República de Colombia

Rama Jurisdiccional del Poder Público
Juzgado Segundo Promiscuo Municipal
Rovira Tolima

Julio veintiuno (21) de dos mil tres (2003)

Rad. 73-624-40-89-002-2003-053-00

Procede esta instancia constitucional a proferir la sentencia que en derecho corresponda dentro de la presente acción de tutela, instaurada por el ciudadano JUAN CARLOS SAMPER POSADA en contra de JAIME TAPIAS, HECTOR CEDIEL Y OTROS, no encontrando el despacho causal alguna de nulidad que pueda invalidar lo actuado.

SITUACIÓN FÁCTICA PROCESAL

1. La narra el apoderado de la parte actora en los siguientes términos:

1.1 Juan Carlos SAMPER es titular del correo electrónico **jcsamper@i-network.com** y de todos los demás correos creados bajo el nombre de dominio "i-network.com".

1.2 Jaime TAPIAS es una persona natural que actúa bajo el nombre comercial "VIRTUAL CARD".

1.3 VIRTUAL CARD ofrece los servicios de mailing, multimedia, bases de datos, boletines electrónicos y consultorías e-business a través de Internet.

1.4 El 21 de Julio de 2002, Juan Carlos SAMPER recibió el primer correo electrónico no solicitado de la firma VIRTUAL CARD

1.5 A este correo, Juan Carlos SAMPER respondió solicitando que fuera retirado de la lista de la base de datos de VIRTUAL CARD, ya que no había informado su correo a ninguna base de datos ni lista de correos.

1.6 El 21 de Julio de 2002 a las 20:31, Jaime TAPIAS, respondió a la solicitud de Juan Carlos SAMPER lo siguiente: i) que Juan Carlos SAMPER se encontraba fuera de la lista de VIRTUAL CARD, ii) que en mercadeo es permitido buscar prospectos de clientes por todos los medios de comunicación, incluido Internet y, iii) que no conocía ninguna legislación sobre privacidad que pudiera limitar la actividad desarrollada por su empresa.

1.7 El 22 de Julio de 2002, Juan Carlos SAMPER reitera su solicitud de ser retirado de la lista de correo y aclara que el problema radica en que la estrategia de mercadeo se realice sin solicitud ni autorización de los usuarios.

1.8 A pesar de que Jaime TAPIAS le había asegurado a Juan Carlos SAMPER en la comunicación enviada el 21 de Julio que se encontraba fuera de la lista de VIRTUAL CARD, el 2 de Septiembre de 2002, Juan Carlos SAMPER recibió un nuevo correo de VIRTUAL CARD en el que le "recordaban" los beneficios del correo electrónico como estrategia de marketing.

1.9 El 3 de Septiembre de 2002, Juan Carlos SAMPER envió dos mensajes a VIRTUAL CARD, en los que solicita una vez más que sus correos sean retirados de la lista de correos. Señala además que ya ha intentado eliminarse de todas las formas posibles

1.10 Un mes después, el 3 de Octubre de 2002, Juan Carlos SAMPER recibió un correo firmado por HECTOR CEDIEL y CONSUELO MORENO en el que le anunciaban la "alianza estratégica" de VIRTUAL CARD, OKSON GROUP y HECTOR CEDIEL y le solicitaban su autorización para enviar sus promociones a su dirección mail

1.11 Juan Carlos SAMPER contestó el 3 de octubre con un contundente "POR N-ESIMA VEZ SAQUEME DE SU LISTA..."

1.12 El 5 de Octubre de 2002, luego de recibir un nuevo correo de TIME SEMINARIOS, cliente de VIRTUAL CARD, Juan Carlos SAMPER intenta una vez más ser retirado de la lista.)

1.13 Ese mismo día TIME SEMINARIOS le responde que en efecto ha sido retirado de la lista

1.14 Todos los intentos anteriormente descritos resultaron fallidos. El 18 de Octubre de 2002, Juan Carlos SAMPER recibió un nuevo correo de la Corporación INNOVAR, otro cliente de VIRTUAL CARD.

1.15 El 19 de Octubre de 2002, Jaime TAPIAS, envió un nuevo correo a Juan Carlos SAMPER en el que señala que "sabe" que su forma de trabajo no es del agrado de Juan Carlos SAMPER. Agrega que "la base general se dejará de usar desde noviembre de 2002 en la cual ustedes se encuentran" y luego señala "creo que es hora de cambiar el método de esperar un permiso de una persona que nunca lo va a suministrar por el problema del spam y el junkmail opt in". Y concluye su correo con la siguiente frase "Señor Samper no es por consolarlo pero a mi correo virtualcard me llegan 150 correos publicitarios, porno, basura, virus, etc. que filtramos en el servidor únicamente por colocar la dirección en un directorio de empresas de publicidad.

1.16 Por un tiempo pareció que VIRTUAL CARD esta vez había cumplido su promesa. Sin embargo, el 2 de Diciembre de 2002, Juan Carlos SAMPER recibió un nuevo correo de LAMY, cliente de VIRTUAL CARD.

1.17 Finalmente, el 27 de Mayo de 2003, Héctor CEDIEL, quien se identifica como el encargado de la base de datos, envió un nuevo correo a Juan Carlos SAMPER

1.18 En resumen, los DEMANDADOS y sus clientes, en conjunto, han enviado por lo menos ocho correos electrónicos a Juan Carlos SAMPER, y éste a su vez les ha enviado por lo menos siete correos electrónicos suplicando de todas las maneras, ser eliminado de la base de datos de VIRTUAL CARD.

