EL CORREO EN LOS TIEMPOS DE INTERNET

Iñigo de la Maza Gazmuri [?]

Cada tecnología engendra sus propios monstruos, y el correo electrónico no es la excepción.
Kenneth Amaditz

No existe una definición canónica de "spam." Ni siquiera existe demasiada claridad respecto al origen de la expresión.[1] Desde luego actualmente existe consenso en el hecho que la expresión incluye el correo electrónico no deseado; esta acepción es la que interesa examinar en las páginas siguientes.

El tema dista de ser un capricho propio de la euforia jurídico-tecnológica que últimamente ha impregnado la actividad de algunos abogados y académicos. El envío de correos electrónicos no solicitados posee costos relevantes que se radican mayoritariamente en los usuarios y en los proveedores de servicios de

[?] Profesor Facultad de Derecho Universidad Diego Portales. Agradezco a Gonzalo Angeli la sabiduría, paciencia y pedagogía de sus explicaciones técnicas. Sin ellas, este texto contendría bastantes más errores de los que probablemente posee. Estos últimos, por supuesto, me pertenecen.

[1] La expresión "spam" corresponde originariamente al nombre de un tipo de carne enlatada con especies -jamón con especias (spiced ham)- producida por Hormel Foods a partir de 1926, cuya principal característica era que no requería refrigeración. Esta característica la hizo extremadamente atractiva para el ejército y la popularizó durante la Segunda Guerra Mundial. (ver Cyberangels. http://www.cyberangels.com/law/spam/ visitado 28/02/2002). Según algunos comentaristas (ver KHONG W. K., *"Spam Law for the Internet"* Refereed article, 2001 (3) *The Journal of Information, Law and Technology (JILT).* http://elj.warwick.ac.uk/jilt/01-3/khong.html/ Visitado 15/01/2001; SORKIN, David. *Technical and Legal Approaches to Unsolicited Electronic Mail.* U.S.F. L. REV. 325 (2001) nota 2) la expresión adquirió relación con las comunicaciones electrónicas a partir de un episodio que tuvo lugar a mediados de los ochenta en el que un participante de un MUSH (Un MUSH [multi-used shared hallucination] es un tipo de MUD es decir "Un entorno simulado [generalmente con base de texto]. Algunos son diseñados únicamente con fines de diversión y otros son desarrollados con propósitos más serios como el desarrollo de software o educación en general...Una característica significativa de la la mayoría de los MUDs es que los usuarios pueden crear cosas que permanecen una vez que ellos han dejado el escenario y con los cuales otros usuarios pueden interactuar, permitiendo de esta manera la construcción gradual y colectiva de un mundo" Enzer, Matisse, Glosary of Internet Terms. http://www.matisse.net/files/glossary.html#M. Visitado 01/03/2002) creó y usó un macro que repetidamente tipeaba la palabra SPAM interfiriendo con la posibilidad de participar de otros. Es muy probable que el creador del macro se haya inspirado en un sketch realizado en la televisión británica por Monty Python´s Flying Circus en el que la palabra SPAM se repetía en el menú de un restorán hasta el absurdo. En un principio, la expresión se utilizó para referir a artículos u otros tipos de adiciones puestas en grupos de noticias (newsgroups) Usenet (Usenet es "un sistema mundial de grupos de discusión con comentarios pasados a través de cientos de miles de máquinas." Glossary of Internet Terms. http://www.matisse.net/files/glossary.html#U. Visitado 11/03/2002) u otros foros de discusión vulnerando las reglas de dichos foros. Posteriormente el uso de la expresión derivó hacia los mensajes de correo electrónico no deseados enviados masivamente. Actualmente, la expresión spam se utiliza para designar cualquier especie de comunicación no solicitada (faxes, llamadas telefónicas, correo regular, etc.), en las páginas que siguen su uso queda restringido a comunicaciones electrónicas no deseadas.

Internet.[2] Se trata además de una práctica que se difunde con bastante indiferencia de las fronteras territoriales. De esta manera la distinción entre países tecnológicamente avanzados y atrasados pierde vigor. Finalmente, el spam es una práctica cuyas especiales características la hacen inédita en la historia de la humanidad.

En las páginas que siguen intento (1) examinar los elementos que deberían reunirse en una definición de spam y examinar brevemente las controversias que giran en torno a las definiciones disponibles. (2) Revisar brevemente la historia del spam a través de tres casos. (3) Argumentar a favor del carácter inédito del spam, exponer sus diferencias con otras especies de marketing directo y la necesidad de restringirlo. (4) Examinar las respuestas que es posible dar a este fenómeno (Sobre esto examino cuatro tipos de modalidades de regulación (i) el derecho, (ii) las normas sociales, (iii) soluciones tecnológicas o de "código", y (iv) el mercado). (5) Revisar brevemente el tratamiento legislativo del spam en las directivas de las Comunidades Europeas; y (6) examinar críticamente el tratamiento del correo electrónico no deseado en la Ley 19.628 sobre Protección de Datos de Carácter Personal.

1. Hacía una definición de spam.[3]

Los requisitos del spam.- Ya se ha informado que no existe una sola definición generalmente aceptada de spam. Definirlo como correo electrónico no deseado no elimina este problema. Al reflexionar sobre la regulación del spam no interesa, en verdad, saber si el correo es deseado o no. De lo que se trata es de decidir cuando resulta legítimo el envío de este correo no solicitado y cuando no. Tomada

[2] Según GAUTHRONET y DROUARD:

> "Respecto al costo financiero soportado por los navegantes de la Web...Asumiendo que un usuario promedio de Internet paga una tarifa plana de € 12 mensual por diez horas de conexión (incluyendo las llamadas de teléfono) y usando equipo estándar (sin banda ancha) puede bajar mensajes a una velocidad de aproximadamente 180 K/bits por minuto, el costo de bajar alrededor de 15 mensajes al día sumando entre 500 y 800 K/bits en tamaño puede costar tanto como €30 al año. Si esta cantidad es multiplicada por el número de usuarios de Internet en un país el costo total llega a ser muy sustantivo. Llevando esto a escala planetaria, asumiendo una comunidad mundial de 400.000 de usuarios, el costo global de bajar mensajes de avisaje utilizando la tecnología actual podría ser estimado conservadoramente en €10 mil millones –y esta es solo una porción de los costos soportados directamente por los navegantes" (GAUTHRONET, Serge, DROUARD, Etienne. Unsolicited Commercial Communications and Data Protection. Commision of the European Communities. Enero 2001. P. 67. Disponible en http://europa.eu.int/comm/internal_market/en/dataprot/studies/spamstudyen.pdf. Visitado 01/03/2002)

[3] En esta sección sigo de cerca a SORKIN (ver *Technical and Legal Approaches to Unsolicited Electronic Mail.* cit. Pp. 328 – 336).

esa decisión, recién es posible preguntarse qué modalidades regulatorias y en qué medida pueden ser utilizadas para enfrentarlo.[4]

Aún cuando para algunos cualquier correo no solicitado es spam, las dos definiciones más aceptadas de spam son (1) correos electrónicos comerciales no solicitados (CECNS) *(unsolicited comercial e-mail [UCE])* y (2) correos electrónicos masivos no solicitados(CEMNS) *(unsolicited bulk email [UBE]).*[5]

Lo que resulta común en ambos casos es que se trata de correo electrónico no solicitado. Generalmente se ha entendido por *no solicitado* un correo en aquellos casos en que:

> no existe relación previa entre las partes y el receptor no ha consentido explícitamente en recibir la comunicación. Puede significar también que el receptor previamente ha buscado terminar una relación existente, usualmente instruyendo a la otra parte de no enviarle más comunicaciones en el futuro[6]

Por supuesto no basta que se trate de correo no solicitado en los términos recién expuestos. Lo que, en principio, cualifica al correo no solicitado como spam es su carácter comercial, la cantidad enviada o, desde luego, una mezcla de ambos.

Aún cuando la definición de *comercial* varía en las distintas legislaciones[7] lo que suele considerarse en el caso de las comunicaciones comerciales es la promoción de algún tipo de bienes o servicios.[8] En este sentido, por ejemplo, la Directiva 2000/31 de las Comunidades Europeas define en su artículo 2 letra f) comunicaciones comerciales como: "todas las formas de comunicación destinadas a proporcionar directa o indirectamente bienes, servicios o la imagen de una empresa, organización con una actividad comercial, industrial o de profesiones reguladas..."

Con respecto al carácter *masivo* se plantean dos interrogantes. La primera es si debe tratarse del mismo mensaje enviado en forma multitudinaria para que

---

[4] Como advierto más adelante, utilizo el esquema de modalidades regulatorias sugerido por LESSIG, quien distingue cuatro especies: las normas jurídicas, las normas sociales, el mercado y el código (ver LESSIG, Lawrence, *The Law of the Horse: What Cyberlaw Might Teach?* http://cyberlaw.stanford.edu/lessig/content/works/finalhls.pdf Visitado 04/06/2001). Más adelante desarrollo el esquema de LESSIG con mayor detalle.

[5] Ver CAUBE. Coalition Against Unsolicited Bulk Email, Australia. http://www.caube.org.au/whatis.htm. Visitado 06/03/02

[6] *Technical and Legal Approaches to Unsolicited Electronic Mail.* cit. P. 229 – 230 (notas a pié de página omitidas).

[7] Ver "*Spam Law for the Internet*" S/P cit.

[8] Ver *Technical and Legal Approaches to Unsolicited Electronic Mail.* cit. p. 330

califique como spam o puede tratarse de mensajes substancialmente similares.[9] La segunda es cuántos mensajes deben enviarse para que dicho envío sea considerado masivo. La principal pregunta a este respecto es si debiese fijarse un umbral –por ejemplo, 1000 correos electrónicos- o dejar la norma abierta.[10]

Aún suponiendo que las definiciones de comercial y masivo no sean problemáticas, un inconveniente que subsiste es si el spam debe ser definido como CECNS o como CEMNS. Existen argumentos a favor de ambas posturas.[11] En el caso de definirlo como CECNS:

- Por que el traslado de costos desde el emisor hacia el receptor de los mensajes es particularmente susceptible de objeciones en el caso comercial
- Si se define como CEMNS entonces resultará necesario fijar un umbral a partir del cual se trate de correo masivo
- Los correos no comerciales –en particular los políticos y los religiosos- pueden estar protegidos por la normativa relativa a libertad de expresión. En el caso de los comerciales la protección suele ser menor.[12]
- La regulación destinada a limitar mensajes comerciales posee mejores probabilidades de ser aprobada que aquella que también cubre otro tipo de discursos.

En el caso de definirlo como CEMNS:

- El principal argumento es que el daño que se inflige con los correos masivos es absolutamente independiente de la naturaleza del mensaje. Los costos soportados por los receptores de los mensajes y la redes intermedias no poseen así relaciones con el contenido de la comunicación. Si de lo que se trata es de cautelar ese daño, distinguir según el contenido no tiene sentido.

Por supuesto una tercera alternativa es definir spam como correo comercial masivo no solicitado. Aún cuando esta idea parece atractiva aún persisten ciertos

---

[9] En este sentido, las leyes 1373, 1373 que serán codificadas en el Código de Idaho § 48-603E(1) (a) define el avisaje masivo de correo electrónico como "el mismo aviso o avisos similares simultáneamente transmitidos a dos o más receptores).

[10] Las objeciones a fijar un umbral pueden revisarse en *Technical and Legal Approaches to Unsolicited Electronic Mail.* cit. p. 332

[11] Los argumentos han sido extraídos de ibid. pp. 332-334. Las notas a pié de página han sido omitidas.

[12] Ver, por ejemplo SUNSTEIN, CASS: DEMOCRACY AND THE PROBLEM OF FREE SPEECH. Free Press. Nueva York 1995. Pp. 121-166. En el caso chileno, la diferencia entre la protección del discurso comercial y otros tipos de discurso ha sido tratada por el Tribunal Constitucional a propósito de las diferencias entre la propaganda política y la propaganda comercial. Un análisis de los fallos del Tribunal Constitucional puede encontrarse en PEÑA, Carlos: *El sonido del dinero: el gasto electoral y la libertad de expresión.* Centro de Estudios Públicos. Serie Documentos de Trabajo. Nº 330 – Marzo 2002.

problemas. Dos de ellos son los consignados en las críticas de definir spam como CEMNS –el daño es independiente del contenido y debe fijarse un umbral. Una tercera crítica, que en verdad resulta aplicable a los tres modelos de definición es que así concebidas las definiciones omiten el problema de la recolección de datos, de esta manera, algunas definiciones incorporan entre sus elementos la forma de recolección.[13]

No se trata aquí de agotar el problema de la definición, sino nada más de dar noticias sobre las dificultades que existen al momento de determinar los elementos que la componen. Como no es difícil advertirlo, estas dificultades son uno de los escollos que deben ser superados al momento de legislar sobre el tema o aplicar la legislación vigente.

Sin perjuicio de lo anterior, en lo que resta de este trabajo, utilizaré una definición de spam como correos comerciales electrónicos no solicitados. La razón de lo anterior es que, como reviso más adelante, esta ha sido la más popular al momento de legislar sobre el problema.[14]

2. Algunas noticias sobre el desarrollo del spam.[15]

Tres etapas en la historia del spam.- El spam –como todos los fenómenos asociados a Internet- es una práctica reciente. Siguiendo el esquema presentado por SCHWARTZ & GARFINKEL es posible, sin embargo, distinguir tres etapas que pueden ser ilustradas a través de tres casos. La primera de ellas corresponde al primer caso de spam ampliamente publicitado, el de un par de abogados de Arizona, Laurence Canter y Martha Siegel quienes se dedicaron a promover sus servicios utilizando grupos de discusión Usenet durante 1994. La segunda etapa queda bien ilustrada a través de la obstinada gestión de Jeff Slaton, conocido como el

---

[13] Un ejemplo de lo anterior es la definición de Commision Nacionelle de l´ínformatique et le liberté. Según esta spam es:

> la práctica de enviar correos electrónicos no solicitados, generalmente de naturaleza comercial, en grandes cantidades a individuos con los cuales quien los envía no tiene previo contacto y cuyas direcciones de correo electrónico han sido recolectadas en espacios públicos en Internet: listados de correo, directorios, sitios web, etc. (Citada en Unsolicited Commercial Communications and Data Protection. cit. P. 88).

[14] Es posible prescindir de la cantidad si se consideran los mensajes comerciales porque estos suelen ser enviados a una multiplicidad de destinatarios. En este sentido cuando se habla de correos comerciales, en la mayoría de las ocasiones, también se está hablando de correos masivos.

[15] Un recuento pormenorizado del desarrollo del spam puede encontrarse en SCHWARTZ Alan & GARFINKEL Simon, STOPPING SPAM. O´Reilly & Associates (1998) falta ciudad. pp. 17-35. Un resumen de los tres casos presentados puede ser encontrado en Michael D. SOFKA. *You Have Spam! How to prevent your machines from eing used to advertise get rich quick schemes, Asian prostitutes and o_-shore gambling.* http://www.rpi.edu/~sofkam/papers/spam-talk.pdf. Visitado 12/03/2002.

"Rey del spam." Finalmente, la última etapa corresponde a la gestión de Sanford Wallace en Cyber Promotions.

