REGULACIÓN DEL CORREO ELECTRÓNICO COMERCIAL NO SOLICITADO (SPAM) EN INTERNET

Julio Núñez Ponce

1. INTRODUCCIÓN

"La red está cambiando con el fin de posibilitar el desarrollo completo del comercio electrónico, este cambio puede generar una mayor regulación del ciberespacio...".[1] Dentro de esta normatividad, surge la necesidad de regular el correo electrónico comercial no solicitado, conocido como *spam*. En pocos años, el *spam* se ha convertido en un fenómeno especialmente preocupante. Se considera que actualmente más del 50 por ciento del tráfico de correo electrónico en el mundo está constituido por *spam*. Aún más inquietante resulta el índice de crecimiento de este fenómeno, puesto que en en el 2001 la proporción se situaba en aproximadamente 7 por ciento.[2]

Se denomina *spam* a todo tipo de comunicación no solicitada, realizada por vía electrónica, que generalmente tiene el fin de ofertar, comercializar o tratar de despertar el interés respecto a un producto, servicio o empresa. Generalmente, se utiliza el

1 LESSIG, Lawrence. *El Código y otras leyes del ciberespacio*. Madrid: Taurus, 2001, p. 89.

2 Parlamento Europeo. *Documento sobre el spam en la Unión Europea* [en línea].<http://www.europarl.es>. [Consulta: 15 de setiembre del 2005].

correo electrónico (aunque puede realizarse por otros medios) y puede efectuarse de forma masiva.

El *spam* constituye un problema desde muy diversos puntos de vista:

- Intimidad.
- Naturaleza engañosa y fraudulenta del *spam*.
- Carácter perturbador de los *spam* pornográficos.
- Pérdida de tiempo (vaciado de los buzones de correo electrónico) y coste financiero al usuario (adquisición de programas de filtrado).
- Costes considerables para las empresas debido a que sus servicios informáticos deben dedicar cada vez más tiempo y dinero a intentar solucionar el problema. El tiempo dedicado a vaciar los buzones supone también una pérdida de eficacia y productividad en el trabajo. Este fenómeno ocasiona, además, costes indirectos por la no recepción de determinados mensajes por obra de las técnicas de filtrado de *spam* actuales.

En nuestros países estamos avanzando hacia la sociedad de la información, donde se puede observar que:

> ... la actual generalización del uso de las nuevas tecnologías, y especialmente de Internet, ha abierto un nuevo e importante campo de actuación a las comunicaciones dado que este nuevo medio permite a los usuarios obtener información de todas las materias de interés general o comunicarse con personas de cualquier país del mundo, así como potencia el incremento de las transacciones mercantiles dado que a través del nuevo medio o canal de distribución –en el lenguaje empresarial– las empresas ofrecen sus productos y servicios a un gran número de potenciales clientes, en lo que constituye el comercio electrónico.[3]

Por lo cual el uso de correos electrónicos en forma indiscriminada debe ser regulado.

En el ámbito técnico se utilizan dispositivos de filtro para luchar contra el *spam*. No obstante, todas las prácticas de filtrado no ofrecen el mismo grado de control al usuario ni las mismas garantías de protección de los datos y de la intimidad.

Por otra parte, esas técnicas pueden plantear problemas de eficacia, en particular si los sistemas de filtrado bloquean el correo electrónico legítimo (los "falsos positivos") o dejan pasar el *spam* ("falsos negativos"). Esto implica la necesidad de que además de las medidas tecnológicas se incluyan medidas jurídicas, propendiendo a que haya un equilibrio entre seguridad informática y seguridad jurídica.

El objetivo del presente artículo es el de examinar el correo electrónico comercial no solicitado (*spam*) desde el punto de vista del derecho informático, tratando su marco legislativo e interrelacionando con temas jurídico-informáticos relevantes, en el contexto de los negocios electrónicos.

2. REGULACIÓN DEL ACCESO Y USO DE INTERNET Y DE LOS CORREOS ELECTRÓNICOS

El acceso y uso de Internet, debido a que los gobiernos están procurando dar los pa-

3 BERROCAL LANZAROT, Ana Isabel. "El comercio electrónico y la responsabilidad de los prestadores de la sociedad de la información". *Memorias del X Congreso Iberoamericano de Derecho e Informática*. Santiago: Universidad de Chile, 2004, p. 179.

sos necesarios para llegar a la sociedad de la información, es un tema central que implica una serie de medidas conducentes a disminuir la brecha digital y a regularla de tal forma que se logre paulatinamente un acceso universal a la red.