TRÁMITE DE LA ACCIÓN

La presente acción de tutela fue remitida al Juzgado Promiscuo Municipal Reparto, por correo electrónico oficial (adiazg@cendoj.ramajudicial.gov.co) por el accionante JUAN CARLOS SAMPER POSADA representado por apoderado judicial Dr., ÁLVARO RAMIREZ BONILLA, poder presentado virtualmente ante el Señor Notario Diecinueve del Círculo de Bogota (info@notaria19.com) Dr. Norberto Salamanca F. quien da fe del contenido del mensaje/poder otorgado, acción que fuera repartida extraordinariamente en soporte electrónico, correspondiéndole al Juzgado Segundo Promiscuo Municipal su trámite.

Mediante auto de fecha julio ocho de dos mil tres se admitió la solicitud de tutela y se corrió traslado a los accionados JAIME TAPIAS, HECTOR CEDIEL Y OTROS, a su domicilio virtual por medio electrónico (Hcediel@virtualcard.d2g.com; jtapias@virtualcard.d2g.com; virtualcard@007mundo.com y jaime@virtualcard.dns2go.com para que dentro del término de tres (3) días dieran contestación, todo lo anterior con base a los preceptos del artículo 12 de la ley 794 de 2003, que modificó el artículo107 del Código de Procedimiento Civil, en donde se permite a los Despachos Judiciales hacer uso de las nuevas tecnologías

R E S Ú M E N E S D E L A S C O N T E S T A C I O N E S

1. CONTESTACIÓN DEL CIUDADANO JAIME LEONARDO TAPIAS GONZÁLEZ

Manifiesta el accionado que la competencia para conocer de la acción de tutela recae sobre los jueces donde ha ocurrido la violación o la amenaza que motivan la solicitud en primera instancia sea contra autoridad pública o particular y por consiguiente no es el Juez promiscuo municipal de Rovira el competente para conocer y fallar la presente tutela ya que los hechos no ocurrieron en este Municipio.

Argumenta que el factor territorial es el elemento principal para que se conozca o no de la acción y que los hechos denunciados ocurrieron en la ciudad de Bogotá por lo cual sería éste el territorio donde se debió instaurar la acción de tutela pues ha sido desde esa ciudad donde se han enviado los correos electrónicos y donde el señor Samper supuestamente recibió los agravios.

Igualmente, agrega no estar de acuerdo con lo plasmado en el auto que admitió la tutela pues dice que la tesis plasmada por el señor Juez no tiene un respaldo legal, doctrinario ni jurisprudencial, pero que sí es aplicable para casos en que las comunicaciones puedan enviarse desde cualquier parte y para un usuario que supuestamente no se tiene conocimiento en donde se encuentra pero que en el

presente evento se tiene conocimiento el lugar donde se produjo y donde se recibió el supuesto agravio.

Sigue argumentando el accionado que el accionante ha escogido este Despacho judicial en forma deliberada pudiéndolo hacer en la ciudad de Bogotá donde funcionan cerca de ciento cincuenta (150) Despachos Judiciales competentes para conocer de la misma con competencia funcional y territorial para hacerlo y por consiguiente buscar: Impedimento de ejercer el Derecho de defensa. Precisamente, ante la distancia existente y la dificultad de comunicaciones no se puede tener acceso a la totalidad del libelo de tutela. Vulneración del Debido proceso. Este aspecto manifiesta que todas y cada una de las pruebas se solicitan a entidades destacadas en esta ciudad o al suscrito en la misma ciudad de Bogotá. Por lo anterior no se puede tener un debido proceso, por no existir la inmediación, porque la práctica de Inspección Judicial, medio idóneo y eficaz para aclarar los supuestos alegados por el accionante y poder determinar que no se ha vulnerado principio fundamental alguno al supuesto ofendido, no se podrá practicar debido a la distancia existente entre el lugar donde funciona este Despacho y la ciudad, de Bogotá donde reposan los diferentes medios de prueba.

Respecto de los derechos vulnerados como lo son el de la intimidad y de Habeas Data, estos no han sido violados en ningún momento pues no se encuentran descritos en las sentencias aportadas y que por el contrario con estas sentencias se está explicando que estos derechos no han sido coartados pues ninguno de los textos enviados por él se ajustan a la descripción realizada por la Corte Constitucional y por el Congresista que defiende una ley relacionada con delitos y situaciones informáticos, luego no entiende de donde se pueda generar la vulneración del derecho fundamental a la intimidad.

Respecto de la violación del Habeas data manifiesta que solo posee una dirección electrónica del señor JUAN CARLOS SAMPER, y no tiene almacenado algún dato personal. Es mas que inicialmente no conocía el nombre de la persona que mantenía este correo, menos aún su actividad, lugar de residencia y cuales sus ocupaciones.

Argumenta el accionado que luego de cruzar algunas comunicaciones con el señor SAMPER, su correo electrónico desde finales del año pasado ha sido suprimido de sus bases de datos y en lo corrido del año no ha enviado correos ofreciendo productos. Que si ha sido otra persona en este caso el señor HECTOR CEDIEL y quizá otras personas quienes han remitido correos al señor SAMPER a ellos y solo a ellos corresponde abstenerse de hacerlo como el ya lo hizo desde finales del año 2002.

Que en su base de datos solo existía su correo electrónico, el cual puede ubicarse en cualquier seminario en el que el mismo actúe, en bases de datos que se adquieren de otras personas o clientes con fines comerciales, etc., pero que nunca contienen ninguna información personal del supuesto ofendido como tampoco nada que pueda serle negativo en su intimidad.

Que no es un hecho cierto que el señor SAMPER continúe en sus bases de datos ya que para finales de 2002 fue definitivamente retirada esta dirección electrónica de su base de datos y que en sus comunicaciones siempre se da la opción al cliente de marcar si quiere recibir mayor información del producto que se le ofrece o si por el contrario, no quiere recibir mas información y para ello, solo basta dar un clic en la casilla que se escoja. Este corresponde al permiso que se le solicita a la persona.

