

## Algunas notas sobre el spamming y su regulación

Fuente: <http://www.alfa-redi.org/rdi-articulo.shtml?x=6102>

**Abstract:** El spamming o en español “envío de correo electrónico no solicitado” se ha convertido en fuente inagotable de ideas encontradas respecto de su regulación legal. En un extremo se propone la autorregulación del mercado y su utilización casi irrestricta, con fundamento en la necesidad del desarrollo de los negocios en Internet. En el otro extremo, se reclama su prohibición mas completa, en tanto se lesiona la privacidad e intimidad como derechos básicos de la persona.

Nuestro comentario comienza con una breve nota sobre la concepción del spamming, su evolución y utilidad. Luego transitaremos por los inconvenientes generados a partir de casos judiciales que han sido resueltos en diferentes países. Posteriormente centraremos la atención en el análisis de la normativa vigente en diferentes países para concluir con una necesaria opinión sobre la procedencia de la regulación del spamming en nuestro ámbito.

Por [Favio Farinella](#),

### I- Introducción

Es tal vez repetido mencionar que corría 1993 cuando dos abogados norteamericanos, Laurence A. Canter y Martha S. Siegel, especialistas en migraciones, utilizaron masivamente los mensajes de correo electrónico para ofertar sus servicios de asesoría a aquellas personas potencialmente interesadas en obtener la “green card”. Esto fue juzgado negativo por la sociedad, los destinatarios denunciaron el hecho lo que les valió a los abogados la interrupción de su servicio de Internet, su desafiliación como barristers en el Estado de Arizona y posteriormente una mas que importante cantidad de dinero al publicar un libro donde explicaban cómo lo habían hecho.[1]

Vemos que el spamming como conducta pasible de regulación jurídica es básicamente un tema actual.

Utilizaremos el verbo en gerundio inglés “spamming” y el sustantivo “spam” en función de la ya universalización del término, que resulta de combinar “(s) piced (p)ork” y “h(am)”, un producto a base de carne de cerdo, enlatado, al que hacía referencia un sketch televisivo del famoso grupo satírico británico “Monty Phyton”. [2] El spam es el correo electrónico que se envía sin que haya sido solicitado, en tanto el spamming es la acción de enviar este correo con diferentes fines, aunque el comercial es la mayor parte de las veces, prioritario. El diccionario Merrian Webster incluye el término desde 1994 y brinda su definición que concuerda con lo dicho.[3]

Existe consenso en considerar que un mensaje puede ser considerado spam si posee al menos una de estas condiciones: (a) no permite al destinatario dar de baja a futuro la suscripción; (b) el remitente es una persona difícilmente identificable; (c) en caso de envíos periódicos, éstos se realizan sin previa suscripción; (d) idéntico mensaje es enviado en forma masiva a personas que no lo han solicitado.

¿Y por qué estamos hablando de él?. Pues bien, también existe acuerdo en considerarlo un problema: (a) para los destinatarios porque les implica tiempo de trabajo y de

conexión leer mensajes que no les interesan en absoluto y luego descartan; (b) para los proveedores de servicios de Internet que reciben quejas de los usuarios y que además como luego veremos son responsabilizados y potencialmente penados por permitir o no controlar este tipo de envíos; y (c) para los propios spammers, que alegan que ciertas regulaciones que prohíben los envíos, coartan su libertad de comercio, expresión y ejercicio de industrias lícitas, en tanto cualquier persona puede ofrecer sus productos por la calle, o telefónicamente sin recabar previo permiso.

Sin embargo, es bueno conocer que esta plaga ocupa entre la mitad y las tres cuartas partes de todo el correo electrónico que se envía en el mundo. Time is money: el tiempo es dinero. He aquí el problema.

Argentina ocupa un lugar de “dudoso honor”, ya que es uno de los primeros productores mundiales de correo electrónico - basura. Se calcula en España que casi la mitad del spam que satura las casillas de correo proviene de Argentina y la organización internacional Spamhaus ubica al país sudamericano en el quinto lugar mundial de generadores de “correspondencia basura”. [4]

## II- Inconvenientes y soluciones

Tecnológicamente, el correo electrónico fue diseñado para permitir una comunicación fluida, sencilla y a bajo costo. En este sentido no discrimina entre mensajes solicitados o no solicitados. Nació aquí la idea de utilizar este medio para ofertar productos en forma masiva a un costo casi inexistente si se lo compara con los medios de publicidad tradicionales.

La Comisión de la Unión Europea, en una Comunicación del 22/01/2004, señala que el spamming constituye un problema que afecta varias esferas: “intimidación, fraude a los consumidores, protección de los menores y de la dignidad humana, costes suplementarios para las empresas, pérdida de productividad. Más en general, el fenómeno socava la confianza de los consumidores, algo indispensable para el éxito del comercio electrónico, de los servicios en línea e incluso, de la sociedad de la información”. Indica además que este fenómeno “ha alcanzado proporciones inquietantes y podría inducir a los usuarios actuales de mensajes electrónicos o SMS a dejar de utilizar el servicio de correo electrónico –que es una de las aplicaciones más populares de Internet– o los servicios móviles, o a utilizarlos de manera más restringida.” [5]

Sin embargo, antes que la prohibición lisa y llana, la vía pertinente parece constituirse en la regulación legal que permita y controle efectivamente. Si consideramos otras utilidades del correo electrónico, hallamos que trasciende el uso publicitario y comercial que es el considerado perjudicial. Así, Internet ha desarrollado un red intangible de contactos y afinidades que trasciende fronteras y elude censuras de todo tipo. La prohibición absoluta del envío masivo de correo podría ciertamente ser utilizada para silenciar campañas a favor de los fines mas loables dentro de las cuales se encuentran la defensa y promoción de derechos humanos, sobre todo en aquellos países donde la censura oficial solo puede ser burlada a través de Internet.

En este sentido, rescatamos una nota de Diciembre de 2003 en una revista jurídica [6], donde se afirmaba que el proveedor de servicios le había prohibido al medio “utilizar sus servicios para enviar copias de un mensaje no solicitado, sea cual fuese su contenido

o finalidad a más de 30 destinatarios en el curso del día". En la misma nota y a manera de queja se mencionaba que se "destruirá la red de comunicaciones espontáneas que permitió en su momento organizar cacerolazos y otras formas de manifestación social, recibir advertencias sobre trampas de las concesionarias de los servicios públicos, campañas de esclarecimiento sobre la degradación ambiental, desastres ecológicos, búsqueda de niños, aportes para trasplantes urgentes..."