Ahora bien, la regulación puede implicar distintos criterios, como el de fortalecer las regulaciones nacionales, armonizar las legislaciones de los distintos países, dar lineamientos para establecer convenios internacionales sobre la materia y concordar la legislación con los códigos de conducta y medidas contractuales.

Para plantearse el tema de la regulación hay que tener en cuenta que:

> ... con toda esta disponibilidad de contenidos el control de acceso pasa a ser una cuestión debatible, sobre todo en lo que concierne a los niños. Internet se dirige a una audiencia mundial, pero las definiciones de lo que son contenidos objetables varían de un país a otro. Al mismo tiempo, es difícil localizar a los autores de contenidos ilegales. El medio no es propicio para la censura.[4]

No obstante lo señalado, es necesario regular, por lo que surgen distintas normas en el ámbito jurídico informático, normas que pueden ser perfectibles pero que son una alternativa válida frente a la inacción. El derecho no puede ser ajeno a los problemas que origina la realidad tecnológica.

Los mensajes de datos incluidos en los correos electrónicos pueden utilizarse en forma individual o colectiva, ser correos electrónicos privados o institucionales, vincular a una persona natural o a una jurídica. Al respecto, hay que tener en cuenta que:

> ... el correo electrónico institucional es una herramienta de comunicación e intercambio de información oficial entre las personas, no es una herramienta de difusión indiscriminada de información, con excepción de las listas de interés establecidas por las instituciones para fines institucionales. Tener una cuenta de correo institucional compromete y obliga a cada usuario a aceptar las normas establecidas por la institución y a someterse a ellas. Los usuarios de las cuentas de correo electrónico son responsables de todas las actividades que realizan con sus cuentas de correo electrónico proporcionadas por la institución que laboran. Cualquier usuario que deje su cuenta de correo abierta en lugar público es responsable de todo lo que se realice desde dicha cuenta.[5]

Por lo que si se envía o se recibe *spam* desde o hacia un correo electrónico institucional, origina implicancias jurídicas que es necesario analizar.

La infraestructura tecnológica cambia. Además de las conexiones alámbricas, surgen las conexiones inalámbricas, que aplicadas a Internet originan nuevas implicancias al problema del *spam*, porque pueden ser recibidas desde distintos receptores inalámbricos, llámense computadoras portátiles, celulares digitales u otros.

> El Internet inalámbrico es la opción de acceder a Internet sin la necesidad de una conexión a través de cables. La señal necesaria para acceder a Internet se emite y se recibe a través de una banda de frecuencia, según sea la plataforma para emitir la señal.[6]

4 GATES, Bill. *Los negocios en la era digital*. Barcelona: Plaza & Janés, 2000, p. 180.

5 Normas para el Uso del Servicio de Correo Electrónico en las Entidades de la Administración Pública. Directiva 005-2003-INEI/DTNP, aprobada por Resolución Jefatural 088-2003-INEI. *El Peruano*. Lima, 3 de abril del 2003. Separata Normas Legales, pp. 242090-242091.

6 ARANGO RUEDA, Ariana. "Expectativas, desarrollo y evolución del Internet inalámbrico". *Derecho de Internet & Telecomunicaciones*. Bogotá: Legis S.A./Universidad de los Andes, 2003, p. 934.

Esto implica un mayor uso de Internet y origina un acrecentamiento de la vulnerabilidad con respecto al *spam*.

Entre las formas de *spam* que pueden ser recibidas por distintos medios tecnológicos podemos mencionar las siguientes:

- Correo electrónico.- Debido a su facilidad, rapidez y capacidad en transmisión y recepción de datos.
- *Spam* por ventanas emergentes (*pop ups*).- Se trata de enviar un mensaje no solicitado que emerge cuando nos conectamos a Internet. Aparece en forma de una ventana de diálogo y advertencia del sistema Windows, titulado: "servicio de visualización de mensaje".
- *Hoax*.- Se trata de un correo electrónico con contenido falso o engañoso y normalmente distribuido en cadenas.
- *Spam* en celular.- Además de las comunicaciones del operador de telefonía mediante mensajes de texto (SMS-Short Message Services) o mensajes multimedia (MMS-Multimedia Message Services), existen otros tipos de comunicaciones publicitarias en las que no media un consentimiento previo ni una relación contractual, por lo que son consideradas comunicaciones comerciales no solicitadas.