Por lo demás, el usuario puede bloquear o no abrir los correos no deseados o basura que diariamente inundan nuestras direcciones electrónicas, especialmente si las mismas corresponden a Hotmail, cuyos servidores operan en el exterior,.

Define el término Spam como aquella actividad por la cual se envía información no solicitada a un destinatario especifico, sin su consentimiento u aprobación. Este se caracteriza por que no registra el origen donde procede entendiéndose por ello la dirección electrónica Email de origen y se envía a múltiples destinatarios.

El sistema de envío de Virtualcard, por el contrario, detalla en sus mensajes la dirección de correo de origen, el asunto, la solicitud de permiso para recibir más información, la opción de salir de la lista de envío y la opción de salir de cualquier lista que se encuentre el usuario que lo solicita. Todo lo anterior dando cumplimiento a las características mínimas de cumplimiento de los boletines de permiso y las herramientas que debe contener para que el usuario no reciba más información.

Por Lo anterior considera que no se ha violado el derecho fundamental de HABEAS DATA que alega el accionante, por lo que tampoco puede prosperar la acción elevada.

Concluye diciendo que hará las averiguaciones correspondientes para verificar la legalidad del correo utilizado para su notificación ante el Consejo Superior de la Judicatura y lo relacionado con la reglamentación o cambio de competencia para que la tutela se tramite fuera de Bogotá.

2. CONTESTACIÓN DEL CIUDADANO HÉCTOR CEDIEL

El despacho por el mismo medio electrónico notificó la acción de tutela al señor HÉCTOR CEDIEL, correo que según su manifestación escrita abrió el l4 de julio del año en curso y se “enteró “ del contenido de la acción respondiéndola escuetamente de la siguiente manera :

Dice haber enviado un propuesta como agencia de publicidad buscando nuevos productos por este medio electrónico ya que según él, el e-mail marketing es un medio novedoso y de refuerzo y asegura: “ siempre y cuando no se maneje como SPAM “.

Que es de conocimiento del accionante Juan Carlos Samper que al colocar el e-mail en tarjetas comerciales o en eventos empresariales está sometido a recibir comunicaciones en cualquier momento.

Argumenta que es totalmente viable por su parte y como publicista profesional utilizar las empresas que poseen los equipos para enviar esta información por esta razón recurrió a Jaime Tapias por la economía del servicio. Por lo tanto considera que no incurrió en ninguna violación de la intimidad al ya mencionado señor Samper por cuanto se trataba solamente de una propuesta comercial y que su mail es utilizado únicamente para recibir propuestas comerciales y que es solo su responsabilidad el envío del paquete promocional.

Concluye tomando esta situación como un impase y no como una situación que genere un conflicto judicial.

C O N S I D E R A C I O N E S D E L D E S P A C H O

1. El problema jurídico planteado

Conforme a los antecedentes que se han planteado el problema jurídico planteado impone al despacho determinar si es procedente la tutela contra el particular JAIME LEONARDO TAPIAS y determinar que la tutela es viable procesálmente, si analizada la situación que dio origen a ella deben ampararse o no los derechos fundamentales cuya protección invoca el actor.

2. La Competencia del Juzgado

Se ha planteado que el Juzgado no es competente porque la consumación de la conducta vulneradora del derecho fundamental acaeció en la ciudad de Bogotá y que el lugar de residencia de las partes es ese Distrito Capital.

El demandado, algo extraño pues conocedor de las nuevas tecnologías, precisamente porque haciendo uso de ellas se le acusa de vulnerar un derecho fundamental, alega una jurisdicción material, olvidándosele la virtualidad que comprende todos las conductas informáticas con implicaciones jurídicas.

Ya sobre el lugar de los efectos que produce la vulneración de un derecho fundamental el Consejo de Estado[1] precisamente estudiando el decreto que el demandado arguye en su contestación, al respecto la Sala Plena de esa Corporación se ha pronunciado al afirmar que el lugar donde se produce la violación o amenaza al derecho fundamental no sólo es aquel donde se despliega la acción o se incurre en la omisión, sino también a donde alcanzan los efectos de tales conductas; si bien es cierto que no habla textualmente sobre los efectos virtuales, tal vez por lo novedoso del tema, no es menos verdad que los efectos jurídicos del manejo inadecuado de las nuevas tecnologías se desplegaron en el ciberespacio en donde está ubicado el domicilio virtual del actor; el hecho que ninguna norma lo establezca hasta este momento no nos impide considerar que este Juzgado como cualquier otro en cualquier parte de la República de Colombia, es el competente para conocer de un asunto de esta naturaleza hasta cuando taxativamente la ley señale lo contrario.

Los efectos jurídicos del uso de las nuevas tecnologías y su jurisdicción, considera el Estrado no se deben tomar con una simple subsunción, como lo pretende hacer ver el demandado de ubicarlo materialmente en un circunscripción física y formal como se le ha conocido desde antes que se creara la informática como medio de comunicación. Además la Ley Estatutaria de la Administración de Justicia[2], contempla el uso de las nuevas tecnologías al servicio de la administración de justicia, precisamente en su artículo 95, reza que los Juzgados, Tribunales y Corporaciones judiciales podrán utilizar cualesquier medio técnico, electrónico, informático y telemático para el cumplimiento de sus funciones. Agrega la norma en comento que los documentos emitidos por los

---

[1] Acción de Nulidad Decreto 1382 de 2000. Diciembre 18 de 2002. Consejo de Estado. Sala de lo Contencioso Administrativo CP. Dr. CAMILO ARCINIEGAS ANDRADE. Actor. Franky Urrego Ortiz y otros. Radicación 11001-03-24-000-2000-6414-01. Mayor ilustración en la web site del Consejo de Estado www.ramajudicial.gov.co

[2] Ley 270 de 1996

citados medios, cualquiera que sea su soporte, gozarán de validez y eficacia de un documento original siempre que quede garantizada su autenticidad, integridad y el cumplimiento de los requisitos exigidos por las leyes procesales. También dice que los procesos que se tramiten con soporte informático garantizarán la identificación y el ejercicio de la función jurisdiccional por el órgano que la ejerce, así como la confidencialidad, privacidad y seguridad de los datos de carácter personal que contenga en el término que establezca la ley.