Podemos dividir las soluciones en "físicas y técnicas" y las de "corte jurídico". Si bien en nuestro comentario nos ocuparemos de estas últimas, existen también respuestas pensadas por los cuadros técnicos (ingenieros, licenciados) que no se limitan a esperar la aprobación de una norma y luego su puesta en práctica. A este fin, la estrategia básica para filtrar el correo basura que se encuentra disponible en casi todos los programas y servicios de correo, consiste en la confección de "listas blancas" de personas conocidas que están registradas en nuestro directorio y "listas negras". Los envíos de las primeras se aceptan y los de las segundas se rechazan.

Otra potencial solución es la idea de crear un "sello" informático, que pondría un precio a cada mensaje electrónico enviado, tal como ocurre con la correspondencia epistolar. Microsoft dio detalles sobre el proyecto, llamado "Penny Black", en referencia al sello que se introdujo en Gran Bretaña en el siglo XIX, el primer método que obligaba a pagar al remitente de las cartas. En lugar de pagar con dinero, se sugiere que el remitente pague con los segundos que emplearía en resolver una sencilla ecuación matemática. La fórmula causaría un gran trastorno a los spammers, ya que tendrían que utilizar equipos informáticos adicionales. En este sentido, Bill Gates a través de Microsoft, dueño de los servicios de correo electrónico MSN y Hotmail, formalizó ya una alianza con America Online (AOL), Earthlink y Yahoo para explorar y coordinar una estrategia "anti-spam" a escala global.

Es bueno conocer este detalle al momento en que cada estado intenta aisladamente a través de su normativa interna, detener este inconveniente global. A problemas globales, soluciones globales y control e instrumentación local.

### III- Una perspectiva sociológica

Estados Unidos es el país que genera mayor cantidad de correo basura o spam en el mundo, donde como ya dijimos Argentina aparece en un "decoroso" quinto lugar.[7] Es por esto que su jurisprudencia y normativa es la mas antigua y desarrollada en el tema. Existen normas anti – spam tanto propias de los Estados de la federación como también una ley federal reciente que regula la materia. Sólo a título de ejemplo, en el Estado de California, la ley anti-spam asume como delito penal a los mensajes publicitarios no deseados. Es por esto que comenzamos con una referencia a la jurisprudencia norteamericana.

En primer lugar, la causa a la que es obligatorio hacer referencia es Washington v. Heckel.[8] Este proceso enfrentó al Estado de Washington y Jason Heckel, un ciudadano de Oregon que actuando en representación de su empresa "Natural Instincts", había enviado entre cien mil y un millón de mensajes publicitarios a direcciones de correo electrónico obtenidas utilizando el programa "Extractor Pro". Los mensajes ofertaban una obra de Heckel ("How to Profit from the Internet", cómo sacar provecho de Internet) que podía ser adquirida en línea a 39,95 dólares norteamericanos. El Estado de Washington demandó a Heckel por infracción de la legislación anti-spam local en

vigor desde 1999, y según la cual, se considera ilícito el envío de mensajes utilizando direcciones que ocultan la identidad del remitente, así como aquellos que contienen información falsa o engañosa en el encabezado. Éste había sido el modus operandi de Heckel, quien refirió haber realizado entre treinta y cincuenta ventas mensuales de su producto.

La Corte Suprema de Washington tuvo la última palabra, en tanto Heckel alegó con éxito en primera instancia en su defensa, que la legislación de Washington en materia de correo electrónico comercial no solicitado, al prohibir este tipo de envío de publicidad a los ciudadanos de Washington o desde una computadora ubicada en Washington, no respetaba la llamada “dormant Commerce Clause” de la Constitución estadounidense (artículo 1, sección 8, letra c), según la cual es facultad del Congreso reglar el comercio entre los diferentes Estados de la Federación.[9] Esto mismo sucede en Argentina (CN, art. 75, inc. 13).

El fallo de la Corte Suprema de Washington es importante porque más allá de reconocer la constitucionalidad de la normativa anti-spam cuestionada, identifica claramente los intereses en juego en la problemática en estudio. La juez Susan Owens reconoció tres tipos de intereses lesionados: en primer lugar, el de los proveedores de servicios de Internet (ISPs en inglés), quienes ven incrementados sus costos, al tener que invertir en la detección de las cuentas desde las cuales se envía el spam, o en personal que atienda los reclamos de los usuarios, y/o en equipos adecuados para administrar el tráfico excesivo; en segundo lugar, el de los titulares de nombres de dominios, porque es común que los spammers usen identificaciones ajenas, a estos inocentes terceros los destinatarios terminan enviando equivocadamente y en forma masiva, sus quejas; y en tercer lugar, el de los usuarios, por su pérdida de tiempo y dinero.

Declarada adecuada a las previsiones Constitucionales la ley estatal anti-spam, el caso fue devuelto a la instancia inferior, para nuevo juicio. En 2002, Heckel fue condenado al pago de 98,000 dólares estadounidenses en carácter de multa mas las costas del proceso.

También en Estados Unidos, Jeremy Jaynes pasó a la historia en abril del 2004 como el primer condenado a prisión por cargos de conductas ilícitas relacionadas con el spam (“felony spam charges”), pocos meses después de haber sido denunciado por el envío de decenas de miles de anuncios publicitarios a las cuentas de correo electrónico de clientes de la empresa America Online (AOL).[10]

Vinculado con AOL, fue noticia el caso de Jason Smathers, un ingeniero que trabajaba para la misma, que fue declarado culpable de la venta de 92 millones de direcciones de correo electrónico que poseía AOL a un spammer en la suma de 28,000 dólares estadounidenses. En este caso, la pena que podría recaer consiste en una condena de hasta dos años de cárcel, más una reparación civil que oscila entre 200,000 y 400,000 dólares.[11]

Continuando con la jurisprudencia Norteamericana, un juez del estado de Iowa dictó sentencia contra las compañías AMP Dollar Savings Inc., Cash Link Systems Inc. y TEI Marketing Group, obligándolas al pago de daños que en su conjunto, superan el billón de dólares, a favor de CIS Internet Services, bajo el amparo normativo de la ley federal CAN Spam Act del 2004 que posteriormente comentamos[12] y con el sostén de la legislación federal que reprime severamente las organizaciones criminales y las conductas delictivas en el ámbito industrial.[13]

Mientras tanto, el Departamento de Protección al Consumidor dependiente de la Comisión Federal de Comercio de EE.UU. (Federal Trade Commission's Bureau of Consumer Protection) ha informado que recibe unas mil comunicaciones diarias sólo de quejas de receptores de spam. Al respecto, el primer caso en que la misma Administración Norteamericana actuó contra el spam involucra a esta dependencia.[14] Un juez federal de Las Vegas (Nevada), accedió el 05/01/2005 al pedido de una medida precautoria solicitada por la Comisión Federal de Comercio, imponiendo restricciones a seis compañías y a sus directivos, por presunta violación de las normativas que regula el correo electrónico comercial.