En lo que respecta a la realidad peruana, hay que añadir el caso de las cabinas públicas de acceso a Internet. En la legislación nacional se ha regulado que estas deben tener filtros que impidan el acceso a las páginas pornográficas a los menores de edad.

Igualmente, se ha establecido que provean facilidades y *software* adecuado para los discapacitados, pero aún falta dictar normas promocionales que fortalezcan este sector económico, formado predominantemente por pequeñas y medianas empresas.

Es necesario tener en cuenta que gracias a las cabinas de Internet los cibernautas locales son reconocidos como un grupo muy activo, tanto para descargar programas como en la participación en campañas, elegir en línea a un grupo de rock, una deportista triunfadora o una candidata a Miss Mundo; asimismo, ha permitido que en el Perú se reduzca la brecha digital y se democratice el acceso de distintos estratos sociales a Internet. Es desde las cabinas públicas que se pueden enviar y recibir los *spam*, por lo que una regulación debe considerar el caso de estos espacios de acceso a Internet.

El tema de los delitos informáticos debe también ser considerado y concordado. En el Perú se han tipificado los delitos de violación a la intimidad, hurto agravado por transferencia electrónica de fondos, intrusismo informático, sabotaje informático, pornografía infantil y turismo sexual por Internet. No obstante, hay otras figuras delictivas que pueden configurarse asimismo con los correos electrónicos no solicitados, como son la difamación y los chantajes vía Internet.

Los expertos en seguridad comenzaron a detectar intentos de chantaje en línea hace tres o cuatro años. Las autoridades señalan que el número de casos de chantaje en línea va en aumento, pero es difícil dar cifras porque los autores a menudo son procesados en virtud de leyes que cubren otras infracciones, como el lavado de dinero o los delitos relacionados con la piratería.

La vulneración de los *spam* en materia delictiva debe ser regulada por la legislación penal, por tanto, la normativa comercial y civil del *spam* tendrá un tratamiento paralelo, que deberá ser concordado cuando sea necesario.

3. LA REGULACIÓN DE LOS CORREOS ELECTRÓNICOS COMERCIALES NO SOLICITADOS (*SPAM*)

En este orden de ideas consideramos que:

> ... el *spam* constituye un problema desde muy diversos ángulos: intimidad, fraude a los consumidores, protección de los menores (muchas veces el contenido de estos mensajes son ilegales u ofensivos como pornográficos) y de la dignidad humana, costes para las empresas, pérdida de productividad, entre otros. En general, este fenómeno socava la confianza de los consumidores, algo indispensable para el éxito del comercio electrónico, de los servicios en línea e, incluso, de la sociedad de la información en nuestro país.[7]

Por lo que su regulación es necesaria.

Las fórmulas utilizadas en la regulación internacional sobre este tema son los modelos inclusivos (*opt-out*) y excluyentes (*opt-in*). El modelo *opt-in* supone que el *spam* está prohibido *per se* y es por ello que se requiere del consentimiento previo del destinatario del mensaje para poder enviar un mensaje publicitario. Australia y la Unión Europea han optado por incluir en sus legislaciones la fórmula *opt-in*. Por el contrario, el modelo *opt-out* supone que los mensajes pueden ser enviados a cualquier persona, con excepción de aquellas que han manifestado expresamente su voluntad de no recibir dichos mensajes. Estados Unidos, Corea del Sur y Colombia han empleado este sistema.[8] El legislador peruano ha optado por aplicar la fórmula *opt-out* cuando promulgó la Ley 28493.