Como Juez Constitucional el ámbito jurisdiccional es todo el territorio nacional y la norma no excluye mi competencia en el ciberespacio, porque recordemos de que se está hablando de un hecho ocurrido en este ámbito así el demandado no lo quiera reconocer pese a que se trata de un informático, resultando muy asombroso su actitud de que querer quitarle relevancia al medio en donde precisamente está realizando sus tareas de e-marketing. La competencia, el demandado la está circunscribiendo a unas coordenadas físicas, pero se le ha olvidado que el meollo del asunto es la virtualidad y precisamente el domicilio virtual del señor JUAN CARLOS SAMPER es su correo electrónico, tan seria es esta dirección que nuestra legislación le dio amparo cuando obliga a los comerciantes a registrar su domicilio virtual en la cámara de comercio en donde aparecen asociados, tal es el caso del artículo 29, parágrafo único de la Ley 794 de 2003.

Sobre la implementación de los recursos informáticos, ya el Dr. Santiago Muñoz Medina[3] director del cendoj, realizó una dilecta conferencia en el Hotel Ambalá de Ibagué y para aquella oportunidad afirmó: “Con esto (la informática) tiene que ver con la descongestión física del despacho, no es fácil implantar la informática y la telemática, no es suficiente dotar una red para que nos mantenga informados, lo mas importante de esta nueva política es la resistencia a la tecnología que no hace fácil el uso de estos recursos, además el abuso en la utilización de este recurso porque en realidad no se utiliza para lo que debería utilizarse, no se le da eficiencia y eficacia que exige la Constitución.[4]”

Sobre la competencia virtual, pese a que somos pocos los colombianos que lo exponemos, existen varios tratadistas latinoamericanos que hablan sobre el domicilio, entre otros, el Maestro Julio Núñez Ponce[5] que afirma que el tema de domicilio virtual está directamente relacionado con el tema de jurisdicción y competencia en Internet y que los comentarios efectuados a normas existentes a su ordenamiento jurídico (Perú) le permiten aproximarse al contenido que podría darse al domicilio virtual en sus implicaciones civiles, societarias y tributarias, esto es, que el domicilio material de un ciudadano se le toma como el de la dirección (o lugar) de la ciudad en donde habita ora en donde desarrolla sus actividades profesionales, igualmente pasa con la dirección del correo electrónico, es allí en donde desarrolla diferentes actividades virtuales las que puede realizar en cualquier parte del mundo, siendo éste su domicilio virtual que jamás debe ser asimilado en forma exacta con la materialidad de otros domicilios. .

El Domicilio Virtual estaría conformado por la dirección electrónica que constituye la residencia permanente en la Web de la persona.

---

[3] CENDOJ. Centro de documentación Judicial de la Rama Judicial de Colombia, adscrito al Consejo Superior de la Judicatura y encargada de todo lo relacionado con los recursos informáticos.

[4] Conferencia del Dr. Santiago Muñoz Medina, director del CENDOJ dictada en el Hotel Ámbala de Ibagué Tolima, a los estudiantes de tercer año de derecho de la Universidad Cooperativa de Colombia Seccional Ibagué. Memorias reposan en la Biblioteca del Claustro.

[5] NUÑEZ PONCE, Julio. Abogado, Magíster en Derecho Empresarial, Catedrático de Derecho Informático en la Universidad de Lima. Mayores detalles puede encontrarlos en la Revista Electrónica de Derecho Informático en www.alfa-redi.org

Pensemos que el domicilio ordinario de un ciudadano común lo constituye la residencia habitual que tiene en un lugar, lo que implicaría en tratándose de su domicilio virtual, la utilización constante de una dirección electrónica, la que puede ser su homepage ora su e-mail, como lo son actualmente los comerciantes y personas jurídicas[6] inscritos en el registro mercantil, porque deben registrar su e-mail pop3 o smtp[7] ora el de su Homs page que es otra forma de notificación virtual, ya en otrora oportunidad este Estrado notificó a Ministros del Despacho de la Administración del Dr. Andrés Pastrana, por acción de tutela que se incoó para ese entonces en contra de la Nación, accediendo a su página virtual; lugar en donde se le enviarían las notificaciones informáticas; algo igual acontecería, con las personas jurídicas o comerciantes para la ejecución de actos jurídicos electrónicos, sobre todo en materia de notificaciones judiciales, comercio electrónico y transferencia de fondos.

Por lo plasmado anteriormente, no es de recibo para el Estrado lo referente por el accionado respecto del contenido del auto admisorio de la tutela en donde manifiesta que lo anteriormente esbozado es una simple teoría sin respaldo legal, doctrinario o jurisprudencial, cuando la realidad legal es totalmente diferente, porque el parlamento no solo ha proferido las leyes 527[8] de 1999 y 794[9] de 2003, que se refieren al uso del dato informático, porque además existen toda una reglamentación que sobre el tópico expiden las diferentes superintendencias del país.

