración teórica carente de idoneidad práctica y que no constituye una solución al problema de fondo. El Servicio del Consumidor le pregunta a los consumidores chilenos si ellos sabían que a partir de la aprobación de la Nueva Ley del Consumidor el envío de correos electrónicos no deseados está regularizado. Agrega que ellos cuentan con medios para protegerse frente a los correos publicitarios no solicitados o spam; que la ley del Consumidor obliga a todo aquel que envíe una comunicación promocional o publicitaria por correo electrónico a indicar la materia de que se trata en el encabezado (porque así se permite -dice el SERNAC- a quien recibe un correo eliminarlo sin necesidad de abrirlo cuando la materia no es de su interés), a identificar quién envía el correo y a establecer una dirección válida a la que pueda solicitarse la suspensión de los envíos; y que solicitada que sea la suspensión si el envío de los correos persiste el remitente puede ser castigado con multa de hasta 50 UTM (un millón y medio de pesos app.), sanción que también procede si el correo original no cumple con los requisitos señalados o, particularmente, es anónimo.

Se olvida que el sólo hecho de recibirlo importa un perjuicio económico para el destinatario, porque copa conexión y porque quita tiempo eliminarlos; que el 90% de los correos no contienen direcciones válidas de remoción, sino que ellas sólo confirman que la casilla está activa; que cuando un receptor solicita la remoción, no tiene como confirmar que ella se realice efectivamente; que el 90% de los correos no tienen la información necesaria para presentar un reclamo ante el SERNAC, porque provienen de casillas gratuitas tipo *www.latinmail.com*, *www.hotmail.com* y porque sólo indican un teléfono celular de contacto (y casi nunca la individualización de quién envía el correo permite saber qué proveedor está detrás, su nombre, domicilio, actividad, representantes, teléfonos y otros datos relevantes).

Las acciones legales que se han presentado invocando la infracción del artículo 28 B de la ley también demuestran su ineficiencia, concretamente, el que se contempla

²⁸⁰ Véase la URL <http://www.sernac.cl/consejos/especiales.asp?cod=1002&CodArea=7>

"Revolución Informática con Independencia del Individuo"

sancionar sólo a quien directamente realiza la promoción y no al empresario o prestador de servicios que la encarga. Así ocurre con el caso de una famosa multitienda, que no obstante haber sido beneficiada con promociones navideñas que recibimos en nuestras casillas, alegó ante el tribunal de Policía Local que la campaña de marketing por e-mail no había sido realizada por ella sino que por otra empresa distinta, lo que se probaba porque la emisora de los correos no usó direcciones de correo con la extensión de la multitienda.

Sólo a modo de comentario. Este artículo 28 B también alude a los llamados telefónicos promocionales, y establece que al realizarse debe ofrecerse a quien contesta el teléfono la opción de ser removido de la base de datos. La diferencia con los correos electrónicos promocionales deriva de que parte de la gente que es contactada por teléfono son clientes (actuales, vigentes y/o activos) o militantes de las organizaciones que realizan o encargan los llamados y que los contactan (empresas, partidos políticos, etc.), mismas que -a diferencia del spam- asumen el costo monetario de la llamada²⁸¹. Por ende, esta estrategia de marketing telefónico de salida o *outbound* no debería ser considerada como "intrusiva" sino más bien como "*de retención*" -un mecanismo de información y comunicación que ayuda a mejorar el conocimiento del cliente y de la relación propiamente tal-. Incluso los militantes de un partido político también podrían caer en esta categoría, en la que por ende no se requeriría autorización previa. El problema se genera para aquellos que no son clientes o militantes de las respectivas instituciones, donde evidentemente se está tratando de conquistar a un nuevo integrante y por ende de crear y mantener una relación de más largo plazo "*sin su permiso*".

VI. La validación legal del *spam* en el contexto de la ley sobre tratamiento de datos personales (19.628)

1. Las implicancias y menoscabos para la privacidad o intimidad de las personas devienen mayoritariamente del mundo "on line" o de las redes del literaria y sociológicamente llamado "ciberespacio", en particular de Internet y concretamente en consideración al dato personal y nominativo "dirección de correo electrónico". Hoy, en el contexto de Internet, el problema se ha masificado. Este es el antecedente -el elemento de conectividad y la existencia de múltiples, dispersos y desconocidos "responsables de bases de datos" que anónimamente procesan direcciones de correo electrónico-, que debe llevar a la formulación de propuestas sobre concretas modificaciones y adaptaciones a la norma que en Chile pretende regular el uso -para proteger- y sancionar el abuso en materia de procesamiento de datos personales o nominativos.

Como dijimos al inicio de este estudio, el envío indiscriminado de correos electrónicos no solicitados con promociones comerciales es un problema que en sus orígenes utiliza como materia prima el mayor número posible de listas, archivos, ficheros o bases de datos de direcciones de correo electrónico, un dato personal o nominativo *per se*, lo que justifica considerarlo dentro de los tópicos relacionados con la privacidad o

²⁸¹ Téngase presente: en las Campañas de e-mail marketing con permiso (opt-in e-mail), parte del costo lo asume el receptor del mensaje quien recupera los e-mails desde el servidor de correos y para lo cual es necesario conectarse a Internet.