1. Canter y Siegel.- Laurence Canter y Martha Siegel eran una pareja de abogados que un día de 1993 comenzaron a ofrecer servicios legales relacionados con asesoría en materias de inmigración que consistían en asegurar a sus potenciales clientes –previo pago de US $100- su inclusión en las listas de lotería que seleccionan las solicitudes de visa que serán tramitadas. La oferta de la firma de abogados fue llevada a cabo poniendo un aviso en más de 6.000 grupos de discusión Usenet. La pequeña firma de abogados recibió un buen número de respuestas de clientes potenciales. Junto a esto, recibieron miles de respuestas airadas reclamando el envío de publicidad no solicitada. Esta avalancha de respuestas excedió la capacidad del proveedor de servicios de Internet de los abogados, de manera que, al corto andar, su cuenta fue cancelada. Algo más tarde, la pareja de abogados publicó un libro llamado HOW TO MAKE A FORTUNE ON THE INFORMATION SUPERHIGHWAY dando noticia sobre técnicas de recolección de direcciones de correo electrónico desde grupos de discusión y sobre cómo enviar masivamente publicidad por medios electrónicos.[16]

2. Jeff Slaton, el rey del spam.- Uno de los lectores del libro de Canter y Siegel fue Jeff Slaton, el representante de Yellow Pages en Alburquerque, quien se dedicó a enviar avisos a grupos de discusión ofreciendo los planos de la bomba atómica por US $18. Slaton descubrió que el negocio prosperaba y cambio su modelo de negocios desde el envío de publicidad hacia la venta de campañas publicitarias realizadas a través del envío de spam. De esta manera Slaton se transformó en el primero en ofrecer sus servicios como "spammer", autoproclamándose el rey del spam. Junto a esto inauguró algunas técnicas actualmente comunes en el envío de publicidad masiva en plataformas electrónicas como direcciones falsas de correo electrónico en el caso del emisor y nombres de dominio falsos para evitar la detección y desviar las quejas.[17] De esta manera, Slaton inauguró las empresas dedicadas al spam.

3. Sanford Wallace y Cyber Promotions.- Durante la primavera de 1996, Sanford Wallace (quien luego sería conocido como "Spamford"[18]) dueño de Cyber Promotions, una compañía con sede en Philadelphia, comenzó a enviar publicidad

---

[16] Canter y Siegel parecen formar haber entrado a los anales de Internet, hace algunos años el New York Times señalaba que "Laurence Canter and Martha Siegel fueron los primeros en ver Internet y advertir las increíbles oportunidades a nivel de marketing ¿Ellos son las serpientes en el Edén o pioneros en la frontera final?" (citado por Ron Newman en Newsgroups: alt.current-events.net-abuse,news.admin.misc,alt.flame.canter-and-siegel,alt.culture.internet. Subject: Re: Ad for C&S book in 12/2/94 NY Times business section. Date: 3 Dec 1994 03:56:40 GMT Lines: 49

[17] Una descripción y explicación de la mayoría de estas prácticas puede ser encontrada en *IP Spoofing and Other Header Fraud Resources* (Center for Democracy and Technology). Disponoble en http://www.cdt.org/speech/spam/ipspoof.html. Visitado 05/03/2002.

[18] Ver *You Have Spam! How to prevent your machines from being used to advertise get rich quick schemes, Asian prostitutes and off-shore gambling.* cit. P. 6.

no solicitada a los correos electrónicos provistos por AOL[19], llegando, en su punto más álgido, al envío de 30 millones de correos diarios.[20] AOL respondió a esto bloqueando las direcciones desde donde Wallace enviaba sus correos. En respuesta Wallace demandó a AOL por infringir el derecho a la libertad de expresión consagrado en la Primera Enmienda de la Constitución de los Estados Unidos. Una semana antes que la demanda de Wallace fuera desestimada, este compareció una vez más ante los tribunales, pero esta vez como demandado. Los demandantes eran tres proveedores de servicios en línea (online service providers), Compuserve, Prodigy y Concentric Networks alegando que Cyber Promotions estaba utilizando sus nombres de dominio para evitar los filtros instalados por AOL para prevenir el ingreso de correos electrónicos enviados por Cyber Promotions.

Spamware y proveedores de servicios de spam[21].- Actualmente quienes se dedican a enviar spam utilizan dos tipos de herramientas, las primeras sirven para recolectar direcciones de correo electrónico y las segundas para enviar las comunicaciones electrónicas masivas no deseadas. A estas dos herramientas en conjunto se les denomina spamware.

Las herramientas de recolección como Target 98, Post News 2000 y Atomic Harvester 2000, permiten recolectar direcciones de correo electrónico de la Red y de grupos de discusión. Aún cuando existen listas de correos electrónicos disponibles para la venta, la ventaja de las herramientas de recolección es que evitan –o al menos disminuyen sensiblemente- el número de direcciones duplicadas de correo electrónico que suelen contener las listas. El segundo riesgo que se evita al no optar por listas es que quienes figuren en dichas listas ya hayan sido víctimas de numerosas campañas de spam y posean sistemas de filtro y bloqueo.[22] Las herramientas de recolección son sencillas de utilizar[23] y permiten al

---

[19] America On Line es uno de los principales proveedores de servicios de Internet en los Estados Unidos.

[20] Según SOFKA, quienes a esta fecha poseían correos provistos por AOL recibían en sus cuentas de correos entre 50 y 60 correos diarios enviados por Cyber Promotions. Ver *You Have Spam! How to prevent your machines from eing used to advertise get rich quick schemes, Asian prostitutes and off-shore gambling.* Ob. cit. P. 6. Esto no resulta demasiado lejano al caso de Hotmail. En mi propia casilla recibí 45 correos no deseados entre el 7 y el 14 de marzo de 2002, algunos de los encabezados son las siguiente frases entre comilladas: "Bachelors, masters, MBA, and doctorate (Phd), Hi cutie havent talked to you in a while!, RE: Hi how are you?, SLEEP your weight away! Guaranteed!, Get Out Of Debt & Retire Quickly, Debt Worries? FREE Help – No Loan, Skinny White Young Teens make their first poor..., Here´s some really raunchy stuff for you, Mejor estilo de vida, re: FR-E-E TRIAL!!!, Need More Trafic To Your Website?, NOW! YOUR immediate FINNANCIAL SECURITY!, FREE LIFETIME ADULT SITE VIP PASSWORD!, Generate More Business Now!, Low cost lawyers!, Greetings from sunny California!, Do you want to understand those legal papers!..., Want to see some really raunchy pics?."

[21] La información contenida bajo este título ha sido obtenida de Unsolicited Commercial Communications and Data Protection. cit. pp. 31-36.

[22] Reviso con mayor detalle ambos mecanismos más adelante

usuario discriminar las direcciones que pretende recolectar, exceptuando, por ejemplo aquellas que contengan determinados TLDs (top level domains) como gov, org, mil, etc. Junto a lo anterior, algunas de estas herramientas poseen la capacidad de rescatar información simultáneamente desde varios sitios y luego filtrarla eliminando aquellas direcciones que se repiten.

Las herramientas de envío presentan dos ventajas. Por una parte permiten al spammer enviar cantidades masivas de correo sin que esto lesione al proveedor de servicios de Internet que el spammer está utilizando. Por otra, permiten eludir algunos de los filtros que utilizan los usuarios o los operadores de destino para evitar correos no deseados.

Los proveedores de servicios de spam pueden agruparse en dos actividades: las realización de campañas de spam y la creación de listas. En el primer rubro, el servicio ofrecido es la recolección, el envío de los mensajes y todos aquellos servicios que resulten necesarios para llevar adelante una campaña de publicidad a través de correos electrónicos masivos. En el segundo caso –creación de listas- el servicio ofrecido es la venta de listas de direcciones de correos electrónicos.

3. ¿Nada nuevo bajo el sol? Las diferencias entre el spam y otras especies de mensajes no deseados.

Resulta evidente que el envío de publicidad no deseada como mecanismo de marketing directo es un fenómeno que antecede con creces a Internet y el spam.[24] Diariamente las casas y departamentos son bombardeadas con cartas, a veces nominativas y otras no, que ofrecen servicios no solicitados. Asimismo, aunque quizás con menor frecuencia, no es extraño recibir o recuperar de la contestadora telefónica llamadas a través de las cuales, una vez más, se ofrecen servicios no solicitados.[25] ¿Por qué entonces no tratar al spam como una más de estas prácticas?

Las respuestas son varias. Antes de examinarlas con mayor atención, una aproximación general sería responder que "(M)ientras las solicitudes comerciales

---

[23] Este tipo de software funciona navegando por la Red y deteniéndose en aquellos sitios preestablecidos o bien discriminando sitios según algún parámetro indicado por el usuario. Una vez que localiza uno de esos sitios recoge todas las direcciones de correos electrónicos que encuentre.

[24] Ver Michael W. CARROLL, *Garbage In: Emerging Media and Regulation of Unsolicited Commercial Solicitations,* 11 BERKELEY TECH. L. J. (1996). Disponible en http://256.com/gray/spam/law.html. Visitado 12/03/2002.

[25] En el caso norteamericano, por ejemplo, anteriormente al spam ha existido litigación respecto de las ventas puerta a puerta, las llamadas telefónicas no solicitadas y los faxes no solicitados (ver Ibid. S/P. Notas a pié de página omitidas). En el caso europeo, el problema de las comunicaciones comerciales no deseadas había sido discutido a propósito de la promulgación de la directiva 97/66 respecto a las llamadas no solicitadas

no deseadas han sido un hecho de la vida por un largo tiempo, nunca antes ellas habían amenazado la viabilidad de todo un modo de comunicación."[26] Para utilizar una imagen de ECO, tratar al spam simplemente como otra forma de comunicación directa equivaldría a tratar a un rinoceronte como si fuera un unicornio.[27]

La economía del spam.- La ventaja de los mecanismos de marketing directo es que permiten llegar a los consumidores en términos que, al menos estadísticamente, llamarán su atención con mayor intensidad que mecanismos alternativos como publicidad en las calles o avisos en televisión. Lo anterior, sin embargo, posee costos. En el caso del envío de publicidad por correo regular, por ejemplo, es el avisador quien soporta la gran mayoría –sino todos- los costos del envío de la publicidad. De esta manera se invertirá en marketing directo en la medida que la ganancia proveniente de la respuesta de los consumidores supere a los costos de alcanzar a los consumidores. En el envío de publicidad masiva por correo electrónico, sin embargo, la ecuación entre costos y beneficios difiere.

En el caso del spam la mayoría de los costos del envío no son soportados por quien envía las comunicaciones.[28] En general los costos que asume quien envía el spam son el de encontrar un proveedor de servicios de Internet suficientemente inocente, la composición del mensaje y el establecimiento de un sistema de procesamiento de pago por los bienes o servicios, en el caso que los provea el mismo, o bien la contratación de este servicio en caso contrario. El costo marginal de enviar un correo electrónico más es prácticamente inexistente, por lo tanto, los incentivos del emisor son enviar tantos mensajes como sea posible.

Junto a los costos marginales prácticamente nulos, el envío masivo se justifica porque la tasa de retorno obtenida por el emisor dependerá del número de correos

---

[26] Ibid. S/P

[27] Esta imagen se encuentra en SERENDIPITIES. LANGUAGE AND LUNACY. (Orion Books. Londres: 1998 p. 79), allí ECO relata como toda la tradición medieval convenció a Europa de la existencia del unicornio, un animal que asemejaba un delicado y gentil caballo blanco con un cuerno sobre su hocico. Como encontrar unicornios en Europa no resultaba sencillo, la tradición decidió que estos animales debían habitar en países exóticos. Marco Polo, como habitante de la Europa medieval también se empapó de esta tradición, así cuando viajó a China estaba preparado para encontrar unicornios y, de hecho, durante su viaje los buscó afanosamente. Nos cuenta Eco que el encuentro se produjo mientras el viajero volvía a casa, en la isla de Java. Siendo Marco Polo un cronista honesto no pudo dejar de advertir que estos unicornios presentaban algunas diferencias con aquellos que anunciaba la tradición europea. De acuerdo a la relación de ECO:

> ellos no eran blancos sino negros. Su piel asemejaba a la de los búfalos y sus abdómenes eran tan abultados como los de los elefantes. Sus cuernos no eran blancos sino negros, sus lenguas eran erizadas y sus cabezas asemejaban a las de los jabalíes salvajes (loc cit.)

[28] Ver SINROD, Eric & JOLISH, Barak: *Controlling Chaos: The Emrging Law of Privacy and Speech in Cyberspace.* 1999 STAN. TECH. L. REV. 1. Parag 49. Disponible en http://stlr.stanford.edu/STLR/Articles/99_STLRV_1/. Visitado 14/11/2001

que envíe. Si se suman ambas cosas el resultado es que aún resulta económicamente razonable enviar 10.000.000 de correos electrónicos aún si las respuestas son muy pocas.[29] Como ha advertido AMADITZ "(U)n spammer puede enviar avisaje a través del correo electrónico a un millón de personas por la suma de cien dólares. A este precio, aún si un solo receptor entre diez mil responde, el spammer puede obtener beneficios y olvidar a los restantes 9.999 enojados receptores."[30]

Una segunda razón de carácter económico milita a favor del spam. En el caso de la publicidad por correo normal la tasa de conversión (conversion ratio) es entre 0,5 – 2% en el caso del marketing a través de correo electrónico, esta asciende entre 5 –15%. Igual cosa sucede entre el marketing a través de correos electrónicos y la publicidad de banners la que, en los Estados Unidos ha caído hasta un 0,65%.[31]

En pocas palabras, el envío de correos electrónicos comerciales masivos no deseados es barato y produce resultados.[32] En este sentido, constituye una práctica absolutamente inédita, "no existe otra forma de avisaje que se le pueda comparar".[33]

---

[29] Si bien 10.000.000 de correos parece un número exagerado, según Sorkin, en 1997, una empresa ofrecía 5000.000 correos por US $ 50 (David E. SORKIN, *Unsolicited Commercial E-Mail and the Telephone Consumer Protection Act of 1991*, 45 BUFF. L. REV. 1010 supra 47, 1997. Disponible en http://www.spamlaws.com/articles/buffalo.html. Visitado 11/03/02. Es posible que este ejemplo parezca extraordinariamente alejado de la realidad chilena. El día 28 de Enero de 2002, el dueño de un ISP chileno recibió un correo electrónico con el siguiente texto: " 110 mil email a solo $50.000 + iva...Alrededor de 100.000 e-mail de personas chilenas vinculadas a empresas verán su aviso y conocerán su empresa ¿Cuánto pagaría por un servicio como este?. Ahora puede acceder a este servicio por solo $50.000 + IVA." El día 4 de Abril, la misma persona recibió la siguiente comnicación: (asunto) e-mailing llegue a 350.000 personas. "LLEGAR A 300.000 PERSONAS PUEDE HACER LA DIFERENCIA Somos expertos en e-mail marketing.Promocione su Empresa - Sitio Web - Eventos - Productos – Servicios. Más de 65 campañas para grandes y pequeñas empresas Sistemas de supervisión de envíos de correos para su tranquilidad. 350.000 direcciones de correos electrónicos (e-mail). Bases de datos segmentadas por categorías. Servidores propios. $1.- Por cada mail enviado. Garantizamos el envió de los e-mail y entregamos un sistema de supervisión en línea de envíos. Envió mínimo de 100.000 e-mail."

[30] AMADITZ, Keneth: *Canning "Spam" in Virginia: Model Legislation to Control Junk E-mail.* VA. J.L. & TECH. 4, 1999. Disponible en http:/vjolt.student.virginia.edu/graphics/vol4/home_art4.html. Visitado 14/112001.

[31] Las cifras pertenecen a un estudio de Forrester Research citado en Unsolicited Commercial Communications and Data Protection. cit. P. 13

[32] Estas dos características han llevado a algunos comentaristas a afirmar que el envío de spam desplazaría en definitiva a otras especies de marketing directo. Ver Tad Clarke: *Is E-Mail a Threat?* DMNews. Disponible en http://dmnews.com/cgi-bin/artprevbot.cgi?article_id=19792. Visitado 26/03/2002.