En este sentido, la ley peruana 28493 regula el uso del correo electrónico comercial publicitario o promocional no solicitado (*spam*), sin perjuicio de la aplicación de las disposiciones vigentes en materia comercial sobre publicidad y protección al consumidor, por un lado, y los del ámbito penal, por otro, en lo que fuera aplicable. Reconoce como derechos de los usuarios de correo electrónico los siguientes:

- Rechazar o no la recepción de correos electrónicos comerciales.
- Revocar la autorización de recepción, salvo cuando dicha autorización sea una condición esencial para la provisión de servicio de correo electrónico.
- Que su proveedor de correo electrónico cuente con sistemas o programas que filtren los correos electrónicos no solicitados.

La ley peruana anti-*spam* en comentario, establece que todo correo electrónico comercial, promocional, originado en el país, para no ser considerado ilegal, debe contener:

- La palabra "Publicidad" en el campo del "asunto" (o *subject*) del mensaje.
- Nombre o denominación social, domicilio completo y dirección de correo electrónico de la persona natural o jurídica que emite el mensaje.
- La inclusión de una dirección de correo electrónico válido y activo de respuesta para que el receptor pueda enviar un mensaje para notificar su voluntad de no recibir más correos no solicitados o la inclusión de otros mecanismos basados en Internet que permitan al recep-

7 Exposición de Motivos del Proyecto de Reglamento de la Ley 28493, que regula el *spam*. *El Peruano*, separata especial. Lima, 9 de setiembre del 2005, p. 4.

8 Documento de trabajo: "Análisis comparativo de la legislación sobre *spam*". Unión Internacional del Telecomunicaciones (UIT). Junio del 2005.

tor manifestar su voluntad de no recibir mensajes adicionales.

Asimismo, el correo electrónico comercial no solicitado será considerado ilegal en los siguientes casos:

- Cuando contenga nombre falso o información falsa que se oriente a no identificar a la persona natural o jurídica que transmite el mensaje.
- Cuando contenga información falsa o engañosa en el campo del asunto (o *subject*), que no coincida con el contenido del mensaje.
- Cuando se envíe o transmita a un receptor que haya formulado el pedido para que no envíe dicha publicidad luego del plazo de dos días.

La definición de correo electrónico comercial debe entenderse como referida a toda comunicación publicitaria o promocional de bienes y servicios en general, incluyendo la información sobre eventos, certámenes y actividades, comercializados, ofrecidos, patrocinados u organizados por personas naturales o jurídicas. Será considerado como "no solicitado" cuando ha sido dirigido o enviado por el remitente sin que medie el pedido o consentimiento expreso del receptor.[9]

Conforme al artículo 7 de la Ley 28493, se consideran responsables de las infracciones establecidas y deberán compensar al receptor de la comunicación:

- Toda persona que envíe correos electrónicos no solicitados con publicidad comercial.
- Las empresas o personas beneficiadas de manera directa con la publicidad difundida.
- Los intermediarios de correos electrónicos no solicitados, tales como los proveedores de servicios de correos electrónicos.

Se ha propuesto que se incluya en las normas reglamentarias la precisión de que la definición de proveedor de servicio de correo electrónico no abarca a los proveedores del medio de transmisión, ya sea como operadores de servicios públicos de telecomunicaciones o como proveedores del servicio de conmutación de datos por paquetes que permiten el acceso al servicio de Internet.[10] Con esta propuesta se pretende limitar la aplicación de la responsabilidad a este tipo de proveedores y el consiguiente pago de la compensación pecuniaria establecida.

En efecto, el artículo 8 de la Ley 28493 establece que "el receptor del correo electrónico podrá accionar por la vía del proceso sumarísimo contra toda persona que lo haya enviado, a fin de obtener una compensación pecuniaria". Al limitarse el concepto de proveedor de servicio de correo electrónico, se pretende limitar a las personas contra las que se puede accionar. La compensación pecuniaria establecida en la ley es equivalente al uno por ciento de la Unidad Impositiva Tributaria ((UIT) por cada uno de los mensajes de correo electrónico transmitidos en contravención de la presente ley, con un máximo de dos UIT.

Algunos temas relevantes han sido incluidos para ser regulados en la normatividad reglamentaria conexa al *spam*, que incluyen la prohibición expresa de acciones relacionadas con el uso de Internet y del envío y recepción de correos electrónicos, como son los siguientes casos:

9 Proyecto de Reglamento de la Ley 28493 que regula el *spam*. *El Peruano*, separata especial. Lima, 9 de setiembre del 2005, p. 2.