Traigo a colación una frase sobre la aterritorialidad de la Internet de 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" [10]

3. La Firma Electrónica

El demandado ha argüido que los documentos expedidos por este Estrado en soporte electrónico no tienen ninguna validez en razón a que no están firmados analógicamente y no tiene el amparo de ninguna entidad de certificación de firma digital. Se conoce en el mundo del Derecho Informático la diferencia entre firma digital y firma electrónica,

---

6 Art. 315 Código de Procedimiento Civil, modificado por la Ley 794 de 2003

7 POP Postal Office Protocol: Servidor de correo entrante. SMTP Simple Mail Transfer Protocol: Servidor de correo saliente.

8 Ley 527 de Agosto 18 de 1999, por medio de la cual se define y reglamente el acceso y uso de los mensajes de datos, comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

9 Ley 794 de Enero 8 de 2003. Reforma al Código de Procedimiento Civil.

10 Law and Borders—The Rise of Law in Cyberspace. Para una mejor comprensión visite http://www.cli.org/ X0025_LBFIN.html

precisamente el maestro Rodolfo P. Ragoni[11] define la firma digital como los datos expresados como formato digital utilizados como método de identificación de un firmante y de la verificación de la integridad del contenido de un documento digital, agrega que debe cumplir con los requisitos de pertenecer únicamente a su titular, encontrarse bajo su absoluto y exclusivo control, ser susceptible de verificación y estar vinculada a los datos del documento digital de modo que cualquier modificación de los mismos ponga en evidencia se alteración. El mismo define la firma electrónica como los datos en forma electrónica, asociados a otros datos electrónicos o vinculados de manera lógica con ellos, utilizados como medio de identificación, y que no reúne uno o mas de los requisitos para ser considerada como firma digital.

Parece que el demandado no ha comprendido el sentido de la ley 527 de 1999, en lo que se refiere a la validez de mensaje de datos. Precisamente el artículo 6° de la norma en estudio, establece que cuando cualquier norma requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos, si la información que éste contiene es accesible para su posterior consulta.

Ahora bien en tratándose de la firma, motivo de preocupación del libelista, la ley de marras establece precisamente en su artículo séptimo que cuando cualquier norma exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma, en relación con un mensaje de datos, se entenderá satisfecho dicho requerimiento si se ha utilizado un método que permita identificar al hincado de un mensaje e datos y para indicar que el contenido cuenta con su aprobación. Igualmente que el método sea tanto confiable como apropiado para el propósito por el cual el mensaje fue generado o comunicado.

Y en lo que se refiere al original, preceptúa que cuando la norma requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos si existe alguna garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma. Agrega que de requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona que se deba presentar.

Como se puede observar, todos los requisitos relacionados en la ley en estudio se han surtido en el trámite de la presente acción de amparo, puesto que se han llenado a cabalidad. Hemos realizado la emisión de documentos en soporte electrónico y no hemos estampado allí firmas digitales toda vez que la Rama Judicial aún no cuenta con fedatarios que certifiquen tal situación. No obstante la firma electrónica, no digital, repetimos se debe entender en los documentos expedidos por el Estrado, toda vez que se ha utilizado un método que permite identificar al iniciador, como es el uso de la cuenta oficial del Consejo Superior de la Judicatura, las consecuencias originadas por los documentos emitidos son legales y el contenido ha contando siempre con mi aprobación, que soy su emisor. En cuanto a la integridad y conservación de la información digital creada por este Estrado ha permanecido en forma completa e inalterada en los equipos informáticos del Juzgado, en donde se custodia como cualquier expediente en soporte papel.

El método es confiable, pues se está haciendo uso del derecho constitucional de la Buena Fe y creemos que las partes, hasta cuando no se demuestre lo contrario, están actuando bajo ese derecho fundamental.

---

11 RAGONI. Rodolfo P. E-money, la importancia de definir el medio de pago en el e-commerce, Ed. Prentice Hall, pag.242. 1ª. Edición Buenos Aires Argentina.

Seguramente la presente actuación electrónica generará algunas falencias, por razones propias, tal vez esta pieza procesal se torne en la primera en el país y origina una novedad en el uso de las nuevas tecnologías, pero el Estrado cree que a medida que pase el tiempo el uso de la informática será masivo, cumpliendo así los propósitos del CENDOJ de la descongestión (Despachos al día), economía (no mas soporte papel) y celeridad (rapidez en al información) de las actuaciones judiciales.

La firma digital, cuando se implemente en los trámites judiciales, tal vez superemos los escollos que hoy se presentan con el manejo de los documentos en soporte electrónico. Ésta consiste básicamente en la aplicación de algoritmos de encriptación a los datos, de esta forma, sólo serán reconocibles por el destinatario, el cual además podrá comprobar la identidad del remitente, la integridad del documento, la autoría y autenticación, preservando al mismo tiempo la confidencialidad. La seguridad del algoritmo va en relación directa a su tipo, tamaño, tiempo de cifrado y a la no violación del secreto.

Ahora bien, este despacho judicial está recibiendo correspondencia continuamente procedente de la oficina de la administración judicial, consejo seccional de la judicatura y otros entes judiciales, a la cual se le da plena credibilidad, por provenir, precisamente de despachos acreditados y confiables, así la correspondencia llegue en fotocopia y sin una firma original; pero lo que se quiere dar a entender es la confiabilidad de su procedencia para así mismo no dudar del contenido; para citar el caso mas reciente tenemos el recibo de la circular No. 47 emanada de la presidencia de la Sala Administrativa del Consejo Superior de la Judicatura en donde el presidente Dr. Gustavo Cuello Iriarte, establece unas directrices para el trámite de las comisiones, comunicación que no viene con rúbrica analógica. Siguiendo el lindero interpretativo del demandado, el Estrado no debería acatar lo ordenado en dicha circular por la potísima razón de no venir firmada.