[33] EVANS, James, *Putting the Lid on Junk E-Mail*, citado en *Canning "Spam" in Virginia: Model Legislation to Control Junk E-mail.* Cit. nota 104.

El problema del costo.- Que los spammers no soporten la mayoría del costo de su actividad no significa que dicho costo no sea asumido por alguien. Como ya ha sido suficientemente acreditado, los costos siempre se radican en alguien, el problema es decidir en quién.[34] En el caso del envío de spam los costos son soportados básicamente por los proveedores de servicios de Internet y los usuarios que reciben correo comercial masivo no solicitado.

El problema más serio suele ser de los proveedores de servicios. El spam representa una proporción significativa del tráfico de correos electrónicos, consumiendo de esta manera cantidades relevantes de ancho de banda, memoria, espacio de almacenamiento y otros recursos.[35] Según un Reporte sobre marketing directo evacuado por la Commision Nacionelle de l´ínformatique et le liberté

> (para los proveedores de servicios el spam representa un) peso adicional en sus recursos financieros, humanos, técnicos y comerciales que resulta proporcional al número de sus suscriptores. Financiero y humano en términos del tiempo gastado por los funcionarios, algunos de los cuales se encuentran asignados a jornada completa a batallar contra el spam (los sistemas de monitoreo y detección pueden requerir una operación de 24 horas diarias) mientras otros tienen que responder a las críticas recibidas por parte de los suscriptores. Técnicos en términos del significativo volumen de ancho de banda consumido por un mensaje de correo electrónico enviado simultáneamente a una extensa cantidad de suscriptores. Por lo tanto, se debe proveer más ancho de banda que el que sería necesario si solo se satisficieran las necesidades regulares de los suscriptores. Comercial en términos de la asunción común de parte de los usuarios que sus direcciones de correo electrónicos fueron impropiamente reveladas a terceras partes por sus respectivos proveedores de servicios de Internet.[36]

Junto a los costos monetarios aún pueden registrarse dos problemas más. El primero consiste en la atención de las quejas de los clientes del proveedor de servicios que están recibiendo correos no deseados.[37] El segundo problema tiene

---

[34]Como resulta bien sabido, este es el problema que subyace al planteamiento de Ronald COASE en *El problema del coste social.* (en COASE, Ronald: LA EMPRESA, EL MERCADO Y LA LEY. Alianza Editorial. Madrid: 1994 pp. 121 - 164)

[35] Según KHONG:

> de acuerdo al reporte de una firma de seguridad en Internet, 14% de los correos electrónicos corresponden a spam. Netcom, un proveedor de servicios de Internet (ISP), reporta que el spam incrementa los costos de soporte entre un 15% y un 20%, los de administración alrededor de un 20%, los de descarga de correos entrantes en un e10%, reduce el espacio en el disco alrededor de un 15% y aumenta los costos totales por equipos entre un 10 y un 15% (*"Spam Law for the Internet."* cit. S/P. Las citas se han omitido).

[36] Citado en Unsolicited Commercial Communications and Data Protection. cit. Pp. 94, 95

[37] De acuerdo a cifras entregadas por la Federal Trade Commision, en 1998, recibía 1.500 reclamos diarios por spam. En el caso America Online, Inc. v. IMS, America Online alegó que la práctica del demandado (un spammer) había producido, entre otras consecuencias, 50.000 quejas de afiliados a AOL (Ambos datos citados en FASANO, Cristopher: *Getting Rid of Spam:*

que ver con la pérdida de reputación de los proveedores de servicios de Internet. Una práctica común de los spammers consiste en utilizar direcciones de correo falsas, pertenecientes a proveedores de servicios que no poseen relación con el spammer. Para quien recibe el correo electrónico, sin embargo, el proveedor de servicios que aparece en la dirección del correo es quien permite el uso de sus instalaciones para el envío de correos no solicitados. Junto a la pérdida de reputación, dichos proveedores pueden verse expuestos a ataques de algunos de los receptores de la publicidad no deseada.[38]

Junto a los proveedores de servicios, los segundos afectados son los usuarios de Internet. Quien recibe correos no deseados en su casilla electrónica utiliza su tiempo y dinero para procesarlos. Como ha advertido MIKA:

> (S)i una persona no dispone de filtro, o quien envía los correos electrónicos ha encontrado una forma de eludir el filtro, el receptor de los correos electrónicos debe ocuparse de ellos. Ocuparse de ellos toma tiempo por el cual el usuario debe pagar y el espacio físico que utiliza el mensaje puede disminuir la capacidad de un sistema o consumir espacio que, de otra manera, sería necesario para el procesamiento de tareas más importantes. En este sentido, el receptor de correos no solicitados esta pagando parte del costo por algo que ella o él no desea, ya sea que este costo sea monetario o en otros recursos.[39]

Además de los proveedores de servicios y a los usuarios, el spam puede producir un daño más global a la Red. La proliferación incontrolada del spam podría tener un cierto efecto paralizante sobre Internet, ya sea porque el contenido de los mensajes de publicidad –buena parte de ellos sobre sitios pornográficos con lenguaje extraordinariamente explícito o imágenes suficientemente elocuentes[40]- disuada a los usuarios dejen de interactuar en la Red por temor a que sus datos sean recogidos por spammers o por que el número de correos electrónicos no solicitados simplemente sature la Red.[41]

Addressing Spam in Courts and in Congress. P. 4. Citas omitidas. Disponible en http://www.law.syr.edu/studentlife/pdf/fasano1.pdf. Visitado 11/01/2001

[38] Ver *Technical and Legal Approaches to Unsolicited Electronic Mail.* cit. P. 341

[39] MIKA, Karin: *Information v. Commercialization: The Internet and Unsolicited Electronic Mail,* 4 RICH. J.L. & TECH. 6 (1998) S/P. Disponible en http://www.richmond.edu/jolt/v4i3/mika.html. Visitado 05/03/2002 Sobre lo mismo ver supra nota 2.

[40] Según información proporcionada por CISCO Systems Chile durante 1999, el 30,2% de los e-mail no solicitados poseían contenido pornográfico, 29,6% consistía en ofertas para "hacerse rico", 23,5% buscaba vender otros productos o servicios, 9,9% ofrecía productos relacionados a la salud y 3,3% ofrecía entrada a sorteos o a juegos de azar. Ver http://www.cisco.com/global/CL/cs/ic/de/internet_privacidad.shtml. Visitado 09/04/2002

[41] En este sentido GAUTHRONET Y DROUARD reportan que:

> Existen actualmente 234 millones de usuarios de Internet y es posible que alcancen los 300 millones a fines del 2000. Si se asume que tarde o temprano cada empresa de "marketing email" adquirirá la capacidad técnica de transmitir 100 millones de correos electrónicos al día, los usuarios de Internet podrían quedar potencialmente sobrepasados por la inundación de mensajes –200 emisores que posean esa

Como ha advertido AMADITZ el problema que se presenta en el caso del envío masivo de correos electrónicos puede ser comprendido a la luz de la *tragedia de lo común*, expuesta por primera vez por HUME y popularizada algunos siglos más tarde por Garret HARDIN[42] entre otros. Los incentivos de los spammers se encuentran distribuidos para que estos envíen tantos correos como les permita su capacidad técnica. Las externalidades negativas de esta actividad, sin embargo, podrían llevar a que, en definitiva, el sistema colapsara y que cada uno de los spammers se encontrase en una situación peor que en aquella que se hubiese encontrado de moderar su envío de correo no solicitado.

Lo anterior, por supuesto, no es algo inédito en la historia de la humanidad. A estas alturas es un lugar común que un conjunto de sujetos buscando maximizar su bienestar individual pueda producir subóptimos sociales –quizás el celebre *dilema del prisionero* sea la mejor forma de ilustrar esto. Lo que sugiere, sin embargo, este problema es que resulta necesario hacerse cargo de él. Sobre cómo se ha enfrentado el spam y las ventajas y desventajas de cada respuesta trata la próxima sección.

4. Regulando el spam.

He afirmado más arriba que para examinar las posibilidades de regular el spam utilizaré el esquema presentado por Lawrence LESSIG para examinar la regulación del ciberespacio.[43] Conviene entonces explicar, en sus términos más gruesos, este esquema.

> capacidad podrían significar 20 mil millones de correos electrónicos comerciales enviados cada día. Cada navegante de la Red recibiría un promedio superior a 60 correos electrónicos diarios, lo que, atendido el estado de la tecnología actual le tomaría una hora bajar. Lo anterior es sin considerar el incremento en el uso de contenido de video y fotográfico en los correos comerciales (Unsolicited Commercial Communications and Data Protection. cit. P. 66).

Los pronósticos anteriores corresponden a 1999 y no se encontraban desencaminados. Recientemente, Joyce Graff, vicepresidente de Gartner Group (una de las consultoras más prestigiosas en temas relacionados con comercio electrónico), ha informado que la cantidad de spam en la Red ha crecido dieciséis veces en los dos últimos años. Ver Lou Hirsch: *The Problem of Fighting Spam.* EcommerceTimes.com. Disponible en http://www.newsfactor.com/perl/story/16874.html. Visitado 28/03/2002.

[42] Como es bien sabido, para ilustrar la tragedia de lo común, HARDIN utiliza el ejemplo de una llanura abierta al uso de todos los pastores, de manera que cada uno de ellos podrá llevar todo el ganado que desee a pastar. Mientras el número de animales se mantenga bajo no habrá problema. En la medida que aumenten, sin embargo, el pasto se irá transformando en un bien escaso hasta agotarse. Lo anterior sucederá porque cada pastor tiene incentivos para llevar a pastar la mayor cantidad posible para él de animales toda vez que interioriza la ganancia de cada nueva cabeza que integra. El problema es que cada nueva cabeza posee un costo para el prado, ese costo, sin embargo, no es asumido por el pastor (ver HARDIN, Garrett: *The Tragedy of the Commons.* En ACKERMAN, Bruce: ECONOMIC FOUNDATIONS OF PROPERTY LAW. Little Brown and Comapny. Boston and Toronto, 1975. P. 4.

[43] Ver supra nota 4

El esquema de LESSIG.- Para LESSIG, la conducta humana puede ser regulada utilizando cuatro modalidades, el derecho, las normas sociales, el mercado y la arquitectura.[44]

La forma en que regulan las normas jurídicas según LESSIG se asemeja al sistema de precios sombra postulado por autores como POSNER.[45] De acuerdo a este modelo, las sanciones que se adjuntan a determinadas conductas representarían el costo –o precio sombra- de esas conductas. Se trata de sanciones aplicadas al sujeto en forma centralizada por un órgano que posee el monopolio de la fuerza.

Junto a las normas jurídicas existen un segundo conjunto de normas que constriñen la conducta de las personas. Estas son las normas sociales. Coinciden con las jurídicas en que los incentivos de la conducta quedan determinados por sanciones ex post. Difieren, sin embargo, en el hecho que dichas sanciones son aplicadas descentralizadamente.

Una tercera modalidad de regulación de la conducta en el recuento de LESSIG es el mercado. Por mercado el autor, entiende el sistema de precios explícitos. Buena parte de las cosas que se hagan o no dependerán del acceso que se tenga a los bienes necesarios para llevar a cabo aquello que desea hacerse.

La cuarta modalidad de regulación es la arquitectura. LESSIG entiende por arquitectura "el mundo físico tal como lo conocemos."[46]

Estas cuatro modalidades regulan la conducta de los sujetos independientemente de si esta tiene lugar en el espacio real o en el ciberespacio. De esta manera existen leyes que sancionan el robo con violencia e intimidación en las personas y leyes que sancionan violaciones a la propiedad intelectual en las plataformas digitales. Existen normas sociales que regulan qué decir en una reunión y normas sociales que regulan qué escribir en un grupo de discusión.[47] Los precios constriñen nuestras posibilidades de viajar a Europa una vez al año en primera clase y limitan nuestra posibilidad de disponer de una conexión a Internet por cable para cada uno de los miembros de la familia. Finalmente, la arquitectura de una ciudad favorece la interacción social si posee amplios espacios verdes accesibles a todos sus habitantes, la lesiona si los espacios verdes son

---

[44] Ver *The Law of the Horse: What Cyberlaw Might Teach?* cit. Pp. 506-511

[45] Ver, POSNER: Richard EL ANÁLISIS ECONÓMICO DEL DERECHO. Fondo de Cultura Económica. México D.F.: 1998.

[46] *The Law of the Horse: What Cyberlaw Might Teach?* cit. P. 507

[47] Ver ibid. p. 508

reemplazados por malles. Asimismo la arquitectura –o el **código**[48] en el caso de las plataformas digitales- regula la conducta en el ciberespacio, determinando a qué lugares se puede ingresar y a cuáles no, a dónde se recolecta información y en cuales se respeta el derecho a la privacidad del sujeto, etc.

[48] El *código* es una pieza central en el análisis de LESSIG. Conviene, por lo mismo, detenerse en él. En una extensa nota a pié de página LESSIG lo explica de la siguiente forma:

> "Como defino la expresión *código* refiere al software y hardware que configura el ciberespacio como es -o más exactamente, las reglas contenidas en el software y hardware que unidos configuran al ciberespacio como es. Obviamente existe un montón de "código" que calza con esta descripción, y obviamente la naturaleza de ese código puede variar dramáticamente dependiendo del contexto. Algunos de estos códigos están dentro del nivel del Protocolo Internet (IP), donde operan los protocolos para intercambiar información en Internet incluyendo TCP/IP). Algunos de estos códigos están sobre este nivel IP, o como lo ha puesto Jerome H.Saltzer están como su "límite" (end);
>
> > En el caso de la transmisión de los sistemas de comunicación de información, este rango incluye encriptación, detección de duplicación de mensajes, secuenciamiento de mensajes, entrega garantizada de mensajes, detección de fallas de anfitrión, y recibos de envíos. En un contexto más amplio, el argumento parece aplicarse a muchas otras funciones del sistema operativo de un computador, incluyendo su sistema de archivos.
>
> Jerome H. Saltzer, David P. Reed & David D. Clark, *End-to-End Arguments in System Design,* in INNOVATIONS IN INTERNETWORKING 195, 196 (Craig Partridge ed., 1988). Más generalmente, este segundo nivel incluiría cualquier aplicación que pudiera interactuar con los programas de red (navegadores, programas e-mail, transferencia de archivos) así como con las plataformas de sistemas operativos sobre las cuales estas aplicaciones deberían funcionar.
>
> En el análisis que sigue, el "nivel" más importante para mi propósitos será aquel que se sitúa sobre el nivel IP. Atendida la adopción de la Red del sistema "extremo de a extremo" (en la descripción de Saltzer el sistema de extremo a extremo [end to end] describe el principio que guió la construcción de Intenet, esto es la inteligencia de la red se sitúa en los extremos, manteniendo la red simple. [*N. del A.]*), las regulaciones más sofisticadas ocurrirán a este nivel. *Ver también infra* 24; *cf*. Timoty Wu, *Application-Centered Internet Analysis,* 85 VA. L. REV. 1163, 1164 (1999) (argumentando que el análisis legal de Internet enfocado hacia el usuario necesariamente debe focalizarse en este nivel)." (ibid. nota 15)

Una definición más sencilla de código es como "las instrucciones que ejecutan los computadores." De esta manera, al utilizar la palabra código estamos refiriendo a aquellas instrucciones que dirigen las funciones de los computadores. Algunas de ellas permiten sus funciones más básicas, otras permiten el procesamiento de palabras, música o imágenes visuales, y otras facilitan la interconexión con otros computadores (ver *Developments in the Law-The Law of Cyberspace: the Long Arm of Cyber-reach,* 112 HARV. L. REV. 1610 (1999) S/P. Disponible en http://www.harvardlawreview.org/issues/112/7_1577.htm#fnstar. Visitado 20/03/2002).