10 Ibídem.

- El uso de medios que permitan facilitar la recolección de direcciones electrónicas sin autorización previa de sus dueños, tales como la comercialización de bases de datos de direcciones de correo electrónico.
- Realizar manipulaciones tecnológicas sobre el campo de "asunto" con el fin de evitar los filtros anti-*spam*.
- El diseño, venta y uso de *software* que permita crear, generar, compilar, recolectar, registrar o validar automáticamente direcciones de correos electrónicos, así como recolectar direcciones que ofrecen *chats* o conferencias virtuales –*bulletin board*– sin el conocimiento del receptor del correo electrónico o del administrador del sitio web que contiene la información.
- Generar automáticamente listas de contactos de correo electrónico mediante el uso de algoritmos u otras herramientas tecnológicas que combinen nombres, números, caracteres o códigos.

La regulación en torno al *spam* implica su concordancia con la legislación existente y la que se plantea que exista en el futuro en relación con la protección de datos personales y la legislación anticorrupción.

4. LEGISLACIÓN DE PROTECCIÓN DE DATOS PERSONALES Y ANTICORRUPCIÓN Y REGULACIÓN DEL SPAM

El proyecto de ley sobre datos personales propone, como finalidad, "regular y garantizar el derecho a la protección de datos personales, cautelando los derechos a la intimidad, identidad, honor y propia imagen".[11] Se incluyen en este proyecto de ley tanto principios de protección de datos personales, como los de información, consentimiento y seguridad, como derechos de la persona frente al tratamiento automatizado, como son los derechos de acceso, rectificación y cancelación, entre otros. Asimismo, se plantea la existencia de la Autoridad Nacional de Protección de Datos Personales (APDAP), que estaría adscrita a la Presidencia del Consejo de Ministros y que tendría entre sus funciones garantizar el cumplimiento de la legislación de protección de datos personales, administrar el registro nacional de datos personales, ejercer el control y conceder las autorizaciones, cuando corresponda, de las cesiones y transferencias de datos personales.

En cuanto a su relación con el *spam*, debe tenerse en cuenta que en el modelo inclusivo *opt-in* "el consentimiento marca la diferencia entre el *spam* legítimo o ilegítimo, entre licitud e ilicitud. Dicho consentimiento, otorgado por el receptor del correo electrónico, debe ser consentimiento consciente, informado y aplicable al correo que se hace referencia".[12] En cambio en el modelo *opt-out* los mensajes pueden ser enviados a cualquier persona, excepto a las que han manifestado expresamente su voluntad de no recibir más mensajes.

En los países miembros de la Unión Europea, donde hay una sólida legislación de protección de datos personales, se ha optado por el modelo *opt-in*, considerando que los correos electrónicos tienen datos personales que deben ser protegidos y que

11 Ministerio de Justicia del Perú. *Proyecto de Ley de Datos Personales* [en línea]. <http://www.minjus.gob.pe>. [Consulta: 15 de setiembre del 2005].

12 BRIAN NOUGRERES, Ana. "El *spam*: ¿Dis-función o de-función en la red de redes?". *Memorias del X Congreso Iberoamericano de Derecho e Informática*. Santiago: Universidad de Chile, 2004, p. 274.

para que llegue *spam* debe haber previamente una autorización o consentimiento. En este sentido, las autoridades encargadas de velar por el cumplimiento de la legislación que regula el *spam* son las agencias gubernamentales de protección de datos personales, como la Agencia de Protección de Datos Personales en España, y de la Comisión Nacional de Informática y Libertades en Francia.

En el Perú, el legislador ha optado por el modelo *opt-ut*, que no guarda coherencia con los lineamientos que se expresan en el Proyecto de Ley de Datos Personales elaborado por el Ministerio de Justicia. Así, la Ley 28493 establece como autoridad competente en materia de *spam* al Instituto Nacional de Defensa de la Competencia y de la Propiedad Intelectual (Indecopi), dejando de lado a la Autoridad de Protección de Datos, que se propone crear en el Proyecto de Ley de Datos Personales.

Por otra parte, el modelo *opt-out* permite el envío de correos electrónicos comerciales no solicitados, siendo requisito para su no envío que quien lo recibe manifieste su voluntad electrónica en contrario. Esta manifestación electrónica permite a los receptores compilar esta información en bases de datos, por lo cual se debate si incluir en las normas reglamentarias prohibiciones expresas en este sentido.