Con ello queremos significar que el método utilizado para el envío de dicho documento, la Dirección de Administración Judicial del Tolima, nos permite identificar el iniciador del mensaje, lo que indica que su contenido cuenta con su aprobación; el método de comunicación se torna confiable y apropiado para cumplir los propósitos de su contenido. Todo esto se le debe sumar el principio constitucional de la buena fe, que se entiende plasmado en todas las conductas del hombre hasta cuando no se le pruebe lo contrario.

4. La Solución al problema

Considera el Estrado que desde el punto de vista procesal es procedente la acción de tutela contra el particular Jaime Leonardo Tapias, porque el solicitante con respecto a éste se encuentra en un estado de indefensión.

En relación con el estado de indefensión, recordemos que en el texto constitucional correspondiente al artículo 86, dice que la ley establecerá los casos en que la acción de tutela procede contra particulares respecto de quienes el solicitante se encuentre en estado de subordinación o indefensión.

Es importante resaltar entonces que la indefensión se predica respecto del particular contra quien se interpone la acción. Este particular es quien con su conducta activa u omisiva pone en peligro o vulnera un derecho fundamental correcto del indefenso. Además la tutela se torna procedente porque el accionante acreditó cómo en varias oportunidades lo hizo la súplica a los demandados para que no le enviaran mas mensajes no solicitados como también lo borraran de sus base de datos, porque no había autorizado su difusión y recepción de mensajes.

De conformidad con el numeral 4º. Del art. 42 del decreto 2591 de 1991, el estado de indefensión acaece o se manifiesta cuando la persona ofendida por la acción u omisión del particular, sea éste persona jurídica o su representante, se encuentra inerme o desamparado, es decir, sin medios físicos u jurídicos de defensa o con medios y elementos insuficientes para resistir o repeler la agresión o la amenaza de vulneración a su derecho fundamental; estado de indefensión que se debe deducir, mediante el examen por el Juez de la tutela, de los hechos y circunstancias que rodean el caso en concreto.

No es otra la situación del accionante puesto que el medio utilizado por el particular tiene el suficiente poder de penetración que no ha podido ser repelido por el agredido a pesar de sus múltiples súplicas para que se deje de bombardear con información no solicitada, lo cual denota la situación de indefensión pues este no parece disponer por sí mismo de una situación de equivalencia que le permita contrarrestar en igualdad de condiciones la sensación adversa generada en su contra.

5. Los presuntos derechos vulnerados

5.1. El medio empleado para vulnerarlos El Spam

El apoderado del actor, alega que a su cliente se le vulneraron los derechos de habeas data, autodeterminación informática y el de intimidad, a través de correo spam; antes que analicemos si se han violado o no dichos derechos fundamentales, el Estrado considera necesario entrar a hacer algunas consideraciones sobre lo que es el spam o ACE[12], como lo llaman en Europa .

El Maestro Iñigo de la Maza Gazmuri[13] hace un juicioso estudio sobre la expresión "spam" en donde nos dice que 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[14]. Según algunos comentaristas[15] 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[16] , 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 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

---

12 A.C.E. Abuso del correo electrónico. Mayor información podrá encontrar en www.cauce.org

13Iñigo de la Maza Gazmuri Profesor Facultad de Derecho Universidad Diego Portales.

14 Ver Cyberangels. http://www.cyberangels.com/law/spam/

15ver 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/ ; SORKIN, David. *Technical and Legal Approaches to Unsolicited Electronic Mail.*
U.S.F. L. REV. 325

16 Es el acrónimo de multi-used shared hallucination

un mundo" Enzer, Matisse, Glosary of Internet Terms[17]. 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 restaurante 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.")[18] 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.

El envío de correos electrónicos no solicitados posee costos relevantes que se radican mayoritariamente en los usuarios y en los proveedores de servicios de Internet.2 Se trata además de una práctica que se difunde con bastante indiferencia de las fronteras territoriales ora virtuales. 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.

A continuación el Estrado hará un pequeño estudio sobre el spam, examinaremos los elementos que deberían reunirse en una definición de spam y las controversias que giran en torno a las definiciones disponibles. Haremos una pequeña reseña histórica del spam. Argumentaremos las diferencias que existen con otras especies de marketing directo y la necesidad de restringirlo. Examinar las respuestas que es posible dar a este fenómeno desde el punto de vista del derecho, las normas sociales, soluciones tecnológicas o de "código", y el mercado). Resaltaremos los avances legislativos sobre el tópico en Colombia y en las Comunidades Europeas.

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 esa decisión, recién es posible preguntarse qué modalidades regulatorias y en qué medida pueden ser utilizadas para enfrentarlo. Aún cuando para algunos cualquier correo no solicitado es spam, las dos definiciones más aceptadas de spam son: correos electrónicos comerciales no solicitados CECNS[19] y correos electrónicos masivos no solicitados CEMNS[20].

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

---

[17] Mayo ilustración si visita http://www.matisse.net/files/glossary.html#M

[18] Glossary of Internet Terms. http://www.matisse.net/files/glossary.html#U

[19] El acrónimo de unsolicited comercial e-mail [UCE]

[20] El acrónimo de unsolicited bulk email [UBE])

previamente ha buscado terminar una relación existente, usualmente instruyendo a la otra parte de no enviarle más comunicaciones en el futuro. 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 del mundo, lo que suele considerarse en el caso de las comunicaciones comerciales es la promoción de algún tipo de bienes o servicios. En este sentido, por ejemplo, la Directiva 2000/31 de las Comunidades Europeas[21] 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 califique como spam o puede tratarse de mensajes substancialmente similares. 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.