Utilizando el derecho para regular el spam[49].- Actualmente existe un nutrido conjunto de normas legales que regulan el tratamiento de datos personales y, con diversidad de enfoques y mayor o menor intensidad, el spam.[50] Aún cuando no es posible examinar detalladamente aquí la fisonomía de las distintas regulaciones, un rápido examen de algunas proposiciones para regular el spam puede dar noticia acerca de los contornos entre los cuales se mueven los cuerpos normativos. Siguiendo el enfoque de AMADITZ[51] pueden considerarse cinco opciones al momento de regular el spam: (1) la opción prohibitiva, (2) el "etiquetamiento" de spam como spam, (3) la opción anti-fraude, (4) La utilización de bienes muebles sin autorización (trespass to chattels), y (5) la opción "opt out."

(1) En su versión extrema, la opción prohibitiva consiste en proscribir todo tipo de publicidad comercial no consentida. Una versión más popular consiste en prohibir únicamente el envío de publicidad por correo electrónico cuando esta no haya sido solicitada[52] –es decir el receptor haya prestado su consentimiento sobre la recepción de correos- o bien exista una relación anterior entre el emisor y el

---

[49] Atendido el hecho que en la próxima sección reviso una respuesta legal concreta frente al spam, el objetivo de las líneas que siguen es examinar, en términos generales, la fisonomía de estas respuestas y los problemas que subyacen a la regulación del spam cuando se utilizan herramientas legales.

[50] En el caso europeo pueden citarse las Directivas 95/46 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Diario Oficial de las Comunidades Europeas nº L 281 de 23/11/1995 P. 0031 – 0050); la 97/7 relativa a la protección de los consumidores en materia de contratos a distancia (Diario oficial de las Comunidades Europeas nº L 272 de 08/10/1998 P. 0022 – 0022; la 97/66 relativa al tratamiento de los datos personales y a la protección de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones (Diario Oficial de las Comunidades Europeas nº L 024 de 30/01/1998 P. 0001 – 0008); y la Directiva 2000/31 relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico). (Diario Oficial de las Comunidades Europeas nº L 178 de 17/07/2000 P. 0001 – 0016). Las directivas pueden ser consultadas en http://europa.eu.int/eur-lex/es/. Visitado 15/03/2002. Una buena selección sobre legislación nacional a nivel europeo puede encontrarse en Unsolicited Commercial Communications and Data Protection. (cit. Pp. 131-138). Una selección sobre regulación a nivel nacional puede encontrarse en DAVARA, Miguel Angel: LA PROTECCIÓN DE DATOS EN EUROPA. Grupo Asnef Equifax, Universidad Pontificia Comillas ICAI – ICADE. Madrid 1998. En el caso estadounidense, más de una docena de estados han promulgado legislación antispam, entre ellos California, Illinois, Louisiana, Nevada, Tennesse, Virginia, Washington, Connecticut, Delaware, Missouri, Oklahoma, Pennsylvania) (Ver *Technical and Legal Approaches to Unsolicited Electronic Mail.* Ob cit. Supra nota 212). Finalmente, para el caso latinoamericano puede consultarse PUCCINELLI, Oscar: EL HABEAS DATA EN INDOIBEROAMÉRICA. Editorial Temis SA. Santa Fe de Bogotá. 1999. Sobre la situación de algunos otros países –Australia, Canadá, Checoslovaquia, India, Rusia y Yugoslavia- puede consultarse. Spam Laws. Disponible en http://www.spamlaws.com/world.html. Visitado 03/01/2002.

[51] Ver *"Spam" in Virginia: Model Legislation to Control Junk E-mail*. cit. S/P.

[52] Esto es lo que se conoce como opt-in y que ha sido adoptado en Alemania, Austria, Dinamarca e Italia.

receptor.[53] La ventaja de este enfoque es evidente, por una parte reduce significativamente el número de correos enviados y, por otra, solo reciben correos quienes los desean.[54]

(2) El etiquetamiento de los correos comerciales consiste en indicar en el "asunto" (subject) del mensaje su carácter comercial. De esta manera, solo serían permitidos aquellos correos que identificaran con suficiente elocuencia su contenido Etiquetar correos posee dos ventajas. De una parte permite a los usuarios disminuir el tiempo y recursos que utilizan bajando correos, de otra facilita el funcionamiento de los filtros que utilicen los usuarios para evitar el ingreso de publicidad a sus respectivas casillas.[55] [56]

(3) El enfoque anti-fraude consiste en sancionar aquellos correos electrónicos masivos cuando (1) utilizan el nombre de dominio de una tercera parte sin su autorización o, de otra manera, disfrazan el verdadero punto de origen del correo electrónico o (2) contienen información falsa o engañosa en la línea del "asunto" del correo electrónico. La importancia de ambos mecanismos es que endosan dos de los problemas más frecuentes en el envío de correos no deseados, a saber la introducción de nombres de dominio falsos o información de *enrrutamiento* (routing) y el despliegue de información engañosa en la línea de asunto del correo electrónico. Ambas prácticas son utilizadas por spammers más avanzados para

[53] Este enfoque favorece la regulación de esquemas de "opt-in", esto significa que solo se permite el envío de publicidad cuando el receptor ha dado su consentimiento explícito para que se le envíe publicidad. Lo anterior puede funcionar a través de inscripciones en sitios web específicos aceptando el envío de publicidad o bien en listas más generales en las que el receptor acepta el envío de publicidad.

[54] El problema que esto puede tener –además de los problemas comunes a toda la legislación sobre spam- reside en que es poco probable que la exclusión funcione salvo que se tutele la creación de mecanismos que garanticen la obtención del consentimiento por parte de los receptores. He tratado este problema en otra parte (ver de la Maza, Iñigo: *Los límites del consentimiento* en La Semana Jurídica Nº 70, pp. 5 y 6), de manera que es suficiente aquí dejarlo mencionado.

[55] Aunque vuelvo sobre los filtros al examinar el código como regulador en el caso del spam, lo que interesa advertir por ahora es que para trabajar eficientemente los sistemas de filtro requieren algún tipo de señal que les permita discriminar entre correos deseados y correos no deseados (ver *Emerging Media and Regulation of Unsolicited Commercial Solicitations.* cit. S/P).

[56] Un problema que ha tenido la legislación que endosa este tipo de enfoque en los Estados Unidos son las limitaciones que impone la Primera Enmienda al Gobierno para exigir que se etiqueten las comunicaciones comerciales no deseadas. En general, en el caso norteamericano, el Gobierno debe demostrar dos cosas para llevar adelante dicha regulación, a saber: (1) que el etiquetamiento satisface directamente un interés substancial y (2) que la forma en que la norma promueve la satisfacción de este interés es razonable (ver *Garbage In: Emerging Media and Regulation of Unsolicited Commercial Solicitations.* cit. Notas 179 y 180).

engañar a los servidores y a los usuarios sobre la fuente de los correos electrónicos.[57]

(4) Utilización de bienes muebles sin autorización.[58] Cierta legislación basada en un nutrido contingente de casos resueltos por tribunales norteamericanos en los últimos años,[59] ha utilizado esta figura para enfrentar el spam Para que el spammer sea imputable de la utilización no consentida de bienes muebles, quien la alega debe acreditar algún tipo de interferencia sustancial al ejercicio de su dominio. En el caso del spam, quizás el precedente más famoso sea el sentado a partir de Compuserve Inc, v. Cyberpromotions, en el cual Compuserve alegó que el envío masivo de correos electrónicos por parte de Cyberpromotions había producido daño físico al equipo del demandante y, además, había dañado su reputación y buenas relaciones con sus clientes

(5) Opt-out. Las legislaciones que funcionan con esquemas de opt-out permiten el envío de correos masivos no solicitados a menos que el receptor le haya informado al spammer que no desea seguir recibiendo correos (opt-out específico) o bien el receptor se haya incluido en una lista o registro (registros de opt-out) a través de la cual se informa a los spammers que esa persona no desea recibir publicidad. Aunque el opt-out es una de las opciones preferidas al momento de legislar sobre spam[60] presenta en sus dos versiones bastantes problemas. En el caso del opt-out específico, existe alguna evidencia que un número relevante de spammers utiliza las cláusulas de remoción[61] para verificar la dirección de correo electrónico del receptor y no lo remueve de sus registros aún cuando este ha utilizado la cláusula de remoción según las instrucciones del spammer. En el caso

---

[57] Como resulta evidente, el problema de esta solución es que aún las comunicaciones que cumplan con estos requisitos podrían representar una cantidad suficiente para producir problemas a los proveedores de servicios de Internet (quienes deberían invertir en software de filtro y bloqueo) y los usuarios (un ejemplo de esto es el servicio de bloqueo de Hotmail, el cual envía los correos comerciales hacía una carpeta de correo no deseado). El problema de esta solución, sin embargo, es que dicha carpeta utiliza parte del espacio disponible de cada usuario y, en el largo plazo puede saturar la capacidad de la casilla).

[58] Esta figura –el trespass to chattels- es un "tort" que proviene de la práctica jurisprudencial anglosajona del siglo XIX y que se configura cada vez que una persona usa, interfiere o de alguna manera desposee al dueño de un bien mueble tangible (para un análisis crítico del trespass to chattels respecto al spam ver BURKE, Dan: *The Trouble With Trespass*. Disponible en http://papers.ssrn.com/papepr.taf?abstract_id=223513. Visitado 05/04/2002

[59] Para un considerable muestreo de estos casos, ver *Technical and Legal Approaches to Unsolicited Electronic Mail.* Cit. Nota 160.

[60] Ver para los casos europeos y estadounidense: Unsolicited Commercial Communications and Data Protection. Commision of the European Communities. cit. y *Canning "Spam" in Virginia: Model Legislation to Control Junk E-mail.* cit.

[61] Una fórmula clásica de cláusula de exclusión es algo así como si usted no desea recibir esta publicidad envíe un correo a xxxx con el título remuévame o Si no quiere seguir recibiendo este e-mail envíenos un Reply.

de los registros de opt-out, una de las principales críticas es que los mismos registros pueden ser utilizados para recolectar direcciones.[62] En adición a lo anterior, un segundo problema –que, como reviso más adelante, presenta la Directiva 2000/31 reside en la administración de las listas o registros de exclusión, si existe una gran cantidad de ellos es muy improbable que los spammers asuman el costo de revisar cada una de ellas antes de enviar sus correos.

Los límites de la regulación.- Que Internet no puede ser regulada es todavía –aunque cada vez menos- un lugar común en las discusiones de algunos académicos que se dedican al tema.[63] En estos términos tan amplios, sin embargo, la afirmación parece ser incorrecta. El derecho no es la única forma de regular la Red y las soluciones de código y mercado no necesariamente están constreñidas por las limitaciones que sufre el derecho. Con todo, una afirmación más modesta, esto es que el derecho enfrenta obstáculos sustanciales para regular la Red, parece correcta. Estos obstáculos son las limitaciones de las soluciones legales y los reviso a continuación.

El principal problema de la legislación en el caso de Internet es la ausencia de fronteras definidas. En el mundo que conocemos las fronteras demarcan las áreas donde un determinado Estado es soberano de imponer y hacer cumplir su legislación. Como advierten JOHNSON y POST, aún cuando las fronteras sean el producto de accidentes históricos, ellas permiten el desarrollo y la exigibilidad de las leyes.[64] Desde la perspectiva de estos autores, las fronteras geográficas hacen sentido para ley por cuatro razones: el poder, los efectos, la legitimidad y, el aviso.[65]

El poder. Exigir el cumplimiento de normas precisa, como resulta evidente, un cierto grado de capacidad de coacción sobre quienes infrinjan dichas normas. Esta capacidad de coacción en los estados modernos queda determinada por el espacio sobre el cual ejercen su soberanía. Aún si un Estado dispone de legislación que sancione vigorosamente el envío de correos masivos no deseados se encontrará en problemas cuando dichas normas sean infringidas por un

[62] Una posibilidad de esto es la de un spammer que no queda vinculado por las leyes del país que posee las listas y que, por lo tanto no puede ser sancionado por utilizarlas.

[63] Para una selección de ellas ver *The Law of the Horse: What Cyberlaw Might Teach?* cit. nota 13.

[64] Ver JOHNSON, David y POST, David: *Law and Borders—The Rise of Law in Cyberspace*. 48 STAN. L. REV. 1367 (1996). Disponible en http://www.cli.org/X0025_LBFIN.html. Visitado 20/03/2002.

[65] Ver Ibidem S/P Omito explicar la segunda razón, los efectos, porque parece más propia del ejemplo utilizados por estos autores –derecho de marcas- que de spam.

spammer ubicado en otro país. Particularmente si ese otro país no posee tratados o legislación anti spam.[66]

La legitimidad de las legislación y su notificación. Desde Rousseau al menos afirmamos que la última fuente de legitimidad de la ley reside en el hecho que ella plasma la voluntad de los sujetos imperados por ella. Esta legitimidad se fractura al desvanecerse los límites territoriales en que habitan dichos sujetos. Respecto a la noticia, las fronteras físicas entre países constituyen recordatorios para quienes las traspasan del hecho que están ingresando a un espacio regido por leyes determinadas. En el ciberespacio no existe una diferencia relevante a estos efectos en el acceso a un sitio web ubicado en Nueva Delhi, Tokio, La Paz o Santiago de Chile.[67]

Una defensa frente a la "aterritorialidad" de Internet consiste en sostener que esta puede ser corregida a través de tratados internacionales. Esto, sin embargo, supone uniformidad entre las diversas legislaciones sobre spam que, como se ha advertido, a la fecha no existe.[68]

Junto al problema de la aterritorialidad de Internet, aún es posible registrar tres inconvenientes más al momento de utilizar la legislación para regular el envío masivo de correos no solicitados. El primero es el dinamismo de la tecnología, el segundo es la legitimación de ciertas formas de correo no deseado al prohibir otras. Finalmente, el tercero, tiene que ver con la especial protección que suele recibir la libertad de expresión.[69]

---

[66] Ver *Technical and Legal Approaches to Unsolicited Electronic Mail.* cit. p. 381

[67] Como afirman JOHNSON y POST :

> El ciberespacio no tiene fronteras basadas en el territorio ya que el costo y velocidad de envío de la transmisión de un mensaje en la Red es casi completamente independiente de la ubicación física: los mensajes pueden ser transmitidos desde cualquier ubicación a cualquier ubicación sin arruinarse. degradarse o demorarse sustancialmente más y sin que ninguna barrera física o que pueda mantener lugares y personas remotamente alejados separados unos de otros. La Red permite transacciones entre gente que no se conoce, y en muchos casos , entre gente que no puede conocer la ubicación física de la otra parte. La ubicación continua siendo importante, pero solo la ubicación dentro de un espacio *virtual* compuesto por las "direcciones" de las máquinas entre las cuales los mensajes y la información es ruteada (*Law and Borders—The Rise of Law in Cyberspace.* Ob. cit. S/P. Las notas han sido omitidas).

[68] Esto no significa, por supuesto, que dichos acuerdos no se puedan alcanzar. Una proposición sobre la forma de mejorar la cooperación internacional en el combate de las prácticas que lesionan a los consumidores en plataformas electrónicas puede ser encontrada en ROTHCHILD, John: *Protecting the Digital Consumer: The Limits of Cyberspace Utopianism.* 74 Ind. L. J. 893 (1999)

[69] Ambas tratadas en *Technical and Legal Approaches to Unsolicited Electronic Mail.* cit. p. 382-383.