Asimismo, consideramos que la legislación que regula el *spam* debe ser igualmente concordada con la que regula el hábeas data. Conforme al artículo 200 inciso 3 de la Constitución Política del Perú:

> La acción de Hábeas Data, que procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el artículo 2 incisos 5) [derecho de acceso a la información de entidades públicas] y 6) [derecho a la intimidad] de la Constitución.

El Código Procesal Constitucional, aprobado por Ley 28237, del 31 de mayo del 2004, vigente desde noviembre de ese año (después de seis meses de su publicación) regula los procesos constitucionales de hábeas corpus, amparo, hábeas data, cumplimiento, inconstitucionalidad, acción popular y conflictos de competencia.

Con respecto al proceso de hábeas data, conforme al artículo 61, Derechos protegidos, del Código Procesal Constitucional:

> ... toda persona puede acudir a dicho proceso para:
> 1) Acceder a información que obre en poder de cualquier entidad pública, ya se trate de que la generen, produzcan, procesen o posean, incluida la que obra en expedientes terminados o en trámite, estudios, dictámenes, opiniones, datos estadísticos, informes técnicos y cualquier otro documento que la administración pública tenga en su poder, cualquiera que sea la forma de expresión, ya sea gráfica, sonora, visual, electromagnética o que obre en cualquier otro tipo de soporte material.
> 2) Conocer, actualizar, incluir y suprimir o rectificar la información o datos referidos a su persona que se encuentren almacenados o registrados en forma manual, mecánica o informática, en archivos, bancos de datos o registros de entidades públicas o de instituciones privadas que brinden servicio o acceso a terceros. Asimismo, a hacer suprimir o impedir que se suministren datos o informaciones de carácter sensible o privado que afecten derechos constitucionales.

El Código Procesal Constitucional establece que para la procedencia del hábeas data se requerirá que el demandante haya reclamado previamente, por documento de fecha cierta, el respeto de los derechos constitucionales protegidos y que el demandado se haya ratificado en su incumplimiento o no haya contestado (diez días para el derecho de acceso a información

de entidades públicas y dos días para el derecho de intimidad).

Excepcionalmente se podrá prescindir de este requisito cuando su exigencia genere inminente peligro de sufrir un daño irreparable, el que será acreditado por el demandante. Aparte de dicho requisito no será necesario agotar la vía administrativa que pudiera existir.

Todas estas disposiciones están vigentes y permiten ser aplicadas cuando se vulneran los derechos protegidos, incluso utilizando correos electrónicos, lo que crea la necesidad de concordar esta legislación con la que regula el *spam*.

Por otra parte, con respecto a la legislación anticorrupción, se establece que:

> ... siempre que lo permitan los principios fundamentales de su ordenamiento jurídico interno, cada Estado adoptará, dentro de sus posibilidades y en las condiciones prescritas por su derecho interno, las medidas que sean necesarias para permitir (...) la utilización de vigilancia electrónica (...) con el objeto de combatir eficazmente la delincuencia organizada.[13]

La vigilancia electrónica puede incluir el uso de rastreadores de correos electrónicos y el envío de estos en forma no autorizada, por lo que sería necesario también su concordancia con la norma sobre el *spam*.

Adicionalmente, se establece:

> ... a fin de combatir eficazmente la corrupción, cada Estado parte (...) adoptará las medidas que sean necesarias para prever el adecuado uso (...) de técnicas especiales de investigación como la vigilancia electrónica o de otra índole y las operaciones encubiertas, así como para permitir la admisibilidad de las pruebas derivadas de esas técnicas en sus tribunales.[14]

Con respecto al valor probatorio de los correos electrónicos y de los datos de tráfico de su envío y recepción, hay que considerar que:

> ... la evidencia digital es frágil y volátil. La información residente en los medios de almacenamiento electrónico puede ser borrada, cambiada o eliminada sin dejar rastro, lo cual limita la labor del investigador forense en informática tendiente a identificar y encontrar elementos claves para esclarecer los hechos relevantes de una investigación. En este sentido, la evidencia digital es pieza probatoria básica que requiere una revisión detallada sobre cómo se crea, cómo se recolecta, cómo se asegura y, finalmente, cómo se presenta en la corte, con el fin de aportar con claridad y precisión factores que orienten las decisiones sobre casos en que esta evidencia sea parte fundamental del mismo.[15]