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. En el caso de definirlo como CECNS: ¿Por qué 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?

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 las 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.

El spam es un gran negocio que invade nuestros buzones. La mejora de los accesos a Internet ha incrementado el volumen del spam tanto por parte de los emisores como destinatarios. Los emisores porque disponen de mas posibilidades de ancho de banda y uso de servidores propios. Los receptores porque debido a las tarifa planas y la consecuente reducción del costo de recoger correo ya no es tan gravoso económicamente que la recepción de spam se asumen con *resignación*. El spam es un simple reflejo de la actual sociedad donde la publicidad inunda todos los rincones. Los contenidos del spam son variados y difíciles de clasificar, pero es cierto que los hay de carácter fraudulento e ilegal y sobre todo molesto. La naturaleza internacional de

---

21 Ver http://www.rediris.es/mail/abuso/ace.html

Internet y de las direcciones IP origen inhabilita cualquier medida legal para reducir el spam.

5.1.1. 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[22]. 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. ¿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 mientras las solicitudes comerciales 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. Para utilizar una imagen aproximada de lo que es el spam, para aquellos que lo toman simplemente como otra forma de comunicación directa equivaldría a tratar a un rinoceronte como si fuera un unicornio.

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.[23] 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 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. Como ha advertido AMADITZ[24] “(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.”

---

[22]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

[23]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/

[24] 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

Una segunda razón de carácter económico milita a favor del spam. En el caso de la publicidad por correo normal la tasa de conversión (conversión 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. En este sentido, constituye una práctica absolutamente inédita, “no existe otra forma de avisaje que se le pueda comparar”.

5.1.2. Métodos de captura de direcciones para spam

Las tácticas más populares para recoger direcciones de correo de forma masiva son: · **Compra de bases de datos** selectivas. Son bases de datos de direcciones de correo-e clasificadas por temáticas de interés. Estas bases de datos son creadas por responsables Web sin escrúpulos que recogen direcciones de los usuarios que pasan por su portal. ·

Listas Opt-In. Son servicios a los que cualquiera se puede suscribir de forma voluntaria. Muchas veces marcando la casilla que dice “No me envíe ofertas”, al final las recibe. Evidentemente la mayor parte de las listas optin son legales pero hay mucho engaño e incumplimiento de lo que ellos mismos dicen y además difícil de demostrarlo.

Páginas Web. Son robots capaces de hacer barridos en Internet o determinadas zonas para localizar miles de direcciones de correo-e. Los spammers los usan día y noche.

Servidores de correo-e. Son robots que extraen direcciones de correo de los servidores de correo, simulando una transacción SMTP y preguntando si tal usuario es o no correcto. Hacen barridos automáticos de nombres de usuario con diccionarios.

Virus y códigos maliciosos. Son virus que se propagan por correo-e consistiendo su actividad en capturar los datos de la libreta de direcciones del usuario *contaminado* y enviarlos determinadas direcciones para su procesamiento y almacenamiento.

Métodos de distribución de spam
Distribuir un mensaje a miles de destinatarios es una tarea sencilla y económica. Basta con conocer el diálogo de las transacciones SMTP (Simple Mail Transfer Protocol) descritas en el RFC822 (RFC2822). Los ingredientes para la distribución son:

Programa sencillo que reproduzca un diálogo SMP, colocando los campos Remite: y Destino: que le vengan en gana y falsificando algunas de las cabeceras de tránsito (*Received*:)

Base de datos de direcciones de correo a los que distribuirá el mensaje de spam ·

Máquina (Estafeta) con la que establecer el diálogo SMTP. En este caso puede ser: o Máquina local con un paquete de servidor de correo-e o Máquina remota a la que se accede por el puerto 25 (SMTP).

Entendiendo como spam todo mensaje de correo electrónico no solicitado Podríamos clasificar al spam en dos categorías en función del uso de recursos (máquina, CPU, disco, ancho de banda) por parte de terceros.

Spam *legal*: Uso de recursos propios. Es el spam procedente de Empresas distribuido desde sus propias máquinas dentro de sus campañas de marketing y

promoción. También el procedente de Proveedores de servicios Internet (ISPs) que es usado por usuarios o Empresas que no disponen de recursos propios de distribución masiva.

Spam *ilegal*: Uso de recursos ajenos. Es el spam que para su distribución se aprovecha de Estafetas ajenas mal configuradas openrelay[25]. Existe entre los spammers bases de datos de máquinas (IP) mal configuradas para poder ser usadas.

El spam ilegal es uno de los más extendidos y suele ser el que viene en idioma inglés. Generalmente procede de USA pero utilizan para su distribución máquinas open-relay de cualquier parte del mundo con el objeto de evitar la legislación de dicho país. El spam en idioma castellano suele ser spam legal procedente de ISPs o empresas. El protocolo SMTP que regula todas las transacciones de correo de Internet se creó allá por 1981 de forma insegura para ser usado por científicos sin pensar en ningún uso comercial. Ya existían listas de distribución (LISTSERV-1984) que eran usadas para distribuir información de uno a muchos. La explosión de Internet en 1994 a nivel social y comercial hizo que se "descubrieran" los agujeros de SMTP para ser utilizado como el mejor y mas barato mecanismos para distribuir y hacer llegar directamente a miles de buzones cualquier tipo de información. La gran explosión del spam empezó en 1995-1996 donde cualquier máquina con un servidor de correo podía ser usada por los indeseables spammers para distribuir su información. En esos años el spam que se recibía en el buzón era muy inferior al actual del 2003. El gran problema eran los ataques que sufría el puerto SMTP (25) para distribuir spam. Ya el Cendoj[26] en alguna oportunidad ha recibido estos ataques masivos de spam. En dicha época el servidor de correo mas extendido era Sendmail, el cual solucionó las deficiencias de SMTP con sus reglas de configuración y se empezaron a solucionar muchos de los problemas, los de servidores con otro tipo de sistema operativo llegaron mas tarde. Aún así estos problemas de configuración no están erradicados en el 100% de las máquinas de Internet por lo que siguen existiendo máquinas open-relay.