El problema del dinamismo de la tecnología es un desafío para cualquier normativa que intente regular la interacción social en la Red. Sabemos cómo funciona Internet hoy y la forma en que se desarrollan algunas conductas que nos parecen reprobables. El problema, sin embargo, es encontrar formas de fijar esas conductas en tipos que resulten suficientemente flexibles para evitar su obsolescencia si la tecnología que regulan es modificada.[70]

Al proscribir legalmente algunas formas de correo electrónico no deseado se legitiman otras. SORKIN utiliza como ejemplo el caso del etiquetamiento y el opt-out.[71] Si bien es cierto que si los spammers cumplen con ambos requisitos se facilitará la filtración y el bloqueo de correos no deseados, esto no disminuirá –no substantivamente al menos- el número de correos en la Red, por el contrario, existe alguna posibilidad que en el corto plazo los aumente. Si esto es así, este tipo de legislación no evitará la tragedia de lo común que ha sido advertida más arriba.

Finalmente, el tratamiento privilegiado de la libertad de expresión. Aunque este no sea el lugar para tratar en detalle el problema, conviene anotar que, en general, los legisladores se encuentran con ciertas limitaciones al momento de regular la expresión, el spam contiene una especie de discurso, comercial o no según la definición que se utilice, por lo tanto queda cubierto por estas limitaciones.[72] [73]

Regulando a la sombra de la ley: la utilización de normas sociales para la regulación de la Red.- Existen dos discusiones cercanas a la utilización de normas sociales para regular la conducta en Internet. La primera de ellas tiene que ver con la posibilidad de utilizar esquemas de regulación privada en la Red[74], la segunda, con la deseabilidad de dichos esquemas.[75] En lo que sigue me interesa revisar únicamente la posibilidad –no la deseabilidad- de utilizar una modalidad de regulación privada para regular el spam: las normas sociales.

---

[70] En el caso del spam algunos de los resultados de esta obsolescencia frenética pueden ser consultados en *The Trouble With Trespass.* cit.

[71] Ver *Technical and Legal Approaches to Unsolicited Electronic Mail. Cit.*

[72] No obstante lo anterior, en el caso chileno estas limitaciones podrían ser menos intensas (ver supra nota 12)

[73] El tratamiento de este problema en la práctica jurisprudencial estadounidense puede ser consultado en *Developments in the Law-The Law of Cyberspace: the Long Arm of Cyber-rea.* cit.

[74] Sobre esto puede revisarse LEMLEY, Mark: *The Law and Economics of Internet Norms.* (BORRADOR) Disponible en http://www.law.berkeley.edu/institutes/law_econ/workingpapers/PDFpapers/olinwp98_12.PDF Visitado el 04/01/2002

[75] Una magnífica exposición sobre esto en WEINSTOCK, Netanel: *Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory.* Disponible en www.utexas.edu/law/faculty/nnetanel/primary.pdf Visitado 06/01/2002

Las normas sociales constituyen una modalidad de regulación privada caracterizada por un acuerdo tácito sobre la validez de un cierto esquema normativo.[76] En el caso de Internet este tipo de acuerdos tácitos constituyeron, en los comienzos, la forma más común de regular la interacción social. Como ha señalado SORKIN:

> Aproximadamente hasta 1996 la presión social fue el enfoque predominantemente utilizado para combatir el spam. Particularmente en las primeras etapas de Internet, las reglas informales de netiqueta (netiquette) y algunas políticas de uso aceptables perdidas por ahí, prohibían o al menos desincentivaban la mayoría de los usos comerciales de Internet. El spam, y en menor grado toda la actividad comercial, poseía un estigma suficiente para disuadir a la mayoría de los usuarios de Internet de incurrir en ella.[77]

Como lo ha advertido LEMLEY, el problema con este tipo de regulación, es que únicamente parece funcionar en comunidades pequeñas que presentan escasos cambios en el tiempo en la composición de sus miembros.[78] Tanto la internalización de las normas sociales como la sanción por su incumplimiento se ven perjudicadas en comunidades demasiado extensas, particularmente cuando la composición de estas presenta altos grados de dinamismo.

En el caso de Internet, la comunidad original estaba compuesta por un grupo pequeño y homogéneo de programadores y hackers que compartían una cierta visión de la Red. El grupo, sin embargo, ha crecido, actualmente la "comunidad Internet" cuenta con alrededor de 500 millones de miembros[79] distribuidos alrededor de todo el mundo. En este escenario resulta difícil pensar en la internalización de normas sociales o en una sanción por su incumplimiento.[80]

---

[76] Esta característica distingue a las normas sociales de otros esquemas de regulación privada como la regulación horizontal a través de contratos. El problema del spam, sin embargo, es que los costos de transacción involucrados dificultan la utilización de esquemas contractuales para regular privadamente el spam.

[77] *Technical and Legal Approaches to Unsolicited Electronic Mail.* cit. p. 341-342 (citas omitidas).

[78] *The Law and Economics of Internet Norms.* cit. p. 12

[79] Ver CyberAtlas. http://cyberatlas.internet.com/big_picture/geographics/article/0,,5911_151151,00.html. Visitado 22/03/2002.

[80] Respecto a esto último, LEMLEY afirma

> En la medida que el tamaño de un grupo aumenta resulta menos probable que todos sus miembros sigan compartiendo una comunidad de intereses. Los miembros comienzan a sentirse anónimos y, por lo tanto, a sentir menos presión social sobre sus acciones. Alguien podría sentirse avergonzado de transgredir una barrera moral en frente de personas que conoce, pero deseoso de hacerlo en frente de extraños (*The Law and Economics of Internet Norms.* cit. p. 14)

Respecto de esto último, a diferencia de los mecanismos de regulación legales, la sanción del incumplimiento de normas sociales carece de un ente centralizado que la aplique. Aún cuando exista un cierto consenso respecto a la reprochabilidad de una práctica, la aplicación de la sanción se encuentra distribuida al interior de la comunidad. En el caso del spam, la sanción suele estar de cargo de tres actores: los proveedores de servicios de Internet, algunas asociaciones empresariales, generalmente relacionadas con servicios de marketing y los "vigilantes".

Proveedores de servicios de Internet. Un gran número de proveedores de servicios de Internet contempla entre sus términos de servicios la prohibición a sus suscriptores de incurrir en envío masivo de correo no deseado. Como ha puesto de relieve CARROLL, sin embargo, algunas de las prohibiciones son equívocas, de manera que la prohibición puede referirse únicamente al envío de correos no deseados a suscriptores de ese proveedor. Otro problema advertido por el mismo autor es que los mismos proveedores pueden obtener ganancias vendiendo a spammers las direcciones de sus propios suscriptores o enviar ellos mismos correos no deseados a sus suscriptores.[81]

Asociaciones empresariales. Algunas asociaciones empresariales relacionadas con marketing -por ejemplo la Direct Marketing Association (DMA) y la Association for Interactive Media en el caso estadounidense- han manifestado su rechazo frente al spam, sin embargo, al menos en estos dos casos, su oposición no ha sido especialmente vigorosa.[82] El caso europeo es distinto, según reportan GAUTHRONET y DROUARD: "casi todas las asociaciones de comercio a través de venta a la distancia ha manifestado su oposición en principio al spam."[83]

Los vigilantes. Se trata en este caso de personas privadas que actúan en la Red sancionando a quienes incurren en actividades relacionadas con spam. De esta manera, alguna de las técnicas empleadas para sancionar son poner a los spammers en listas negras, "llamear" (flaming) al spammer o bien utilizar programas llamados Cancelbots que borran automáticamente los avisos múltiples puestos en grupos de discusión. Si no es posible identificar al spammer, entonces se sanciona al proveedor de servicios desde donde se enviaron los correos.[84]

---

[81] Ver *Garbage In: Emerging Media and Regulation of Unsolicited Commercial Solicitations.* cit. S/P. Un ejemplo del uso que hacen los proveedores de servicios de Internet de la información de sus clientes queda suficientemente ilustrado en la oposición de America Online, Yahoo y otros grandes proveedores de servicios de Internet frente a la discusión de una ley que les prohibe revelar información personal de us suscriptores, por ejemplo, los sitios que estos visitan. Ver Associated Press: Bill would ban ISPs from disclosing customer information. Disponible en http://www.startribune.com/stories/535/2218646.html. Visitado 10/04/2002.

[82] Ver *Technical and Legal Approaches to Unsolicited Electronic Mail.* cit. p. 343 – 344

[83] Unsolicited Commercial Communications and Data Protection. cit. p. 88. No obstante esto, como los mismos autores advierten, el deficiente diseño de la normativa que controla las comunicaciones comerciales no consentidas en la Directiva 2000/31 sería, en parte, el resultado de presiones de las asociaciones de marketing. Reviso esto más adelante.

[84] Ver *Garbage In: Emerging Media and Regulation of Unsolicited Commercial Solicitations.* cit. S/P

El caso de los vigilantes ilustra aquello de tomar la justicia en las propias manos, con todas sus ventajas y riesgos. Por una parte, el vigilantismo contribuye a solucionar la falta de posibilidades sancionar a quienes violan una norma social comúnmente aceptada. Sin embargo su falta de institucionalización transforma el vigilantismo en una práctica con escasos niveles de predictibilidad y amplios márgenes de error y arbitrariedad.[85]

El resultado de la aplicación de normas sociales como mecanismos reguladores del spam no es parejo. En Estados Unidos, por ejemplo, los miembros de la Asociación de Marketing Directo (DMA) han intentado enfrentar el problema del spam con mecanismos autorregulatorios. Estos mecanismos, sin embargo, han tenido escaso éxito. Para SORKIN, la explicación de lo anterior tiene que ver con dos razones, la primera es que el spam siempre ha sido una actividad que ha operado al margen de las convenciones sociales, por lo mismo, es poco lo que la presión social puede hacer sobre ella. La segunda es que este tipo de mecanismos carece, por lo general, de métodos suficientes para llevar adelante las sanciones.[86]

Como se ha observado, el caso europeo difiere del escenario estadounidense. En el primero parece existir una cierta cultura de la privacidad que contribuye decididamente a disuadir la práctica masiva de spam.[87] En palabras de GAUTHRONET y DROUARD:

> Europa posee una intensa cultura de protección de datos personales de la cual se encuentra impregnada la industria de ventas a la distancia tradicional. Todos los estados miembros poseen una ley general de protección de datos y una autoridad supervisora, la cual, en algunos casos, ha estado funcionando durante muchos años. Este marco institucional y legal enfatiza el cuidado de los asuntos relacionados con la protección de datos entre las empresas de marketing directo quienes se muestran crecientemente sensibles a la mala publicidad y al daño a sus negocios que puede

[85] Un ejemplo de esto. En 1998 el administrador de red de MIT (Massachusetts Institute of Technology) comenzó a recibir reclamos de los usuarios del sistema de MIT señalando que los correos que dirigían hacía afuera del sistema rebotaban. La razón de lo anterior era que un vigilante, ORBS (Open Relay Behavior-modification System) había puesto a MIT en su lista negra. De esta manera, los suscriptores a la lista negra de ORBS comenzaron a excluir automáticamente los correos de MIT. El motivo del bloqueo es que MIT utiliza un protocolo de correos (SMTP) que permitía a terceras partes enviar correos sin disponer de cuentas en el sistema de correos primario (una descripción más completa puede ser encontrada en *The Law of the Horse: What Cyberlaw Might Teach?* cit. p. 544-545.)

[86] Ver *Technical and Legal Approaches to Unsolicited Electronic Mail.* cit. p. 343 – 344.

[87] Quizás sea más preciso decir que dicha cultura contribuye a controlar el envío de spam de manera que no alcance las proporciones de países como Estados Unidos. En el caso francés, por ejemplo, se enviaron 79,5 millones de comunicaciones comerciales no deseadas durante Diciembre de 2001. Ver Euromedia.net: Promotional e-mails most common in France. Disponible en http://www.europemedia.net/shownews.asp?ArticleID=9554. Visitado 25/03/2002

> resultar de las quejas o de la sanción oficial en relación a la violación de la privacidad.[88]

Si bien es cierto que Europa parece poseer una cultura sobre la privacidad más intensa que la de países como Estados Unidos y, por supuesto, Chile, resulta difícil en el caso europeo desagregar la presión social de las sanciones legales. Como ya se ha advertido, la mayoría de los países europeos posee legislación que protege la privacidad intensamente y autoridades especiales cuya misión es vigilarla.

Como sea, con prescindencia de la intensidad que ejerza la presión social, parece más o menos evidente que por si misma resulta insuficiente cuando se trata de regular el spam.

Levantad la viga maestra carpinteros[89]*: utilizando el código para regular*.- En general, la utilización del código en la regulación de la conducta no constituye una modalidad separada sino una forma de exigir el cumplimiento de normas legales o normas sociales.[90] No obstante lo anterior, la ley y las normas sociales pueden actuar sin utilizar soluciones de código y el código puede ser utilizado al margen de las normas sociales y la ley,[91] es por esta razón que lo trato como una modalidad separada.

Buena parte de los problemas que genera el spam tienen que ver con el diseño del protocolo de transferencia de los correos electrónicos que mayoritariamente se usa. La arquitectura inicial del correo electrónico no fue pensada para permitir la autentificación de quienes enviaban correos.[92]

[88] Unsolicited Commercial Communications and Data Protection. cit. p. 90

[89] La frase, por supuesto, corresponde al título de una pequeña novela de J.D. SALINGER

[90] En ambos casos el código es el regulador directo y la ley y las normas sociales reguladores indirectos (para una explicación de la regulación directa e indirecta ver LESSIG, Lawrence: CODE AND OTHER LAWS OF CYBERSPACE. Basic Books, Nueva York, 1998. Pp. 92-95.

[91] Algunos ejemplos: (1) derecho regulando la conducta en Internet sin utilizar soluciones de código: artículos 4 y 23 de la Ley 19.628 sobre protección de la vida privada. El primero señala los requisitos que deben satisfacerse para tratar datos y el segundo las sanciones en caso de incumplimiento. (2) Normas sociales regulando las conductas en Internet sin utilizar soluciones de código: acuerdos de las empresas de Marketing para evitar el spam. (3) Código regulando las conductas al margen de la ley y normas sociales: los sistemas de confianza (trusted systems) que se utilizan para proteger los derechos de autor en la Red. En este caso la protección que entregan excede claramente la prodigada por la ley a los derechos de autor. Por otra parte, no existe ninguna norma social que sancione el uso justo (fair use) que estos sistemas evitan (una explicación más detallada de esto puede ser encontrada en *The Law of the Horse: What Cyberlaw Might Teach?* Cit. p. 528), por el contrario, la opinión mayoritaria es que estos sistemas alteran el equilibrio entre el derecho de propiedad del autor y el derecho de acceso general (ver Ibidem y *Developments*).

[92] En palabras de LESSIG:

Una posibilidad de combatir el uso indebido de sistemas de correo para enviar spam consiste en alterar la arquitectura de los sistemas de correos evitando el envío de terceras partes. El problema, sin embargo, es que mantener los sistemas abiertos, aceptando el envío de terceras partes posee ciertas ventajas para quienes manejan estos sistemas, ventajas que perderían en sistemas cerrados.