Las firmas involucradas son Global Net Solutions, Open Space Enterprises, Southlake Group y WTFRC, todas ellas con sede en Las Vegas, además de Global Net Ventures, de Londres (UK), y Wedlake, con base en Riga (Letonia), lo cual implicará ciertamente cuestiones de jurisdicción y competencia propias del Derecho Internacional privado. A estas empresas y a algunos de sus directivos se les acusa por violar la ley anti spam de EEUU, al enviar miles de correos sin incluir en ellos la advertencia obligatoria de "contenido sexual explícito", además de prometer falsamente la adhesión gratuita a sus respectivas páginas web y de impedir que los destinatarios puedan dejar de recibir los correos no deseados.

Algunos de los mayores proveedores de correo electrónico del mundo, como Microsoft Corp y la unidad de Internet de Time Warner, AOL, han iniciado acciones judiciales contra quienes envían correo no solicitado en función de los reclamos de sus propios usuarios.

En diciembre de 2004, un tribunal alemán ordenó a tres compañías que dejaran de enviar mensajes pornográficos a usuarios de Hotmail. También recientemente un tribunal francés emitió una orden de cese de actividades comerciales a un hombre que había enviado 150.000 mensajes ofreciendo una "motocicleta eléctrica maleable" a usuarios de AOL y Hotmail.

America Online, EarthLink, Microsoft y Yahoo presentaron seis demandas contra cientos de individuos, en la primera gran acción legal de la industria online Estadounidense bajo la nueva ley anti-spam. Cada uno de los cuatro mayores proveedores de servicio de Internet y correo electrónico de Estados Unidos presentó querellas judiciales ante cortes federales de los estados de California, Georgia, Virginia y Washington, que según indicaron las compañías, incluyen a algunos de los más famosos "spammers" del mundo.

Como vemos, la actividad judicial es intensa en EEUU y básicamente es incoada por los grandes proveedores de servicios como también por el propio Estado Norteamericano. Las millonarias indemnizaciones que generalmente se reclaman es poco probable que puedan ejecutarse debido a la casi insolvencia patrimonial que es característica de los spammers.

#### IV.b. La jurisprudencia en Argentina

Los abogados Gustavo Tanús y Pablo Palazzi, basándose en la Ley de Protección de Datos Personales fueron quienes lograron la primera medida cautelar en Argentina contra un "spammer" o remitente de correo electrónico no solicitado, que ofrecía precisamente bases de datos con el fin de realizar posteriores usos publicitarios.[15]

Estas bases contenían datos personales de individuos que no habían prestado su consentimiento para el tratamiento de su información. Los actores habían solicitado previamente y sin éxito su remoción de la lista de distribución a las direcciones que figuraban en los mensajes, de conformidad con lo dispuesto por la Ley de Protección de Datos Personales 25.326 (arts. 1, 2, 5, 11 y 27).[16] En la acción judicial intentada, acompañaron copias de los mensajes de correo electrónicos recibidos. El juez dispuso en su resolución prohibir a los demandados enviar e-mails a las casillas de los actores, como así también "transferir o ceder a terceros las direcciones de correo electrónico u otro dato personal vinculado a ellos hasta tanto se resuelva el fondo de la cuestión".

La idea manifestada de los actores fue crear conciencia: "la idea nuestra fue poner el tema en evidencia, mostrar que se están manipulando datos personales y se hace publicidad sin respetar la Ley de Protección de Datos (sic...). Estamos tratando de generar un ámbito con propuestas. Por un lado una ley antispam, por otro lado que los principales jugadores en este tema, es decir las ISP (proveedores de Internet), firmen un código de conducta donde se comprometan a no permitir la entrada y salida de spam."[17]

Un punto importante de esta primera resolución consistió en la contienda negativa de competencia que se había establecido con el fuero comercial de la ciudad autónoma de Buenos Aires. Tras la misma, la causa quedó radicada en la justicia en lo civil y comercial federal, con fundamento en que la ley de protección de datos en su art. 36 así lo prevé. Este criterio fue ratificado por la Sala I de la Cámara en lo Civil y Comercial Federal.

Al respecto, hace ya un lustro que la CSJN se ha expedido en el sentido de reconocer a la justicia federal competencia para entender en un conflicto del "ciberspacio". En el caso, el conflicto se suscitaba entre usuarios y empresas que proveían servicios de remates por Internet.[18] Así, el Juzgado Federal de Primera Instancia de Comodoro Rivadavia, provincia de Chubut fue declarado competente para conocer en la demanda iniciada contra las empresas deremate.com, Multimedia Solutions Daltee y mercado libre S.A. por la cual se pretendía que las mismas se abstuvieran de realizar remates a través de sus páginas web sin la actuación de un martillero. Se descartó de esta manera la jurisdicción provincial que era representada por el Juzgado en lo Civil y Comercial N° 1 de la misma localidad.

Se trató aquí de una contienda negativa de competencia ya que la titular del Juzgado provincial resistió la radicación de la causa entendiendo que como lo cuestionado era la realización de actos a través de un medio de interrelación global como Internet, que había sido declarada por el PE de interés nacional, y designada que era la Secretaría de Comunicaciones de la Presidencia de la Nación como autoridad de aplicación, se infería de esto la competencia federal de la materia.