"Revolución Informática con Independencia del Individuo"

intimidad desde la perspectiva de como se ve violentada de la mano de la conectividad a Internet.

Lo realmente importante, para solucionar el problema de raíz, es evitar el tráfico anónimo de bases de datos personales con datos sobre direcciones de correo electrónico, porque en caso contrario, será mera teoría que el derecho genere la existencia de un ámbito del resguardo del derecho del usuario, persona natural o empresa, para poder optar por consentir y autorizar previamente, o no, en que se use su dato personal o atributo "dirección de correo electrónico" (el elemento clave del problema) para hacerlo destinatario de estos correos no solicitados.

Ocurre que el llamado *opt out* o el envío permitido a priori, sujeto a la obligación de ofrecer la posibilidad de ser borrado, no evita que se envíen correos anónimos, no evita que los costos del negocio (el franqueo del correo) lo sigan asumiendo los consumidores, y le sigue traspasando una carga injusta a los receptores de los correos, mismos que se encuentran con las vitrinas de las ofertas en el interior de su PC (lo que constituye "invasión de propiedad") sin que lo hayan querido.

A todo lo dicho debe agregarse la afirmación carente de fundamento, que entiende que por el hecho de publicarse una dirección de correo electrónico en un sitio de la red Internet se contaría con una autorización tácita para que ella sea utilizada para el envío de correos promocionales no solicitados, lo que en toda ley de protección de datos constituye una abusiva e improcedente "desviación de los fines" -por ejemplo laborales o académicos- en consideración a los cuales ellos son publicados.

2. La ley 19.628 sobre protección de datos personales y vigente desde el año 1999, no permite un adecuado equilibrio entre el Derecho a la Privacidad y el Derecho a la Información de las personas naturales y jurídicas.

Concretamente, no permite que los titulares de los datos o antecedentes personales y nominativos que se "tratan" -en términos de la ley 19.628- o "procesan computacionalmente", controlen y autodeterminen el uso que otros, en forma irresponsable y generalmente con fines de lucro, les dan.

Lo anterior, sumado a la inexistencia de un registro de bases de datos personales - como las direcciones de correos electrónicos- y a la no consagración de la obligación legal de que los responsables de bases de datos informen de lo que procesan y almacenan al menos una vez al año a los titulares, son las reales causas de que los chilenos permanezcan ajenos al mecanismo de Habeas Data que -teóricamente en definitiva- establece el artículo 12 de la ley 19.628.

Atendido el anonimato que se genera en Chile en materia de procesamiento de datos al no existir un registro de los que la ley 19.628 califica de "responsables", se hace ilusorio el ofrecer la posibilidad -conforme al artículo 16- de accionar ante los tribunales después de transcurridas 48 horas siguientes al eventual requerimiento de eliminación, actualización o modificación de datos.

"Revolución Informática con Independencia del Individuo"

La Ley chilena N°19.628 establece que en esencia, existen "datos personales" o nominativos que le pertenecen a sus titulares y que son "tratados" manual o automatizadamente, tanto por órganos públicos como por empresas o personas particulares, a quienes la ley califica como "responsables del registro o banco de datos".

La regla general formalmente declarada por el texto legal es que dicho "tratamiento de datos personales" sólo puede hacerse en virtud de autorización legal o del titular de los datos, pero del contexto de las normas se desprende que la mayoría de los datos provienen de "fuentes de acceso público" (por lo cual no se requiere de autorización para su tratamiento) y se consagran -como veremos- importantes y amplias excepciones sobre todo en materia de datos "personales-patrimoniales", lo cual transforma a la regla general en una mera declaración de principios.

El mecanismo de resguardo recogido parcialmente del Derecho Comparado se denomina "Derecho de Acceso" o "Habeas Data", y éste, después de ejercerse ante quien aparezca como responsable del banco de datos -si es que se tiene la suerte de ubicársele porque generalmente actúan en el anonimato- sólo puede reclamarse ante los tribunales ordinarios de justicia y no ante una autoridad administrativa.

3. Existe en esta normativa la necesidad de conciliar el conflicto que se presenta entre dos garantías individuales y de rango constitucional. A saber, por un lado el derecho a la intimidad, tanto en cuanto datos personales o nominativos, sensibles o no, procesados computacionalmente, y por otro el derecho a la información que reclama la sociedad toda²⁸².

En el contexto de los sistemas informáticos y las bases de datos, por un lado está el legítimo interés de aquellas personas cuyos datos nominativos se procesan computacionalmente, en resguardar su vida privada y la necesaria confidencialidad de antecedentes como sus creencias religiosas, su filiación política, sus tendencias sexuales, su estado de salud, el monto de su patrimonio, las direcciones de correo electrónico, etc.