El envío de terceras partes no es, sin embargo, la única técnica utilizada por los spammers. Es perfectamente posible ubicar un proveedor de servicios de Internet que no posea reglas sobre envío de spam y utilizarlo como plataforma de operación. Junto a lo anterior es posible utilizar nombres de dominio falsos o simplemente inexistentes en el encabezamiento del mensaje para evitar respuestas airadas.[93] Para este tipo de problemas existen dos soluciones a nivel de la arquitectura del correo electrónico, los filtros y los bloqueadores.

Un filtro no tiene porque ser una herramienta tecnológica. En su nivel más básico la actividad de filtraje consiste únicamente en la revisión de los "asuntos" de los correos electrónicos eliminado aquellos cuyos títulos resulten sospechosos. Una solución más sofisticada a nivel de usuario –esta vez utilizando el código[94]- consiste en utilizar software que elimine automáticamente mensajes en el servidor sin que sea necesario bajarlos a la casilla del usuario. [95] [96]

Estos últimos filtros simplemente eliminan o modifican el enrrutamiento de los mensajes que poseen determinadas características. De esta manera, el usuario

---

> (L)as ganancias del spam son una función del diseño del correo electrónico. La arquitectura inicial de los correos electrónicos hacía poco por identificar a los usuarios que enviaban mensajes electrónicos. SMTP (Simple Mail Transport Protocol), por ejemplo, que es aún protocolo de correos dominante, permite el envío de correos por terceras partes sin que estas dispongan de una cuenta de correo en el sistema de correos primario. Con los sistemas SMTP configurados para aceptar el envío de terceras partes, yo puedo dirigir mi correo para que sea enviado a través de estos sistemas aún si no dispongo de cuenta en esos sistemas. De esta manera, los spammers pueden usar los sistemas que permiten el envío de terceras partes para inundar la Red con correos electrónicos (Ibidem. P. 543, citas internas omitidas).

[93] Ver *Technical and Legal Approaches to Unsolicited Electronic Mail.* Cit. p. 364

[94] A nivel de código el filtro puede ser definido como un conjunto de instrucciones que impiden el acceso de ciertos mensajes según las preferencias del usuario. Como reviso algo más abajo, los filtros no solo pueden ser utilizados a nivel usuario, sino además por terceras partes como portales, motores de búsqueda y proveedores de servicios de Internet. Ver *Developments* S/P

[95] Ver *"Spam Law for the Internet"* cit. S/P

[96] Dos ejemplos de esto son las opciones de filtro que ofrecen Microsoft Outlook y Eudora.

puede excluir correos electrónicos según el remitente[97], el asunto o de otra manera que decida.[98]

Con prescindencia del nivel del filtro, casi todas las técnicas de filtro resultan en falsos positivos, esto es mensajes legítimos identificados como spam.[99] En virtud de lo anterior resulta útil mantener una carpeta de correo no deseado –como la disponible en las casillas Hotmail. El problema de esto es que para disponer de esa carpeta deben bajarse los mensajes, perdiendo buena parte de las ventajas del filtro.[100] Junto a lo anterior, como el filtro depende de las instrucciones que le sean dadas para discriminar entre aquellos mensajes que pueden ingresar a la casilla y aquellos que deben ser eliminados en el servidor, es posible detectar esas instrucciones –al menos las más comunes- y burlarlas con mensajes cuyos remitentes estén alterados, el "asunto" del correo no corresponda a su contenido, etc.

Una segunda posibilidad en el caso de los filtros es que estos se implanten no a nivel del usuario sino por terceras partes como los proveedores de servicios de Internet o empresas especialmente dedicadas a esto. Las ventajas de asignar esta tarea a terceros especializados tiene que ver con la mayor experiencia y capacidad técnica de estos. Junto a estas ventajas, sin embargo, la solución presenta algunos problemas. En primer lugar los gastos que supone para este tercero la introducción a su sistema de circuitos de enrrutamiento, el examen de los mensajes y la pérdida de espacio de almacenaje y ancho de banda. [101] Otro problema radica en el alto nivel de confianza que debe depositar el usuario en el proveedor de servicios de Internet u otras terceras partes que realicen la actividad.[102]

Los problemas relacionados con costos económicos de la tercera parte que filtra pueden ser enfrentados a través del bloqueo de spam. El bloqueo funciona básicamente a través de *listas negras*. Las listas negras son bases de datos que contienen sitios que, en general, resultan potencialmente proclives al spam. De

---

[97] Ver, por ejemplo, "FILTERING FREE EMAIL" (Rodney Much). Disponible en http://www.optinnews.com/news/showart.asp?DB=NewsTable&ID=1111. Visitado 25/03/2002

[98] Dos ejemplos propuestos por SORKIN son que el usuario reciba únicamente aquellos mensajes que en su encabezamiento digan "esto no es spam" o solo reciba mensajes en la medida que se le efectúe un micropago (ver *Technical and Legal Approaches to Unsolicited Electronic Mail.* Cit., nota 94).

[99] Sobre el problema de inexactitud de los filtros en general ver *Developments.* Cit. S/P.

[100] Ver *Technical and Legal Approaches to Unsolicited Electronic Mail.* Cit. p. 346

[101] Ibidem p. 347

[102] Existe alguna evidencia acerca de negligencia por parte de quienes administran sistemas de filtros en su mantención en términos que permitirían el acceso a sitios que deberían ser filtrados o lo denegarían a sitios benignos. Ver Lisa Gill: *Experts: Filtering Software a Failure.* NewsFactor Network. Disponible en http://www.newsfactor.com/perl/story/16980.html. Visitado 28/03/2002.

esta manera Realtime Blackhole List (RBL), actualmente el servicio de listas negra más popular en el mundo, identifica en su lista servidores que permiten el envío de correos electrónicos por terceras partes y otros sitios que son considerados "amistosos o, al menos, neutrales, a los spammers."[103] Cualquier correo enviado desde de los sitios identificados en la lista de RBL es bloqueado automáticamente por el operador de destino si este se encuentra suscrito.

Aún cuando este tipo de sistemas mejora algunas de las deficiencias de los filtros, tampoco resulta perfecto. Una vez más el sistema funciona dependiendo de un elenco de instrucciones que determinan los criterios que utilizará para discriminar. En un entorno dinámico como el de la Red y el de los spammers resulta extraordinariamente difícil fijar criterios que no permitan el ingreso de spam o bien que no bloqueen el ingreso de correo legítimo. Un problema adicional es la cantidad de poder que se radica en los creadores de las listas, finalmente son ellos quienes deciden qué correos ingresan y cuales no.[104] [105]

La regulación del mercado.- Junto a las tres modalidades exploradas, una cuarta posibilidad es utilizar el sistema de precios para regular el spam. Como se ha revisado, el envío de correos electrónicos masivos es atractivo como mecanismo de avisaje por dos razones. La primera de ellas tiene que ver con su efectividad, la segunda con sus costos. El spam entonces es un modo eficiente y barato de publicitar bienes y servicios. Utilizar el sistema de precios puede modificar la segunda característica del spam como medios de avisaje: su bajo costo.

---

[103] Ver mail abuse prevention system llc. http://www.mailabuse.org/rbl/candidacy.html. visitado 27/03/2002

[104] Un ejemplo de las consecuencias de lo anterior puede ser revisado en supra nota 86. Para un enfoque más amplio sobre los peligros del bloqueo en general –no solo de correos electrónicos- puede consultarse LESSIG, Larry: *What Things Regulate Speech: CDA vs. Filtering.* Disponible en cyber.law.harvard.edu/works/lessig/what_things.pdf . Visitado 27/03/2002.

[105] La actividad aún puede tener otros riesgos. Para verificar si un proveedor mantiene su sistema de transmisión abierto o no quien administra la lista debe "testear" dicho servidor. Existen algunas posibilidades que ese testeo lesione la capacidad de los equipos del proveedor de servicios. Un ejemplo de lo anterior es el caso de ORBZ. ORBZ (open relay black zone) era uno de los numerosos servicios de listas negras que incluían a aquellos proveedores de servicios de Internet que mantenían sus servidores abiertos. Una vez incluidos en la lista negra los correos enviados desde esos servidores a suscriptores de ORBZ eran automáticamente bloqueados. Para determinar si los proveedores de servicios de Internet mantenían o no sus servidores abiertos ORBZ utilizaba un test que inutilizaba las máquinas Lotus Domino (una plataforma colaborativa de aplicaciones de Red producida por Lotus, ver http://www.lotus.com/home.nsf/welcome/domino. Visitado 25/03/2002). Este daño expuso a Ian Gulliver administrador de ORBZ a riesgo de ir a la carcel, antes de verlo concretado prefirió cerrar su lista. Ver *Facing Legal Challenges, Blackhole List Closes.* Jim Wagner, Internetnews. Disponible en http://www.internetnews.com/dev-news/article/0,,10_995251,00.html. Visitado 25/03/2002.

El sistema de precios puede ser utilizado como mecanismo de regulación privada o bien para implementar una solución legal.[106] En lo que sigue me interesa referirme únicamente a esta segunda posibilidad.

Es posible pensar que los spammers aún obtendrían beneficios si utilizaran el sistema de precios para discriminar los receptores de sus mensajes. Una posibilidad sugerida anteriormente sería "sobornar" a los posibles destinatarios con micropagos o bien adscribiendo pequeñas ventajas económicas (suscripciones, descuentos, etc.[107]) a la recepción de correos comerciales. Lo anterior, según me parece, crearía un clima más favorable entre los posibles destinatarios y permitiría discriminarlos con mayor efectividad.

Aún cuando la solución de mercado suena razonablemente atractiva, la realidad se ha encargado de demostrar que sin que el derecho realice una asignación de titularidades inicial, que existan normas sociales susceptibles de ser exigidas o soluciones de código que faciliten la negociación de las titularidades, el mercado resulta incapaz de proteger a los usuarios del correo masivo. Esta constatación resulta suficiente para renunciar al mercado como solución.[108] Con todo, aún puede intentarse explicar por qué esta modalidad es incapaz de controlar el spam. Solo a nivel especulativo es posible pensar que el problema con la regulación de spam por el mercado se encuentran en la relación costo-tasa de retorno. Por una parte es posible que el envío de spam solo se justifique por el escaso costo de enviar millones de comunicaciones, si a ese costo se sumaran

---

[106] La ley puede prohibir el spam, en este caso la ley regula directamente el spam. Una segunda posibilidad es que el legislador asigne a las personas derechos protegidos por reglas de propiedad sobre sus correos electrónicos (utilizo la expresión *derechos protegidos por reglas de propiedad* en el sentido que le asignan CALABRESI & MELAMED. Para estos autores un derecho está protegido por una regla de propiedad "en la medida que quien desea quitarle el derecho a su titular debe comprárselo en una transacción voluntaria, en la que el valor del derecho es aceptado por quien lo enajena" [CALABRESI, Guido & MELAMED, Douglas: *Reglas de reglas de responsabilidad y de inalienabilidad: Una vista de la catedral.* Centro de Estudios Públicos. Estudios Públicos 63, invierno 1996. P. 351]. De esta manera, el spam solo será permitido en la medida que el dueño de una casilla acepte el envío de correos. En clave económica esto significa que el legislador establece las condiciones para que el problema del spam sea resuelto a través de la oferta y la demanda. En este segundo caso la regulación de la ley es indirecta pues utiliza un mecanismo de mercado para controlar la cantidad de correos electrónicos.

[107] Un ejemplo cercano es el "marketing viral". Durante el año 2001 Ebrick.com (un portal de ventas) ofrecía tratos especiales y descuentos a aquellos clientes que enviaran su publicidad a familiares y amigos (ver An Epidemic of "Viral Marketing" Business Week online. Agosto 30, 2000. Disponible en http://www.businessweek.com:/bwdaily/dnflash/aug2000/nf20000830_601htm. Visitado 21/02/2000. Otro ejemplo, esta vez directamente relacionado con correos electrónicos es Hits4pay.com. Un servicios que paga pequeñas sumas a sus suscriptores por leer correos electrónicos. Ver http://hits4pay.com. Visitado 08/04/2002

[108] Aún cuando en el papel parezca una teoría atractiva adolece al menos de impropiedad, es decir sus predicciones fallan. Como ha advertido ELSTER, en estos casos, lo mejor que se puede hacer con la teoría es reemplazarla (ver ELSTER, Jon: JUICIOS SALOMÓNICOS. Editorial Gedisa. Barcelona, 1995. P. 11).

otros como los involucrados en ofrecer descuentos u otros mecanismos promocionales semejantes, entonces la actividad perdería su atractivo económico. Junto a lo anterior, es posible que atendida la mala prensa del spam la tasa de retorno no aumentaría significativamente aún si se incluyeran mecanismos promocionales, por lo mismo la inversión en ellos carece de justificación. Ambas razones, sin embargo, deben aún ser dotadas de plausibilidad empírica.

¿Es posible regular el spam?.- El balance de las cuatro modalidades exploradas no parece especialmente auspicioso. Ninguna de las cuatro modalidades individualmente consideradas ha resultado capaz de resolver los problemas que produce el spam. En el caso europeo la solución ha pasado por una mezcla entre una cultura fuertemente comprometida con la privacidad y un conjunto de leyes que sanciona vigorosamente la práctica. En el caso estadounidense la situación es algo más compleja. Por una parte no existe una cultura de la privacidad similar a la europea que permita confiar en los esfuerzos autorregulatorios del sector empresarial.[109] Junto a lo anterior, no existe a la fecha una regulación federal que condene el spam[110]. Si bien es cierto que a nivel estatal existe una abigarrada legislación y algunos spammers han sido llevados a juicio exitosamente la situación queda suficientemente descrita por las palabras de SORKIN: "(L)as respuestas que se han intentado hasta la fecha no han hecho más que aumentar el nivel de incertidumbre que rodea al spam."[111] En ausencia de normas sociales, la mezcla podría ser entre soluciones legislativas, de código y mercado involucrando al gobierno, las asociaciones de marketing y los proveedores de servicios de Internet.[112]

5. El tratamiento del spam en las directivas de las comunidades europeas.

La protección de los datos personales en el caso de algunos miembros de la Unión Europea precede con holgura al spam. Un número considerable de sus miembros ha promulgado legislación protegiendo la violación al derecho a la privacidad de los sujetos resultante del tratamiento de información personal.[113] En

---

[109] Y si existe no se encuentra suficientemente institucionalizada. Como resulta bien sabido, en los Estados Unidos el tema de la protección de la privacidad ha sido dejado a cargo de los esfuerzos autorregulatorios del mercado. En el caso europeo, en cambio, la protección de la privacidad se encuentra fuertemente regulado (ver DE LA MAZA Iñigo: *Privacidad y comercio electrónico.* En prensa)

[110] Ni parece que vaya a existir en el corto plazo. Ver Cnet Newscom: Congress, critics wrinkle noses at spam bills. 21 Mayo 2001. Disponible en http://news.com.com/2100-1023-257941.html. Visitado el 27/03/2002

[111] *Technical and Legal Approaches to Unsolicited Electronic Mail.* Cit. p. 384.

[112] Ver Joyce Graff: *No easy solution for spam.* ZD Net News. Disponible en http://zdnet.com.com/2100-1107-868530.html. Visitado 27/03/2002.

[113] Utilizo la expresión tratamiento de información personal en el sentido que le asigna el artículo 2 b) de la Directiva 95/46 esto es como:

las líneas que siguen, sin embargo, no me interesa dar noticia de la legislación promulgada a nivel nacional, sino revisar brevemente las cuatro directivas que se relacionan más o menos directamente con el tema del spam, esto es: la Directiva 95/46 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos; la Directiva 97/7 relativa a la protección de los consumidores en materia de contratos a distancia; la Directiva 97/66 relativa al tratamiento de los datos personales y a la protección de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones y; finalmente, la Directiva 2000/31 relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).