Entendemos que no puede ser otra la solución respecto de cualquier conflicto originado en el ciberspacio (Internet) en tanto su característica esencial es conectar territorios, trascendiendo fronteras. En las mismas palabras de la CSJN "toda vez que puedan verse comprometidos servicios empleados en el comercio interprovincial o internacional, la sujeción al ámbito local de la causa a que pudiera haber lugar (sic...), afectaría intereses que exceden los tribunales provinciales y que, de acuerdo con los arts. 2 inc. 8 a 10 de la ley 13.998, art. 11 inc. 9 de la ley 1893 y 42 inc. b) de la ley 48, se encuentran reservados a la jurisdicción federal".[19]

## IV- Una perspectiva normológica doméstica e internacional

### IV.a. La normativa doméstica

Varios países Latinoamericanos lideran una suerte de “avanzada” normativa que tiende a regular el spam, prohibiendo en líneas generales el envío de correo comercial no solicitado, aunque con importantes variantes.

Entre estos, Venezuela trató el tema al reformar la “Ley de Protección al Consumidor y al Usuario”[20], que incorpora un breve articulado de orden público sobre comercio electrónico y dentro del mismo, un artículo que regula el spam. Establece como obligación de los proveedores de bienes y servicios el deber de instrumentar procedimientos fáciles y efectivos que permitan al usuario o consumidor decidir si quieren o no recibir spam. Se sanciona la inobservancia con una multa. Otra obligación que se establece para los proveedores es la de señalar qué información y bajo qué circunstancias podrá ser compartida con terceros, para su aprobación definitiva por parte de los consumidores o usuarios.

Al igual que Venezuela, México regula la cuestión a partir de la protección al consumidor. Permite llevar un registro de consumidores que no deseen recibir correos no solicitados además de obligar al proveedor de servicios a respetar la decisión del consumidor de no recibir avisos comerciales.

En Perú existe también una ley que reprime el spam[21], y curiosamente se basa en el anteproyecto de la Secretaría de Comunicaciones Argentina del 2001.[22] A fin de proteger el derecho a la intimidad, la norma establece el derecho de los usuarios a: (1) rechazar la recepción de los correos comerciales; (2) revocar la autorización de recepción, salvo cuando dicha autorización sea una condición esencial para la provisión del servicio de correo electrónico; y (3) exigir al proveedor de servicios que cuente con sistemas que filtren los correos electrónicos no solicitados. Entre las obligaciones del proveedor destaca el contar con sistemas de bloqueo o de filtro para la recepción o transmisión de spam. Se diferencia al “correo comercial no solicitado”, del “correo comercial no solicitado ilegal”, y se sanciona este último bajo las normas de protección al consumidor con una sanción pecuniaria de hasta 2000 dólares estadounidenses.

Colombia posee una norma específica[23] cuyo fin es regular la comercialización de bienes y servicios a través de Internet. Se hace referencia al spamming al tratar del “uso de los servicios de correo electrónico para difundir mensajes no solicitados de manera indiscriminada a una gran cantidad de destinatarios”. Se impone a los proveedores de servicios de Internet o de alojamiento de páginas web o usuarios corporativos, la obligación de instrumentar sistemas internos de seguridad para su red encaminados a evitar el acceso no autorizado, la realización del spamming o el acceso a la red desde sistemas públicos, con el fin de difundir en ella contenido relacionado con pornografía infantil. Vemos que la regulación del spamming es tangencial, ya que solo abarca el específico caso de la pornografía infantil, dejando librados los demás aspectos a la autorregulación.[24]

Es interesante el caso de Costa Rica, donde sin existir legislación específica, ha funcionado la autorregulación del propio mercado. En este país, la empresa Radiográfica Costarricense que posee el monopolio del servicio en Internet, redactó un reglamento anti-spam. Por el mismo, dependiendo del tipo de suscriptor de que se trate

y luego de una primera denuncia en su contra, se le bloquea el servicio por unos días. En caso de repetir la conducta y existir nuevas denuncias, el servicio es interrumpido de manera definitiva.

En los tres centros económicos mundiales y principales generadores de spam, la Unión Europea, Japón y Estados Unidos, sus legisladores se han ocupado de la cuestión.

En la Unión Europea, hallamos la Directiva 2002/58/CE[25] sobre el “Procesamiento de los Datos Personales y la Protección de la Privacidad en el Sector de las Comunicaciones Electrónicas”. Aunque la norma no hace referencia directa al spam, genera nuevos presupuestos legales que buscan preservar la privacidad en Internet, regular el tráfico de bases de datos y establecer obligaciones a cargo de los proveedores de servicios de Internet. El art. 13 de la Directiva, regula los aspectos referidos a las comunicaciones no deseadas de todo tipo. Se incluye específicamente al correo electrónico, pero sólo cuando se trata de comercialización directa dejando fuera las comunicaciones políticas, mensajes humanitarios y el llamado correo electrónico basura.

La base del sistema la constituye el principio “opt-in” (aceptación para ser incluido), es decir, que los mensajes pueden ser enviados sólo a aquellos usuarios que expresamente hayan manifestado su consentimiento. Debe existir además la posibilidad de que el usuario se oponga a continuar recibiendo comunicaciones futuras. Se prohíbe igualmente el envío de mensajes electrónicos destinados a la venta directa que disimulen u oculten la identidad del remitente o contengan una dirección inválida que impida al receptor comunicar su intención de ser excluido en futuros mensajes.

Se deja a cada Estado miembro el aceptar la regla del principio “opt-in” que se aplica ante su silencio. En caso contrario, deberá declarar expresamente que recepta el principio opuesto (opt-out)[26]. Queda claro que se intenta conciliar el derecho de los usuarios a no recibir comunicaciones indiscriminadas con los intereses de la industria de usar el correo electrónico como medio de comercialización directa.

El ámbito de aplicación de la Directiva 2002/58/CE incluye a los usuarios que sean personas naturales, dejando a las respectivas normas domésticas la regulación del tema para las personas jurídicas.

Recordamos que en el orden normativo Europeo, la Directiva como tal es junto con el Reglamento, el instrumento mas importante de acción comunitaria. El objetivo principal de una Directiva no es unificar el Derecho sino armonizar las legislaciones domésticas. Por esto, se da un plazo determinado a cada Estado miembro para que suprima las diferencias que existan. La directiva es obligatoria respecto del objetivo fijado, dejando a elección de los estados la forma y los medios por los cuales aquél pueda materializarse. Ahora, si una vez concluido el plazo, el estado no armonizó su normativa interna con el objetivo fijado en la directiva, incurrirá en responsabilidad comunitaria por omisión. En 2004, la Comisión Europea amenazó con llevar al Tribunal de Justicia Europeo a ocho estados miembros, entre ellos Bélgica, Francia y Alemania, por no implantar la Directiva de privacidad 2002/58/CE.