Por el otro, el interés -también legítimo- que poseen los gobiernos y los particulares para acceder a cierta información: los gobiernos, para cumplir con sus fines promocionales y asistenciales de orden público, como por ejemplo saber quienes tienen SIDA al momento de fijar políticas de salud; y los particulares, generalmente constituidos en empresas de servicios o entidades gremiales, que para asegurar la vigencia de un orden público económico necesitarán conocer los antecedentes comerciales irregulares o negativos de las personas que actúan en la vida comercial²⁸³.

²⁸² Se ha sostenido desde hace años que el abuso de las posibilidades computacionales constituye la amenaza por excelencia contra la intimidad, porque detentándose un enorme cúmulo de datos y cruzándose telemáticamente datos personales o nominativos, puede obtenerse un perfil determinado de las personas cuyos antecedentes son procesados. Esta imagen inmaterial debe ser resguardada porque puede ser creada errada o dolosamente, lo que eventualmente se traducirá en discriminaciones, en la imposibilidad de ejercer algún derecho, o en la pérdida de algún beneficio.

²⁸³ ¿Cómo conciliar el Derecho a la Información con el Derecho a la Intimidad?, o ¿cómo equilibrar por un

"Revolución Informática con Independencia del Individuo"

En el contexto referido, no se prohíbe expresamente que el tráfico previo y no autorizado de enormes listas y bases de datos con direcciones de correos electrónicos es un elemento que debe acotarse, porque se encuentra a la raíz del problema.

En el contexto referido, la dirección de correo electrónico de cada persona natural o jurídica es uno de sus datos personales y sensibles que le pertenecen e individualizan a una persona en la sociedad -es un atributo de su personalidad- y por ende debe poder ser autodeterminado y controlado por sus titulares²⁸⁴.

La ley 19.628, en concreto, no contempla una exigencia expresa, ya no en el contexto de la ley 19.496 sino que en el ámbito de la protección de datos personales, de que se requiera la autorización de la persona o empresa que sea el propietario de la casilla y el titular de la dirección de correo electrónico, por ejemplo cuando se consiente voluntariamente en registrarse y en aceptarse el envío de mensajes publicitarios al inscribirse en alguno de los sitios o foros de la red Internet.

La ley en comento, posee "*una válvula no cerrada*" que constituyen los artículos 2° y 4° de la ley 19.628; no prohíbe interpretar el hecho de que por estar en Internet pueda entenderse que una dirección de correo electrónico es pública y que se consiente su tratamiento con fines abusivos y de envío de spam; no prohíbe la confección y comercialización sin autorización de listas de direcciones de correos electrónicos; y no otorga mecanismos de resguardo jurídico a los representantes legales de las personas jurídicas.

El artículo 2° establece -ampliamente, a diferencia de toda la legislación comparada- que para los efectos de la ley se entenderá por "*fuentes accesibles al público*" a los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes.

El artículo 4°, aunque sienta como regla general que el tratamiento de los datos personales sólo puede efectuarse cuando la ley u otras disposiciones legales -que sería el caso de la ley 19.496- lo autoricen o el titular consienta expresamente en ello, dispone que no se requiere de tal autorización cuando el tratamiento de datos personales sea respecto de aquellos que provengan o que se recolecten de fuentes accesibles al público,

lado la máxima libertad o acceso a la información con un adecuado resguardo de la privacidad?. "*LA RESPUESTA DOCTRINARIA*" ha sido la formulación de un nuevo concepto del Derecho a la Intimidad, que surge frente a la llamada o reclamada Libertad Informática o de procesamiento de datos personales-nominativos; que deja de lado el enfoque individualista o negativo con que fue concebido para plantearse desde una perspectiva socializadora y positiva (ya no es "el derecho a ser dejado a solas"); y que se concibe como la posibilidad de que los ciudadanos titulares y propietarios de los datos que les conciernan controlen el uso y el eventual abuso de los antecedentes que a su respecto sean recopilados, procesados, almacenados y cruzados computacional y telemáticamente. "*LA RESPUESTA LEGISLATIVA*" ha sido la promulgación de las llamadas leyes de protección de datos, y Chile no ha estado ajeno a ese proceso.

²⁸⁴ Debe entenderse que existe una desigualdad, desproporción o brecha, entre los titulares de los datos personales que aspiran a controlar y autodeterminar el uso con fines de lucro de sus antecedentes y las empresas y entidades -verificadoras de datos, *head hunters*, agencias de marketing directo, etcétera - que cuentan a su favor con normas que amparan sus prácticas.

"Revolución Informática con Independencia del Individuo"

"cuando... sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios".

Teniendo presente que el dato personal dirección de correo electrónico es el elemento clave para la existencia de "spam" o de correos masivos no solicitados -en su mayoría conteniendo promociones comerciales-, la normativa llamada por su naturaleza a regular su uso no pone coto legal a esta práctica, en esencia, porque los titulares de los datos personales no están facultados controlar y autodeterminar el uso y evitar el abuso del dato personal o nominativo denominado "dirección de correo electrónico".