La Directivas 95/46 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.- Como su nombre lo sugiere la Directiva 95/46 busca proteger el derecho a la privacidad de las personas sujetando el tratamiento de datos personales a una serie de requisitos que determinan su licitud. Así las cosas, luego de un conjunto de definiciones –entre las cuales se encuentran *datos personales*[114] y *tratamiento de datos personales*[115]- el artículo 6 establece una serie de principios destinados a regir la recolección de datos personales y su procesamiento.

De esta manera, la recolección de datos es lícita únicamente si se lleva a cabo con fines determinados, explícitos y legítimos. El tratamiento de dichos datos será legítimo si es realizado en consonancia con dichos fines (art. 6.1..b). La regla general es que el procesamiento de datos (esto incluye su recolección) solo es lícito si el titular de la información ha dado su consentimiento en forma inequívoca (art. 7. a). La Directiva se encarga de exigir que ese consentimiento sea suficientemente informado, sea que los datos se recaben del propio interesado (art. 10), o en el caso que se recaben de terceros (art. 11). En ambos casos el titular tiene derecho a saber: (1) la identidad del responsable del tratamiento y (2) los fines del tratamiento de que van a ser objeto los datos.

> cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción .

[114] definidos como:

> toda información sobre una persona física identificada o identificable (el interesado); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social.

[115] Ver supra nota 114

La dirección de correo electrónico constituye, según la normativa recién expuesta, un dato personal[116], en razón de lo anterior tanto para ser recolectada como para enviar mensajes hacia ella debe obtenerse la autorización de su titular. Consecuentemente, a la luz de la Directiva 95/46, las comunidades europeas adscribirían a un sistema de opt in.

La Directiva 97/7 relativa a la protección de los consumidores en materia de contratos a distancia.- El enfoque de la Directiva 97/7 difiere substantivamente del de la 95/46 en términos de hacerlas difícilmente conciliables. Esta diferencia entre ambas directivas introduce dudas en el tratamiento legal de los correos no solicitados en las comunidades europeas.

La Directiva 97/7 consagra en su artículo 10 restricciones a la utilización de determinadas técnicas de comunicación a distancia en los siguientes términos.

1. La utilización por un proveedor de las técnicas que se enumeran a continuación necesitará el consentimiento previo del consumidor:
   - sistema automatizado de llamada sin intervención humana (llamadas automáticas),
   - fax (telecopia).
2. Los Estados miembros velarán por que las técnicas de comunicación a distancia distintas de las mencionadas en el apartado 1, cuando permitan una comunicación individual, sólo puedan utilizarse a falta de oposición manifiesta del consumidor.

El envío de correos electrónicos quedaría así comprendido en el número dos y podría ser llevado adelante "a falta de oposición manifiesta del consumidor". En

---

[116] Esto, sin embargo, presenta algunos problemas que el caso español ilustra. Como resulta evidente, la dirección de correo electrónico puede o no coincidir con la definición de dato personal contenida en la Directiva 95/46. De esta manera, según han sostenido algunos, en aquellos casos en que la dirección permita identificar a la persona se trataría de un dato personal. En caso contrario –esto es si la dirección no posee una relación significativa con su dueño no se trataría de un dato personal No obstante lo anterior, la Agencia de Protección de Datos española ha razonado en forma distinta. Como advierte TÉLLEZ:

> el hecho que la dirección de correo electrónico no aparezca referenciada a un dominio concreto, de tal forma que pueda procederse a la identificación del titular mediante la consulta al servidor en que se gestione dicho dominio, sin que ello pueda considerarse que lleve aparejado un esfuerzo desproporcionado por parte de quien procede a la identificación, hace que la APD [Agencia de Protección de datos], en aras de asegurar la mxima garantía del derecho a la privacidad contenido en el artículo 18.2 de la CE [Constitución española] considere a estas direcciones de correo también datos amparados por el regimen protector de la LOPDP [Ley Orgánica de Protección de datos Personales]. (TÉLLEZ, Abel: NUEVAS TECNOLOGÍAS: INTIMIDAD Y PROTECCIÓN DE DATOS. Edisofer. Madrid 2001. P. 114-115)

este caso, la Directiva 97/7 parecería estar consagrando un sistema de opt out incompatible con el sistema de opt in de la 95/46.[117]

Directiva 97/66 relativa al tratamiento de los datos personales y a la protección de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.- La Directiva 97/66 aplica el principio del consentimiento previo consagrado en la Directiva 95/46 al sector de las telecomunicaciones. Así, su artículo 12, respecto de llamadas telefónicas exige que quienes reciban dichas llamadas las hayan aceptado previamente.[118]

El nivel de protección que garantiza la Directiva 97/66 genera problemas con el nivel de protección brindado por la 97/7. Si bien la 97/66 no se refiere a las comunicaciones electrónicas resulta poco adecuado que el envío de correos electrónicos no deseados se regule en forma diferente a la regulada en lo que refiere a las llamadas telefónicas no deseadas. Lo anterior, porque como señalan GAUTHRONET y DROUARD, las características de ambos medios de comunicación son extremadamente similares, los correos electrónicos pueden ser considerado el mecanismo de marketing más intrusivo, además no existe forma de evitarlo y, finalmente, se está transformando en el mecanismo más costoso para los receptores.[119]

Directiva 2000/31 relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).- Aún cuando no

---

[117] Ver GAUTHRONET, Serge, DROUARD, Etienne. Comunicaciones comerciales no solicitadas y protección de datos. Resumen de las conclusiones del estudio (). Enero de 2001 P. 13. Disponible en europa.eu.int/comm/internal_market/en/media/dataprot/studies/ spamsumes.pdf . Visitado 10/03/2002

[118] Artículo 12 Llamadas no solicitadas

1. La utilización de sistemas de llamada automática sin intervención humana (aparatos de llamada automática) o facsímil (fax) con fines de venta directa sólo se podrán autorizar respecto de aquellos abonados que hayan dado su consentimiento previo.

2. Los Estados miembros tomarán las medidas adecuadas para garantizar, gratuitamente, que no se permitan las llamadas no solicitadas con fines de venta directa por medios que no sean los mencionados en el apartado 1 sin el consentimiento de los abonados de que se trate o respecto de los abonados que no deseen recibir dichas llamadas. La elección entre estas posibilidades será la que determine la legislación nacional.

3. Los derechos conferidos en virtud de los apartados 1 y 2 se aplicarán a los abonados que sean personas físicas. Los Estados miembros garantizarán asimismo, en el marco del Derecho comunitario y de las legislaciones nacionales aplicables, la suficiente protección de los intereses legítimos de los abonados que no sean personas físicas en lo que se refiere a llamadas no solicitadas.

[119] GAUTHRONET, Serge, DROUARD, Etienne. Unsolicited Commercial Communications and Data Protection. Cit. p. 100

resulte claro todavía cuáles son exactamente los "servicios de la sociedad de la información,[120] la Directiva 2000/31 contiene algunas reglas sobre comunicaciones comerciales[121] en sus artículos 6 y 7 que, según examinaré, aunque no resultan especialmente satisfactorias, contribuyen en algo a despejar la incertidumbre sembrada por las diferencias existentes entre sus predecesoras respecto al tratamiento legal de los correos no solicitados.

La sección dos del capítulo II de la Directiva 2000/31 dedica sus tres artículos (6,7 y 8) a las comunicaciones comerciales. Para efectos de estas líneas solo los primeros dos resultan relevantes. El artículo 6 refiere a la información exigida en las comunicaciones comerciales.[122]

---

[120] Los servicios de la sociedad de la información se definen por referencia a la Directiva 98/48 CE. Según esta son los relativos a cualquier servicio prestado normalmente a título oneroso, a distancia, mediante un equipo electrónico para el tratamiento (incluida la comprensión digital) y almacenamiento de datos, y a petición individual de un receptor del servicio, quedando expresamente excluidos aquellos que no impliquen tratamiento y almacenamiento de datos. Ver MAESTRE, Javier: *LSSI: Análisis Legal.* S/P. Disponible en http://www.glub.ehu.es/lssi/02.html. Visitado 01/04/2002

[121] La Directiva 2000/31 define las comunicaciones comerciales en la letra f de su artículo 2 como:

> todas las formas de comunicación destinadas a proporcionar directa o indirectamente bienes, servicios o la imagen de una empresa, organización o persona con una actividad comercial, industrial, artesanal o de profesiones reguladas. No se consideran comunicaciones comerciales en sí mismas las siguientes:
> — los datos que permiten acceder directamente a la actividad de dicha empresa, organización o persona y,
> concretamente el nombre de dominio o la dirección de correo electrónico,
> — las comunicaciones relativas a los bienes, servicios o a la imagen de dicha empresa, organización o persona, elaboradas de forma independiente de ella, en particular cuando estos se realizan sin contrapartida económica.

[122] Art. 6 **Información exigida.**

> Además de otros requisitos en materia de información en el Derecho comunitario, los Estados garantizaran que las comunicaciones comerciales que forman parte o constituyen un servicio de la sociedad de la información cumplan al menos las condiciones siguientes:
> a) las comunicaciones comerciales serán claramente identificables como tales;
> b) será claramente identificable la persona física o jurídica a nombre de la cual se hagan dichas comunicaciones comerciales;
> c) las ofertas promocionales, como los descuentos, premios y regalos, cuando estén permitidos en el Estado miembro de establecimiento del prestador de servicios deberán ser claramente identificables como tales y serán fácilmente accesibles y presentadas de manera clara e inequívoca las condiciones que deban cumplirse para acceder a ellos.
> d) los concursos o juegos promocionales, cuando estén permitidos en el Estado miembro de establecimiento del prestador de servicios, serán claramente identificables como tales las condiciones de participación; serán fácilmente accesibles y se presentaran de manera clara e inequívoca.

El artículo 7 por su parte refiere a las comunicaciones comerciales no deseadas. En términos gruesos, este artículo exige el cumplimiento de dos requisitos para que el envío de comunicaciones comerciales no solicitadas sea realizado conforme a derecho. El primer requisito refiere a los mensajes y el segundo a los prestadores de servicios que realicen comunicaciones comerciales no solicitadas por comercio electrónico.[123] De esta manera los mensajes comerciales deben ser claramente identificables como tales y quienes envíen correos que contengan comunicaciones comerciales no deseadas y los prestadores de servicios que envíen correos comerciales no deseados deben consultar listas de exclusión que contengan a los usuarios que no deseen recibir correos comerciales.

El primer problema del artículo 7 es que no deja clara la periodicidad de la consulta regular. De esta manera no resulta evidente que el prestador de servicios que desee llevar adelante campañas de publicidad a través del envío de correos electrónicos deba consultarlas cada vez que va a implementar una campaña o solo "regularmente". Un segundo problema refiere a las listas de exclusión. Nada en la Directiva 2000/31 indica cómo se formarán estas listas o si serán varias o una sola. El número de listas resulta relevante pues de existir una pluralidad de ellas aumentan los costos de monitoreo para los prestadores que deseen enviar correos electrónicos comerciales no solicitados.

Como se ha advertido, las cuatro directivas configuran un escenario contradictorio, GAUTHRONET y DROUARD proponen examinar los tres escenarios en que puede presentarse el envío de spam para analizarlo. De acuerdo a estos autores debe distinguirse cuando (1) ha existido previo contacto entre quien envía y quien recibe la comunicación comercial; (2) la dirección de correo electrónico ha sido proveída por un tercero a quien envía la comunicación comercial y, (3) la dirección de correo electrónico ha sido recogida desde espacios públicos en Internet.[124]

(1) Contacto previo.- En este caso un cliente potencial ha suministrado su dirección de correo electrónico. Si quien envía los correos electrónicos comerciales ha cumplido con los requisitos fijados en el artículo 10 de la

[123] Art. 7 **Comunicación comercial no solicitada.**

> 1. Además de otros requisitos establecidos en el Derecho comunitario, los Estados miembros que permitan la comunicación comercial no solicitada por correo electrónico garantizarán que dicha comunicación comercial facilitada por un prestador de servicios establecido en su territorio sea identificable de manera clara e inequívoca como tal en el mismo momento de su recepción.
>
> 2. Sin perjuicio de los dispuesto en las Directivas 97/7/CE y 97/66/CE, los Estados miembros deberán adoptar medidas para garantizar que los prestadores de servicios que realicen comunicaciones comerciales no solicitadas por correo electrónico consulten regularmente las listas de exclusión voluntaria (*´opt-outª*) en las que se podrán inscribir las personas físicas que no deseen recibir dichas comunicaciones comerciales, y las respeten.

[124] Unsolicited Commercial Communications and Data Protection. cit. pp. 105-108

Directiva 95/46 –en particular los fines del tratamiento que van a ser objeto los datos- puede enviar dichos correos hasta que el receptor solicite su remoción, es decir se oponga a su envío (Art. 10 nº 2 Directiva 97/7). En adición a lo anterior, y considerando el nº 1 del artículo 7 de la Directiva 2000/31, los correos deben ser identificables de manera clara e inequívoca como comerciales.

(2) Dirección obtenida de terceros.- El cliente potencial esta vez ha suministrado su dirección de correo electrónico a una persona distinta a aquella que le envía los correos quien se la ha cedido a esta última. De acuerdo al artículo 14 b) de la Directiva 95/46 esta cesión es lícita siempre que sea informada al titular de los datos. En adición a lo anterior, el titular debe ser informado de su derecho a oponerse sin costo a la utilización comercial de sus datos. Como en el caso anterior, el titular tiene derecho a solicitar su remoción y el mensaje debe explicitar inequívocamente su carácter comercial.

(3) Dirección obtenida en espacios abiertos.- La recolección de direcciones de correo electrónico en espacios abiertos de Internet (grupos de noticias, mailing lists, etc.) se encuentra prohibida por la Directiva 95/46 pues se realiza al margen del consentimiento del usuario (arts. 6, 7, 10, 11 y 14).

6.- El tratamiento del spam en la legislación chilena.

El envío de comunicaciones comerciales no deseadas se encuentra explícitamente tratado en la Ley 19.628 sobre protección de la vida privada, de 28 de Agosto de 1999. Conviene, por lo mismo detenerse algunos momentos en ella para luego examinar si protege a los titulares de datos de la recolección de sus direcciones de correo electrónico y el posterior envío de comunicaciones no deseadas.

En un título provocativo, pero acertado según me parece, Renato JIJENA se ha referido a la "no protección de la intimidad en Chile."[125] En palabras de este autor la Ley 19.628 constituiría:

> una normativa que apuntó a proteger y legalizar el negocio del procesamiento de datos personales desde la perspectiva de las empresas del ramo, más que a resguardar los derechos de los titulares a quienes aluden o a quienes refieren los datos personales o nominativos.[126]

Para justificar la intensidad de la afirmación anterior es necesario dar una mirada a las ideas matrices de la Ley 19.628.

---

[125] JIJENA, Renato: *Sobre la no protección de la intimidad en Chile. Análisis de la Ley 19.628, de Agosto de 1999*." S/P. Disponible en http://www.alfa-redi.org/upload/revista/101301--19-19-Redi1101.doc. Visitado 02/04/2002

[126] Ibidem.