Juega también normativamente en la Unión Europea, la Directiva 97/7/CE[27], relativa a la “Protección de los Consumidores en materia de Contratos a Distancia”. En la introducción señala que “la técnica de promoción consistente en enviar un producto o



proporcionar un servicio a título oneroso al consumidor sin petición previa o acuerdo explícito por parte de éste, siempre que no se trate de un suministro de sustitución, no puede admitirse”. Reconoce luego el derecho del consumidor a la “protección de la vida privada, en particular frente a ciertas técnicas de comunicación especialmente insistentes”. De esta forma les fija a los Estados miembros el objetivo de “tomar las medidas adecuadas para que los consumidores que no deseen ser contactados mediante determinadas técnicas de comunicación puedan ser protegidos de forma eficaz de este tipo de contactos, sin perjuicio de las garantías particulares de que disponga el consumidor en virtud de la legislación comunitaria referente a la protección de la intimidad y de los datos personales”.

En julio de 2002 entra en vigencia en Japón, una norma que obliga a los remitentes de correo electrónico a aclarar en el mismo mail, que se trata de un aviso publicitario no solicitado y la forma en que el destinatario puede rechazar futuros avisos. También se prohíbe el envío de correos a una gran cantidad de direcciones, entendiéndose que esta práctica es realizada mayormente por los remitentes de correos no solicitados. La sanción consiste en la interrupción del servicio y en casos extremos de desobediencia continua, se prevé condena de prisión de hasta dos años o el pago de hasta 3 millones de yens; en caso de compañías, la suma puede ascender hasta 300 millones de yens.

En los Estados Unidos, existe desde hace poco mas de un año la ley federal Estadounidense referida al "Control del ataque de Pornografía y Marketing no solicitado" (Controlling the Assault of Non-Solicited Pornography and Marketing Act, conocida en inglés como CAN-SPAM).[28] El proyecto tiene origen en la misma Casa Blanca impulsado por George Bush y contó con la aprobación de Republicanos y Demócratas lo que manifiesta el consenso logrado en torno de un tema que en EEUU se ha tornado irritante.[29]

La norma crea un registro especial en donde todos los usuarios de Internet con domicilio en EEUU se deberán inscribir y manifestar su voluntad de no recibir ofertas publicitarias en sus cuentas de correo electrónico. En principio, la ley no prohíbe completamente las ofertas comerciales realizadas mediante el correo electrónico, sino que obliga a las empresas a identificarse debidamente además de estar obligadas a ofrecer a usuarios y consumidores la posibilidad de no ser contactados en el futuro, brindando su nombre, dirección física y hasta su número de teléfono. No obstante, de manera previa el destinatario debe haber expresado afirmativamente su voluntad de recibir los mensajes, lo que la ley llama “affirmative consent” o consentimiento afirmativo (Sección 3 Definiciones).

Se penalizan prácticas específicas que los spammers usan para propagar el correo electrónico basura, tales como poner en la cabecera del mensaje títulos o temas engañosos, direcciones de retorno falsas y el uso de computadoras de terceros para disfrazar el punto de origen. También se castiga con multas que pueden llegar a ser millonarias, el ofertar indiscriminadamente y sin anuencia del destinatario, pornografía, y los tan conocidos productos milagrosos para la salud o la imagen física, o métodos para hacer fortunas en minutos.

La autoridad de aplicación es la Comisión Federal de Comercio (Federal Trade Commission, Sección 7). Es interesante conocer que la legitimación activa no se brinda a los consumidores y usuarios sino que las acciones legales se reservan para los fiscales generales de cada Estado que pueden reclamar indemnizaciones en nombre de los

usuarios residentes perjudicados (Sección 7, f.1) salvo que la acción haya sido ya comenzada por el gobierno federal. De igual manera se brinda en especiales casos legitimación activa a los proveedores del servicio de Internet perjudicados (Sección 7, g.1). La jurisdicción en este caso es la de la Corte de Distrito que corresponda según el demandado tenga domicilio en el mismo o se encuentre allí alguna sede de sus negocios. Las penas son de multa e incluso prisión (Sección 4).

En Argentina no existe legislación que regule el spam, aunque sí pueden mencionarse diferentes proyectos a los que haremos referencia. No obstante, no nos encontramos desamparados ya que tanto la CN en su art. 43, como la ley de Protección de Datos Personales No. 25.326 mas su Decreto reglamentario 1558/2001, y la ley de Defensa del Consumidor No. 24.240 y Dec. Reglamentario 1798/94, compatibilizada con las leyes de Defensa de la Competencia y de Lealtad Comercial conforman un bloque uniforme tendiente a proteger en lo que nos importa la intimidad, privacidad y la relación de consumo que se ven afectadas por el envío masivo de correo electrónico no solicitado.

Aun sin legislación anti – spam, en Argentina se realiza un seguimiento sobre la protección de los datos personales. La Dirección Nacional de Protección de Datos Personales (DNPDP)[30] es el órgano de control de la Ley 25.326. Su misión primaria consiste en fiscalizar el cumplimiento de la citada norma y asistir a los particulares para el pleno ejercicio de sus derechos. La Disposición 1/2004 de la DNPDP[31] instrumenta de forma obligatoria, el primer censo nacional de archivos, registros, bases o bancos de datos privados.[32] Esta Disposición 1/2004 es producto de la anterior Disposición 2/2003 DNPDP[33] que dispuso además de la realización del censo, habilitar el Registro Nacional de Bases de Datos, que funciona en el ámbito de la misma DNPDP.

Es conveniente aclarar que tanto el censo como el Registro la DPDP no recaban datos personales, sino sólo información sobre las características, la propiedad y la finalidad de los bancos de datos. Ambos elementos cumplen tres funciones: educar; controlar y garantizar el ejercicio de los derechos de los titulares de los datos en función de la acción constitucional de Hábeas Data (art. 43 CN), a la vez que permite a la DNPDP un control homogéneo, eficaz y fácilmente auditable.