5. LA REGULACIÓN DEL CORREO ELECTRÓNICO COMERCIAL NO SOLICITADO (*SPAM*) EN INTERNET Y EL DERECHO INFORMÁTICO

El derecho informático tiene por objeto resolver los problemas jurídicos que plantea el uso de la informática, aplicando para ello los propios métodos jurídicos y los enfoques de sistemas existentes. Tal es así que el método sistemático permite el trata-

13 Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional. Palermo, 12 de diciembre del 2000, artículo 20, numeral 1.

14 Convención de las Naciones Unidas contra la Corrupción. Artículo 50, numeral 1. Nueva York, 2003.

15 CANO, Jeimy. "Admisibilidad de la evidencia digital: De los conceptos legales a las características técnicas". *Derecho de Internet & telecomunicaciones*. Op. cit., p. 178.

miento de los temas jurídico-informáticos en forma coherente e integral.

Los problemas jurídicos que se originan por internet, el ciberespacio, la informática, las nuevas tecnologías de la información son materia de estudio del derecho informático y su solución eficaz posibilita la mayor aceptación y confianza del ciudadano en el comercio electrónico y en la contratación electrónica en general.

El correo electrónico comercial no solicitado (*spam*) se ha regulado en el Perú mediante la Ley 28493, siguiendo el modelo *opt-out*. En países donde se protegen los datos personales en forma robusta (como los países de la Unión Europea) el modelo adoptado es *opt-in*. La aplicación del modelo *opt-out* no guarda suficiente coherencia con la orientación y lineamientos planteados en el Proyecto de Ley de Datos Personales elaborado por el Ministerio de Justicia ni con los alcances de la protección ya vigente del proceso de hábeas data conforme al Código Procesal Constitucional. No obstante, consideramos que la regulación del *spam* era necesaria, por lo que ya adoptado un modelo, las normas reglamentarias que se dicten deben procurar adecuar las normas generales a la realidad tecnológica imperante.

Consideramos que la regulación deberá incluir, entre otras, normas que permitan: determinar las distintas variantes de correos electrónicos originados en el país, acciones relacionadas con el *spam* que son prohibidas, la implementación adecuada de la compensación pecuniaria en la vía judicial, la existencia de una vía paralela administrativa ante Indecopi en materia de protección al consumidor y publicidad, la concordancia con normas penales cuando por correo electrónico se cometa un delito debidamente tipificado, la valoración adecuada de la evidencia digital.

Por otra parte, consideramos que la legislación que regula el *spam* debe ser concordada con la legislación de telecomunicaciones, especialmente en torno a los problemas de resguardo de la privacidad y el secreto de las telecomunicaciones. En este sentido, tengamos en cuenta que:

> ... la regulación de las telecomunicaciones (...) ha sido orientada en los últimos años hacia la introducción de la libre competencia, bajo el supuesto de que la apertura de estos mercados permitirá una maximización de la cobertura de servicios, una elevación de su calidad, disminución de sus precios y una racionalización de gastos estatales.[16]

Lo que no debe limitar la protección de la privacidad y secreto de telecomunicaciones, por lo cual debe concordarse igualmente la legislación de telecomunicaciones con la que regula el *spam*.

La visión jurídico-informática propia del derecho informático permite este enfoque sistemático, necesario y adecuado para hacer en forma coherente la concordancia e interrelación de las normas que regulan el *spam*, con las otras normas de nuestro ordenamiento jurídico.

Por otra parte, las normas planteadas sobre el *spam* tienen carácter territorial; la solución integral de los problemas planteados por la informática en torno al *spam* también requieren disposiciones de carácter supranacional, mediante convenios internacionales u otros instrumentos, en los cuales, creemos, debe aplicarse el enfoque del derecho informático para lograr una regulación del *spam* coherente y eficaz.

16 SÁNCHEZ GARCÍA, Carlos Andrés. "Apertura de la red de acceso: Experiencia europea y perspectiva colombiana". *Derecho de internet & telecomunicaciones*. Op. cit., p. 901.