Las ideas matrices de la Ley 19.628.- En primer lugar la Ley establece dos tipos de datos relevantes, los de carácter personal (o datos personales) y los datos sensibles.[127] Los datos personales refieren únicamente a las personas naturales y por la amplitud de su definición corresponden a cualquier información sobre una persona que pueda ser identificada. La Ley 19.628 no provee de criterios para determinar cuándo es identificable una persona. En este sentido, siguiendo a Herrera[128], puede recurrirse al artículo 2 a) de la Directiva 95/46 y señalarse que se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social. Respecto a los datos sensibles, a diferencia de otras normativas sobre privacidad, la Ley 19.628 establece, a diferencia de la Directiva 95/46 que contiene un catálogo cerrado, una categoría de datos y luego ejemplos que la ilustran.[129]

En segundo lugar, la Ley 19.628 consagra como principio general la obtención del consentimiento del titular de los datos[130] para su tratamiento.[131] De esta manera el artículo 4º prescribe en su inciso primero que: "el tratamiento de los datos personales con fines de publicidad, investigación o mercado sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello." Como en otros casos, sin embargo, la amplitud de las

---

[127] Art. 2 f) Datos de carácter personal o datos personales, los relativos s cualquier información concerniente a personas, identificadas o identificables.

Art. 2 g) Datos sensibles, aquellos datos personales que se refieren a las características físicas o morales de las personas a hechos o circunstancias de su vida privada o intimidad tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

[128] HERRERA, Rodolfo: *Análisis de la ley chilena Nº 19.628 sobre protección de la vida privada, de 28 de agosto de 1999.* P. 13. Disponible en http://www.alfa-redi.org/areatematica/articulo.asp?idCategoria=38. Visitado 02/04/2002

[129] A diferencia de HERRERA, mi opinión es que referirse a una categoría de datos e ilustrarla a través de ejemplos es una técnica legislativa superior a los catálogos cerrados. Lo anterior por dos razones, la primera es porque los casos más paradigmarios de datos sensibles corresponden a los ejemplos. Sobre estos el nivel de discreción del juez al aplicar la norma es bajo. La segunda razón es porque me parece que respecto de los demás –que no quedarían consagrado en un escenario de catálogo cerrado tampoco- la principal carga no es para los titulares de dichos datos sino para quienes intentan tratarlos, son ellos los que deben lidiar con la incertidumbre de un resultado adverso en un proceso judicial. Por lo mismo, me parece evidente que si a alguien perjudica este tipo de norma es a quienes tratan datos y no a los titulares de estos (cfr. Ibidem pp. 13-16).

[130] Art. 2 ñ) Titular de los datos, la persona natural al que se refieren los datos de carácter personal

[131] Art. 2 o) Tratamiento de datos, cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma.

excepciones que atendió el legislador transforman a la regla general –la obtención del consentimiento del titular- en la excepción al momento de tratar datos personales.[132]

Las excepciones a la obligación de obtener el consentimiento del usuario se encuentran consagradas a partir del inciso 2º del artículo 4, algo más abajo de la regla general.[133] La primera excepción queda constituida por la obtención de datos personales en fuentes accesibles al público.[134] La accesibilidad al público de las fuentes quedará determinada según si estas se encuentran o no restringidas a los solicitantes ¿cuáles son entonces las fuentes accesibles al público? La interpretación más razonable parece ser que son aquellas en que por ley el acceso no se encuentra restringido por ley.[135] Si esta es la interpretación es correcta, entonces la regla general es que todas las fuentes, salvo las exceptuadas explícitamente por ley, son accesibles al público y, por lo tanto puede llevarse el tratamiento de los datos personales contenidos en ellas sin autorización de sus titulares.

En tercer lugar la Ley 19.628 consagra un derecho a conocer la información propia. Dicho en otras palabras, la Ley consagra el Habeas Data. Esta garantía se encuentra recogida en los artículos 12, 13, 14 y 15 de la Ley bajo el título "De los derechos de los titulares de datos."

---

[132] Lo anterior no es igualmente exacto respecto del tratamiento de datos personales por parte de organismos públicos (Título IV de la Ley). No obstante lo anterior, considerando que el spam no es un problema que se haya presentado en las relaciones del sector público con los privados, dejo ese tema de lado.

[133] Art. 4 incisos 4º y 5º

> No requiere autorización el tratamiento de datos personales que provengan o que se recolecten de fuentes accesibles al público, cuando sean de carácter económico, financiero, bancario o comercial, se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento, o sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios.
> Tampoco requerirá de esta autorización el tratamiento de datos personales que realicen personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquéllos.

[134] La ley define en su artículo 2º letra i) como: los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes.

[135] En este sentido ver : *Análisis de la ley chilena Nº 19.628 sobre protección de la vida privada, de 28 de agosto de 1999.* Cit. p. 17 y *Sobre la no protección de la intimidad en Chile. Análisis de la Ley 19.628, de Agosto de 1999.* Cit. S/P. Ejemplos de estos datos de acceso restringido serían el secreto estadístico, el secreto tributario, el secreto bancario, el secreto de filiación política (los ejemplos están en Ibidem.)

En pocas palabras, haciendo pie en esta garantía, toda persona tiene derecho a exigir a quien sea responsable de un banco[136] que se dedique al tratamiento de datos **información** sobre los datos relativos a su persona, su procedencia y destinatario, el propósito de almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente. Junto a lo anterior, puede exigir que los datos se **modifiquen** cuando sean erróneos, inexactos, equívocos o incompletos, siempre que así se acredite. Podrá solicitarse además que dichos datos sean **eliminados** si su almacenamiento careciere de fundamento legal o dichos datos se encontraran caducos[137]. Igualmente podrá solicitar la eliminación cuando se hubieren entregado voluntariamente y se utilizaran para comunicaciones comerciales. La información, modificación o eliminación deberá ser absolutamente gratuita.[138] Finalmente, si los datos personales cancelados o modificados hubieren sido comunicados previamente a personas determinadas o determinables, el responsable del banco de datos deberá avisarles a la brevedad posible la operación efectuada. Si esto no fuera posible entonces la Ley impone la obligación al responsable del banco de datos de poner un aviso de general conocimiento que dé noticia sobre dicha modificación o eliminación.

No se trata en estas páginas de analizar exhaustivamente el estatuto de protección de los datos personales consagrados en la Ley 19.628 sino nada más de dar noticia sobre sus ideas matrices y la forma en que se encuentran plasmadas para luego revisar la situación del spam, eso es lo que hago a continuación.

La situación legal del spam en Chile.- Según se ha advertido anteriormente, el problema del spam tiene que ver con dos cosas, la primera es la recolección de datos y, la segunda, con el envío masivo de correos. Se trata de examinar entonces ambas situaciones bajo el prisma de la Ley 19.628.

---

[136] La Ley define en su artículo 2 letra m) registro o banco de datos como el conjunto organizado de datos de carácter personal sea automatizado o no y cualquiera sea la forma o modalidad de su creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos.

En el mismo artículo, pero esta vez en la letra n) define responsable del registro o banco de datos como la persona natural o jurídica privada, o el respectivo organismo público, a quien compete las decisiones relacionadas con el tratamiento de datos de carácter personal.

[137] Dato caduco se encuentra definido en el artículo 2 letra d) como el que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o si no hubiese norma expresa, por el cambio de los hechos o circunstancias que consigna.

[138] Conviene advertir, sin embargo, que, al menos en el caso de la modificación, los costos de acreditar que los datos personales son erróneos, inexactos equívocos o incompletos recaen sobre el titular de dichos datos. Así se desprende de la lectura del inciso 2º del artículo 12.

Aún cuando la expresión tratamiento de datos personales comprende, según la letra o) del artículo 2º de la Ley 19.628 la recolección de datos personales y, por lo tanto, esta es regulada a partir del artículo 4º, el artículo 3º establece ciertas limitaciones a ella. La limitación, sin embargo, solo se aplicaría a aquella recolección de datos que se realice a través de encuestas, estudios de mercado o sondeos de opinión pública u otros instrumentos semejantes. La limitación en cuestión exige que se informe a los titulares de dichos datos acerca del carácter obligatorio o facultativo de sus respuestas y el propósito para el cual se está solicitando la información. Además le asigna al titular la posibilidad de oponerse a la utilización de sus datos personales con fines de publicidad, investigación de mercado o encuestas de opinión.

La actividad que parece estar reglando esta norma no es la recolección de direcciones de correos electrónicos con el fin de enviar publicidad, sino más bien la recolección de información sobre algún tipo de hábitos del sujeto para luego hacer públicos los resultados sin que sea posible identificar a las personas consultadas. No obstante lo anterior, aún cuando el fin inmediato de esta recolección no sea el marketing a través de correos electrónicos es perfectamente posible que estos se utilicen más adelante por quien los recolecta o bien por otra persona a quien sean transferidos, para campañas de spam. La protección de la Ley consiste en que el sujeto debe ser informado del carácter facultativo u obligatorio de sus respuestas y el propósito para el cual se está recolectando su información. En segundo lugar, el titular de los datos puede oponerse a su utilización con fines de publicidad. Cabe advertir que no se exige el consentimiento explícito del sujeto, sino nada más informar acerca del carácter de la respuesta. En segundo lugar no se exige que la persona autorice que sus datos sean utilizados con fines de publicidad, sino que se le da el derecho a oponerse.[139]

Ahora bien, no es el artículo tercero la principal causa de preocupación. Como ya se ha advertido, en lo hechos, el artículo 4º autoriza el tratamiento de datos personales –incluida su recolección- sin necesidad que el titular lo autorice, siempre y cuando estos:

1. provengan de fuentes de acceso público
2. cuando sean de carácter económico, financiero, bancario o comercial
3. se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento
4. sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes y servicios

[139] En la práctica ambos mecanismos dejan un amplio espacio de maniobra a quien solicita la información para recolectar direcciones de correo electrónico y luego utilizarlas para enviar comunicaciones comerciales no deseadas.

5. sean tratados por personas jurídicas privadas para el uso de exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquellos.

Una respuesta respecto a la situación legal del spam en Chile puede intentarse sintetizando el artículo 4º de la siguiente manera:

No requiere autorización el tratamiento de datos personales cuando estos sean necesarios para las comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes y servicios.

Pues bien, se ha advertido ya que en Chile no existen limitaciones legales para recolectar direcciones de correo electrónico ¿qué sucede con el envío? La respuesta más sintética consiste en afirmar que el envío también queda cubierto por la expresión "tratamiento de datos" y por lo tanto no requiere autorización previa.

¿Puede oponerse el titular al envío de correos comerciales no deseados? Para responder a esta pregunta, en el caso chileno, debe distinguirse si el titular ha proporcionado voluntariamente sus datos o no.

1) Si ha proporcionado sus datos en forma voluntaria. En este caso, según lo preceptuado en el artículo 12 inciso 4º de la Ley, el titular puede exigir su eliminación o bloqueo. Cabe advertir, sin embargo, que la Ley reconoce este derecho al titular bajo la siguiente fórmula:

> Igual exigencia de eliminación, o la de bloqueo de los datos, en su caso, podrá hacer cuando haya proporcionado voluntariamente sus datos personales o ellos se usen para comunicaciones comerciales y no desee continuar figurando en el registro respectivo, sea de modo definitivo o temporal.

Como ya se ha advertido, el derecho que reconoce la ley al titular de exigir la eliminación o modificación de sus datos personales se encuentra condicionado a que estos sean erróneos, inexactos, equívocos o incompletos en el caso de la modificación y que el almacenamiento carezca de fundamento legal o los datos estén caducos en el caso de la eliminación. A estas hipótesis entonces se reduce el derecho del titular cuando ha entregado voluntariamente sus datos.

2) Si el titular no ha entregado voluntariamente sus datos a quien los utiliza para enviar comunicaciones comerciales, deben distinguirse dos situaciones (i) los datos han sido entregados a quien envía comunicaciones por un tercero y (ii) los datos han sido obtenidos en espacios abiertos en la Red.

(i) Si el titular entregó sus datos voluntariamente a quien a su turno los transfirió al emisor de las comunicaciones comerciales, respecto del primero se aplican las reglas del caso anterior. La Ley establece la obligación para quien entregó los datos de comunicar que los datos se encuentran modificados o eliminados al

emisor de las comunicaciones comerciales y este según la regla general quedará vinculado por los incisos segundo y tercero del artículo 12.

(ii) Si los datos han sido obtenidos de espacios abiertos no resulta claro si el titular de dichos datos tiene derecho a exigir que se le elimine del envío de correos aún cuando se cumplan los requisitos de los incisos segundo y tercero del artículo 12 . Lo anterior porque la Ley solo se pone en este escenario cuando los datos han sido proporcionados voluntariamente. Por supuesto es posible afirmar que, *a fortiori*, la misma regla debería aplicarse en el caso en que los datos sean tratados sin la voluntad del titular, sin embargo, a primera vista pareciese que la Ley únicamente brinda esa protección en el caso de las comunicaciones comerciales cuando los datos hayan sido entregados voluntariamente.

En resumen, una interpretación pro titular de los datos llevaría a sostener que, con prescindencia de cómo se hayan obtenido los datos, la regla es aquella contenida en los incisos segundo y tercero del artículo 12. Lo anterior, sin embargo, no es una garantía demasiado intensa. Sólo podré evitar que se me envíen comunicaciones comerciales electrónicos no solicitadas cuando el almacenamiento de mi dirección de correo electrónico carezca de fundamento legal y la Ley, según se ha advertido, es pródiga al momento de proveer fundamentos.

Dónde nos deja todo esto.- La Ley 19.628 no es la única herramienta que puede utilizarse en el caso chileno contra el envío de comunicaciones comerciales no solicitadas. Es posible pensar en el mercado (por ejemplo a través de cláusulas anti spam en los contratos con los proveedores de servicios de Internet), el código (aunque, hasta donde llegan mis noticias no existen servicios chilenos de filtro o bloqueo[140]), las normas sociales (aunque únicamente en espacios reducidos donde estas puedan internalizarse y sancionarse). Sin perjuicio de lo anterior, la experiencia de otros países demuestra que estos mecanismos no son suficientes si no se encuentran apoyados por una legislación vigorosa. Esto nos deja entonces frente a dos alternativas. La primera es simplemente modificar la Ley 19.628 e introducir algún mecanismos que proteja efectivamente a los usuarios de la recolección de sus direcciones de correos electrónicos y el posterior envío de spam. La segunda es explorar el ordenamiento jurídico en busca de argumentos en contra del spam. No es ese el cometido de estas páginas, sin embargo, puede sugerirse la protección del derecho de propiedad, el enriquecimiento sin causa y el derecho a la privacidad. Todo esto, sin embargo, necesita ser reflexionado con bastante más cuidado.

* * * *

[140] No obstante ello, no existe ningún problema para un proveedor de servicios de Internet chileno en contratar los servicios de uno de estos servicios extranjeros.

Post scriptum: la necesidad de reflexionar sobre el tema en Chile. Es posible pensar que este es un tema que aún no ha llegado a Chile y por lo tanto su discusión puede ser postergada. El argumento, sin embargo, es deficiente en un triple sentido. Primero, no es tan daro que no haya llegado.[141] Segundo, de que no haya llegado no se deriva necesariamente que no vaya a llegar, como de que de una presa aún no se hay roto no se deriva que no pueda fracturarse y que debiéramos estar preparados frente a ese evento. Con todo, si estos dos argumentos no son convincentes el tercero si lo es. Actualmente se está negociando un tratado de libre comercio con la Unión Europea, uno de los requisitos de este tratado es la protección de ciertos estándares de protección a los datos personales, como se ha intentado advertir, la Ley chilena, al menos en lo que refiere al spam no está en condiciones de garantizar a los titulares de datos prácticamente ninguna protección.

[141] Según un informe publicitado por ACUI en junio de 200, el 70 % de los sitios web que operan en Chile no cuentan con políticas de privacidad. El 100 % de los sitios analizados recogen datos y los utilizan para hacer marketing a través de Internet. Ver http://www.acuicertifica.org/noticias/noti3.shtml. Visistado 04/04/2002