Para garantizar el pleno ejercicio de los derechos consagrados por la ley 25.326, el acceso al Registro es público y gratuito. No así la inscripción, que tendrá un valor proporcional al tamaño de la base de datos cuya inscripción se solicita. El pago del formulario de inscripción también puede realizarse online.

En lo que respecta a los usuarios y consumidores, la norma específica ley 24.240 en su art. 35 prohíbe expresamente las ofertas al consumidor sobre cosas o servicios que no hayan sido requeridos previamente y que obliguen al consumidor a manifestarse por la negativa. La legislación argentina se pronuncia por el sistema de opt – in, reafirmando que el silencio del ofertado no hace presumir su aceptación (CCiv. art. 919).

Ahora bien, respecto de la protección de los datos personales y del consumidor - usuario, podemos afirmar que la República Argentina se encuentra entre los países líderes en lo que hace a la existencia de normativa protectoria. Posee como explicamos las herramientas legales necesarias: una ley, su decreto reglamentario, el organismo de control, la graduación de sanciones y un censo, un Registro de Bases de Datos y las normas mínimas de seguridad obligatorias.

Sin embargo como fuimos adelantando en nuestro trabajo, la protección de los datos personales, léase intimidad y privacidad, es solo una de las aristas de la cuestión. Falta conocer la protección de los proveedores de servicios de Internet (ISPs) y de la propia industria que debiera poder utilizar el correo electrónico para publicitar sus servicios.

Los ISPs son convidados de piedra en la discusión del spam. Ellos quieren brindar el servicio a la mayor cantidad de usuarios posible. Ese es su negocio. La inexistencia de normativa específica implica para ellos desamparo legal. La tendencia internacional los considera víctimas de los spammers ya que intermedian entre éstos y los usuarios corrientes del sistema y sufren perjuicios adicionales a los de los usuarios ya que deben invertir en nuevos y mejores equipos para impedir los envíos masivos, soportar reclamos de los usuarios y atender los mismos.

Por su parte, asumir la realidad implica posibilitar que los ofertantes de bienes y servicios utilicen de manera legal las Nuevas Tecnologías de la Información y la Comunicación. Para esto existe la autorregulación que en general es aceptada y observada por las grandes y medianas empresas reconocidas, pero no por la enorme cantidad de oferentes individuales que utilizan el spam de manera corriente por ser la vía mas directa y carecer casi de costo. Para esto es esencial una regulación que establezca limites y controle las observancias.

En cuanto a los antecedentes nacionales anti - spam, es necesario destacar que en 2001 la Secretaría de Comunicaciones entonces a cargo de Henoch Aguiar presentó un anteproyecto de ley llamado “Anteproyecto de Ley de protección Jurídica del Correo electrónico” que tuvimos oportunidad de comentar.[34] El mismo distinguía entre correo electrónico genérico y comercial, y dentro de éste, el no solicitado, exigiendo requisitos que de no ser cumplidos conducían a la imposición de multas. Además del usuario, el proveedor de servicios también era protegido ya que se lo consideraba un intermediario. Lamentablemente este anteproyecto que contenía importantes soluciones armonizadas internacionalmente, tras sucesivas reuniones en la Comisión de Comunicaciones e Informática, no tuvo tratamiento parlamentario. Paradójicamente, tuvo mejor suerte en Perú donde fue la base de la actual ley anti spam.

Existen varios proyectos de ley referidos al tema[35], entre ellos el oportunamente presentado en la Cámara de Senadores por el senador Guinle (del PJ-Chubut), y otro en Cámara de Diputados presentado en su momento por el diputado Mukdise (de la UCR-Santiago del Estero). El primero estuvo en tratamiento en la Comisión de Sistemas, Medios de comunicación y Libertad de expresión del Senado; el segundo prevé la interrupción del servicio o multa para aquellos spammers que operen dentro del país.

En 2004 la diputada Bertoni presentó una propuesta de modificación de la Ley de Defensa del Consumidor para incluir la temática. Planteaba modificar el art. 8 obligando al oferente a incluir el nombre, domicilio y número de CUIT, debiendo mencionar la leyenda “publicidad” en el asunto y proporcionar una dirección de correo electrónico para que el receptor pueda notificar su voluntad de no recibir envíos futuros. En el punto reconoce como antecedente el referido Anteproyecto de 2001.

## V- Conclusiones

Un derecho humano básico como es la privacidad parece oponerse al desarrollo económico y la generación de negocios que redundarán en un mejor nivel de vida. Este aparenta ser el planteo de la cuestión: principios contra resultados.

Sin embargo debemos intentar un planteo conciliador. ¿Hasta dónde estamos dispuestos a aceptar una invasión a nuestra privacidad e intimidad para sumar al progreso económico de nuestra sociedad informática?. En otro contexto como es el de la seguridad, la privacidad ya ha cedido terreno, a causa del miedo producido por el terrorismo internacional. No hay derechos absolutos y es previsible que ceda en alguna proporción frente a la necesidad de utilizar y desarrollar las nuevas tecnologías.

En la Unión Europea, el órgano iniciador de las propuestas de legislación, la Comisión Europea afirma que la atención de esta cuestión es prioritaria ya que estima que Internet y otros medios de comunicación electrónica (como el acceso de banda ancha, el acceso inalámbrico o las comunicaciones móviles) se constituirán en elementos esenciales del crecimiento de la productividad de cualquier economía moderna. Por esto ha instado a los Estados miembros a velar para que existan vías de recurso y sanciones. “Toda violación de los derechos garantizados por la legislación nacional debe ir acompañada del derecho individual a un recurso judicial [...]. Cualquier perjuicio sufrido a causa de un tratamiento o de un acto ilícitos debe ir acompañado de un derecho individual a una indemnización. Deben estar previstas sanciones en caso de infracción”.

Enfrentados a la realidad, la normativa específica deberá permitir sin lesionar. Permitir la utilización de las modernas herramientas que brindan las Nuevas Tecnologías de la Información y la Comunicación, como lo es el correo electrónico o las llamadas cookies, sin que esta habilitación sea en desmedro de los legítimos derechos e incluso intereses de los usuarios – consumidores y los proveedores de servicios de Internet, siempre relegados cuando no olvidados.

En primer lugar, se necesita normativa específica. El spam causa beneficios y daños. Y estos últimos no pueden ser obviados o dejados a una autorregulación mezquina. El origen del spam es ilegal mas allá que esté prohibido o no. Esto porque se envía utilizando bases de datos que han sido obtenidas ilegalmente ya que sus titulares no han prestado su consentimiento.

En segundo lugar, deben protegerse todos los intereses involucrados: los de los usuarios – consumidores, los de los proveedores de servicios de Internet y especialmente de las casillas de correo electrónico, y también los de la industria, oferentes de bienes y servicios que promueven el comercio utilizando las nuevas tecnologías.

En este punto sin embargo, habrá que decidir la extensión de la legitimación activa. La misma puede ser amplia y hallarse en cabeza de cada titular de un derecho o interés lesionado o restringida como en el caso de la ley federal de EEUU donde el gobierno federal a través de la autoridad de aplicación o los fiscales generales de cada Estado y en algunos supuestos los proveedores de servicios de Internet son los únicos habilitados para reclamar. Creemos superior esta última solución.

En tercer lugar, hay consenso en el derecho comparado respecto de ciertos elementos que deben estar presentes: la afirmación cierta en el encabezado del mensaje respecto de la oferta que se realiza en el cuerpo del mismo; la certeza de los datos completos y comprobables del remitente; la obligación de la existencia de una dirección electrónica

cierta donde poder realizar cualquier reclamo y las sanciones que comienzan con la suspensión e interrupción del servicio, pasan por la aplicación de multas y en algunos casos terminan en penas privativas de la libertad respecto de los spammers recalcitrantes.

En cuarto lugar, en relación con el valor del silencio como declaración de voluntad, nos pronunciamos claramente por el sistema de opt – in, no sólo por una cuestión de respeto del derecho a la privacidad sino por el carácter del derecho positivo argentino que ya ha optado por el mismo conforme lo explicamos anteriormente. EEUU y la Unión Europea adoptan igual criterio.[36]

En quinto lugar y respecto de la jurisdicción, vimos en la jurisprudencia comentada que existe una tendencia a preferir a los jueces federales, asimilando la navegación por la red como un servicio empleado en el comercio interprovincial y aún internacional agregamos, ya que es característica básica de Internet el trascender las fronteras.

Al respecto, además de la ley de Protección de Datos Personales, la ley federal de firma digital No. 25.506 y su Dec. Reg. 2628/02 constituyen un antecedente valioso en este punto ya que dispone la competencia de la Justicia en lo Civil y Comercial Federal para entender en los conflictos que se susciten entre usuarios – consumidores y los certificadores licenciados que son quienes proveen el servicio de firma digital, y establece la justicia en lo Contencioso Administrativo Federal para los conflictos entre particulares y un organismo público certificador licenciado (ley 25.506, art. 46).

En suma, la relación entre derechos privados y derechos sociales debe entenderse conciliadoramente, generando una justa convivencia que no violenta libertades de parte alguna. Las Nuevas Tecnologías de la Información y Comunicación constituyen una realidad imposible de esconder. Asumirla implica aceptar una regulación efectiva que limite la utilización del correo electrónico comercial siguiendo la tendencia internacional expuesta.

---

[1]) El episodio es recordado por SMITH, Reagan, “Eliminating the Spam from your Internet Diet: the Possible Effects of the Unsolicited Commercial Electronic Mail Act of 2001”, en “Texas Tech Law Review”, vol. 35, 2004, p. 416 y nota.

[2]) La referencia es de STRÖMER, Tobias H., Online-Recht – Rechtsfragen im Internet und in Mailboxnetszen, Dpunkt, Heidelberg, 1997, p. 109, nota (279). En el sketch todos los platos del menú de un restaurante incluían un mismo ingrediente: 'spam', que entonces debía inevitablemente ser consumido por los clientes lo hubieran solicitado o no.

[3]) Dice la entrada en el diccionario: “unsolicited usually commercial E-mail sent to a large number of addresses” correo electrónico no solicitado usualmente comercial enviado a una gran cantidad de direcciones.

[4]) En el sitio web de SpamHaus: [www.spamhaus.org](http://www.spamhaus.org)

[5]) En Leysser, L. León, “Spamming y responsabilidad civil (Compensación pecuniaria y protección resarcitoria ordinaria en el régimen jurídico del correo electrónico comercial no solicitado), en Internet [www.jus.unitn.it/cardoza/Review/2005/Leon1.pdf](http://www.jus.unitn.it/cardoza/Review/2005/Leon1.pdf) .

[6]) Nota editorial, revista jurídica “Fojas Cero”, Dirigida por la Dra. Silvia Beatriz Dopazo, en su número 134 de diciembre de 2003.

[7]) Según una lista difundida por la compañía de seguridad en Internet Sophos.

[8]) Washington v. Heckel, 24 P. 3d 404 (2001). La sentencia se encuentra en [www.lexis.com](http://www.lexis.com), además de la comentada reseña crítica publicada en la “Harvard Law Review”, vol. 115, 2002, pp. 931 y ss. (Leysser, L. León).

[9]) Esta “dormant Commerce Clause” se deduce implícitamente, y en sentido negativo, de la citada disposición de la Constitución estadounidense. La interpretación jurisprudencial que rige es que la Constitución es contraria a la intromisión singular de los Estados en la regulación del comercio interestatal, al reconocer la potestad federal en dicho ámbito. Con particular referencia a la Internet, GOLDSMITH, Jack L. y Alan O. SYKES, “The Internet and the Dormant Commerce Clause”, en “Yale Law Journal”, vol. 110, 2001, p. 786, recuerdan que la “dormant Commerce Clause is a judge-made doctrine that prohibits states from regulating in ways that unduly burden interstate commerce”, citado por Leysser, León.

[10]) Véase: <http://www.washingtonpost.com/wp-dyn/articles/A38788-2005Apr8.html>.

[11]) El caso es referido en “Datenschutz-Berater”, año XXIX, 2005, núm. 3, p. 8.

[12]) La “Controlling the Assault of Non-Solicited Pornography and Marketing Act”, que se puede consultar en: <http://www.spamlaws.com/federal/108s877.shtml>. En ella se expone que el correo comercial no solicitado supera la mitad del total de la correspondencia electrónica en circulación, y con tendencia a aumentar, lo cual afecta la conveniencia y eficiencia del correo electrónico (Sec. 2.a.2).

[13]) Véase: <http://www.thestandard.com/internetnews/000777.php>. Este caso surgió a raíz del envío, por parte de las compañías sentenciadas, de millones de “spam pieces” a los cinco mil clientes de CIS Internet Services, entre agosto y diciembre del 2003. Según la legislación del Estado de Iowa, se aplica una sanción de diez dólares por cada mensaje de correo no solicitado.

[14]) Fuente Agencia EFE en internet [www.efe.com](http://www.efe.com) del 6/01/2005.

[15]) Dictada en fecha 11/11/2003 por el titular del Juzgado Nacional en lo Civil y Comercial Federal N° 3, Secretaría N.º 6, de la Capital Federal Argentina, Dr. Roberto Torti.

[16]) Transcribimos el art. 27 de la ley 25.326:” (Archivos, registros o bancos de datos con fines de publicidad). 1. En la recopilación de domicilios, reparto de documentos, publicidad o venta directa y otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u

obtenidos con su consentimiento. 2. En los supuestos contemplados en el presente artículo, el titular de los datos podrá ejercer el derecho de acceso sin cargo alguno. 3. El titular podrá en cualquier momento solicitar el retiro o bloqueo de su nombre de los bancos de datos a los que se refiere el presente artículo. “

[17]) En palabras del dr. Gustavo Tanús.

[18]) En autos “CAMPOLI, Gabriel Andrés s/Acción de Amparo”, CSJN, Buenos Aires, sentencia de 1/06/00.

[19]) Ver CSJN, doct. de fallos 313:1467.

[20]) En fecha 04/05/2004.

[21]) Ley Peruana N° 28.493 del 18/03/2005, llamada “Ley que regula el uso del correo electrónico comercial no solicitado”. El Decreto Supremo 031-2005-MTC, que "Aprueba el Reglamento de la Ley No. 28493 que regula el envío del correo electrónico comercial no solicitado (SPAM)" apareció el 4/01/06 en la Pág. 309276 del Diario Oficial Peruano (noticia publicada por Erick Iriarte Ahon <eiriarte@alfa-redi.org>).

[22]) Puede encontrarse un profundo análisis y crítica de esta norma en Leysser, L. León, citado en nota al pie No. 6. En su trabajo el autor se opone de manera enérgica y con sólidos argumentos tanto a la protección exclusiva del usuario como a la responsabilidad que se asigna a quien él considera otra víctima del spamming, como es el proveedor de servicios de Internet.

[23]) Decreto 1524 de fecha 24/07/2002 expedido por el Ministerio de Comunicaciones de Colombia.

[24]) Al respecto puede consultarse Ceballos Suárez, Alvaro, en “Nueva regulación Colombiana del mail spamming”, alvaro.ceballos@attla.com.

[25]) De fecha 12/07/2002, puede hallarse en archivo acrobat en el sitio web [http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l\\_201/l\\_20120020731en00370047.pdf](http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf)

[26]) El sistema opt –out es el principio opuesto por el cual el remitente envía indiscriminada y masivamente sus mensajes, estando luego legalmente obligado a discontinuar los mismos respecto de aquellas personas que lo soliciten expresamente.

[27]) De fecha 20/05/1997.

[28]) Es la Consumer Antispamming Act (CAN-SPAM Act de 2003, Public Law 108-187), aprobada en 8/12/2003 por la Cámara de Representantes de Estados Unidos y con vigencia desde el 01/01/2004. La ley federal americana se encuentra en <http://www.spamlaws.com/federal/can-spam.shtml>.

[29]) La ley tuvo entrada en el Senado de Estados Unidos. Su antecedente inmediato había sido un proyecto del año 1998 elaborado conjuntamente por representantes de los dos partidos principales, el senador republicano por Alaska Frank Murkowski y el demócrata por New Jersey, Robert Torricelli. En Internet <http://www.el-mundo.es/navegante/98/julio/16/spamming.html>

[30]) Dependiente de la Secretaría de Política Judicial y Asuntos Legislativos del Ministerio de Justicia, Seguridad y Derechos Humanos.

[31]) Publicada en el Boletín Oficial en fecha 26/02/2004.

[32]) El censo estuvo abierto desde el 01/03/2004 hasta el 30/04/2004, debiendo inscribirse las siguientes bases privadas de datos personales: (i) aquellos archivos, registros, bases o bancos de datos privados destinados a dar informes; (ii) aquellos que exceden el uso exclusivamente personal; y (iii) los que tienen como finalidad la cesión o transferencia de datos personales, independientemente de que la circulación del informe o la información producida sea a título oneroso o gratuito (artículo 1° de la reglamentación de la ley N° 25.326, Dec. N° 1558/01). Existieron dudas respecto de las “zonas grises” donde es difícil establecer si una base debe o no ser censada. Como ejemplos, se citan el acceso a una base de datos interna de personal por parte de empresas de un mismo grupo económico; o la tercerización de algunos servicios como la liquidación y pago bancario de sueldos; ciertos servicios de marketing; o el deber de informar a autoridades administrativas como el BCRA, la Superintendencia de Seguros, la AFIP, etc. .

[33]) Publicada en el Boletín Oficial el 27/11/2003.

[34]) Resoluciones 333/2001 y 338/2001 de la Secretaría de Comunicaciones de la Nación, dependiente del Ministerio de Infraestructura y Vivienda. B.O. 11/09/2001. Puede leerse nuestro comentario en El Derecho, Legislación Argentina, Boletín No. 18 del 26/10/2001.

[35]) Puede leerse un resumen completo de los mismos a mayo de 2005 en el trabajo “Comentario a los proyectos de ley en materia de control del spam y regulación del uso del correo electrónico en Argentina” de la Lic. Claudia Fonseca Martínez, en Revista Electrónica Alfa Redi, edición de mayo de 2005, [www.alfa-redi.org](http://www.alfa-redi.org)

[36]) En la Unión Europea, de los 25 Estados Miembros, 10 estados han adoptado el principio (Austria, Bélgica, Dinamarca, Finlandia, Alemania, Grecia, Hungría, Italia, Eslovenia, España); 2 lo tienen en tratamiento legislativo (Francia y Suecia) y el resto no lo ha aprobado aún (datos a diciembre de 2005)