5.1.3. Efectos del spam

Algunos los efectos negativos y problemas del spam:

1 Inunda los **buzones** saturando la capacidad máxima de los mismos y por tanto provocando la pérdida de correo deseado y útil.

2 Reduce la **efectividad** del correo-e al ser molesto u ofensivo al receptor.

3 Afecta a los **recursos** de la Estafeta de correo-e ya que mientras está procesando spam ralentiza el procesamiento del correo normal.

4 Afecta al ancho de banda congestionando las **infraestructuras** de comunicaciones

5 Afecta el **tiempo** de los usuarios empleado en borrar, denunciar, filtrar etc. y al de los responsables del correo.

---

25 Estafeta open-relay: Son Servidores de correo mal configurados que permiten encaminar correo desde cualquier dirección IP. Esto permite un uso indebido de recursos de la empresa por parte de personas ajena a la misma. Estas Estafetas son las preferidas por los spammers para inyectar mensajes de spam y destinado a miles o millones de destinatarios.

26 Centro de Documentación Judicial de la Rama Judicial de Colombia, mas información en www.ramajudicial.gov.co

6 Afecta la **imagen** de la Empresa que distribuye spam. Por poner un ejemplo un servicio clásico en Internet como las News de Usenet está siendo bastante afectado en su funcionalidad por el incesante uso que se le está dando para distribuir spam a través de muchos de sus grupos. Otros ejemplos graves de efectos del spam en cualquier empresa son:

§ **Tamaño del mensaje**. La distribución masiva de spam incluyendo ficheros grandes puede perjudicar gravemente a las Estafetas de una empresa o inhabilitar el correo de algún usuario. De aquí la necesidad de limitar el tamaño del correo entrante.

§ **Direcciones falsificadas**. Este es un efecto difícil de explicar en pocas líneas. Básicamente consiste en atacar una Estafeta openrelay[27] (E1) para ser la distribuidora del correo. El truco está en que el mensaje de spam lleva como dirección de correo emisora la de cualquier dominio. La Estafeta de este dominio será la atacada. ¿cómo? Dicho dominio es quien recibirá los mensajes de error de las miles de direcciones inyectadas en la Estafeta (E1). Estos errores serán los producidos en las transacciones SMTP desde la máquina open-relay a los diferentes destinos. La máquina atacada (E2) recibirá miles de mensajes destinados a direcciones de su dominio con el agravante que la parte local de la dirección no existe generándose un nuevo error y una nueva transacción SMTP produciendo el colapso de los servidores de correo.

Todos estos problemas nos pueden llevar a pensar en la fragilidad del correo-e en Internet y la pérdida de confianza en este útil servicio. Si al spam habitual, se le añaden sus efectos colaterales mas allá de la simple recepción de correo no deseado, los virus y la generación mensajes y confusión producida por los Antivirus en las Estafetas, la falsificación de mensajes etc. podemos llegar a la conclusión que el Servicio de Correo electrónico en Internet es inútil. Actualmente los virus es el problema mas grave del correo-e pero éstos tienen sus patrones y por tanto son interceptables con los actuales Antivirus. El spam es un problema del correo-e por la dificultad de evitarlo.

Un problema colateral del incesante aumento del spam es la regulación legislativa que puede llegar a encubrir la regulación de otros aspectos de Internet. Es claro que la legislación en Internet ya comenzó y mucha de ella está relacionada con la protección de datos, el correo-e y el spam.

5.1.4. Medidas contra el spam

Qué es lo que se quiere solucionar:¿ el correo basura en los buzones de los usuarios? o ¿reducir el impacto en los servidores de correo y líneas de comunicaciones? O por el contrario se quiere combatir el spam en general por ser un tormento en la Internet.

En función de cuales sean nuestros objetivos, debemos enfocar las posibles alternativas al problema. No son iguales las soluciones o medidas a adoptar para una Empresa que para un Proveedor de servicios Internet que para una comunidad amplia como puede ser la Comunidad científica Colombiana o latinoamericana Alfa-Redi o mejor la mejor comunidad española RedIRIS. En función de cómo queremos reducir los efectos del spam podemos clasificar las soluciones en:

Precavidas: Medidas que colaboran a evitar recibir o distribuir spam en o desde Empresa o Proveedores. En este bloque se englobaría: eliminación del *tag html*

27 Ob cit

"malito:" en las páginas Web, Políticas de Uso Aceptable en Empresas y Proveedores, Formación, cumplimiento de la LOPD y registro de ficheros etc.

Reactivas: Medidas que se toman después que el correo (spam) haya llegado a los servidores y buzones. Son medidas del tipo Filtros de contenidos (Content-Filter) tanto para servidores como clientes de correo. Filtros como los existentes en nuestras cuentas oficiales suministradas por el cendoj[28] para evitar el acceso de éstos.

Proactivas: Medidas que se toman antes que el correo (spam) llegue a los servidores. Son medidas del tipo *listas negras* , denuncias y Legislación.

Es necesario dejar claro que no hay solución ni exacta ni infalible ni global, la aplicación de todas si reducirá el impacto del spam. Esto no implica que no se deban tomar medidas porque las que se tomen siempre reducirán en mayor o menor grado el impacto del spam. Las técnicas de los *spammers* cambian continuamente a medida que aparecen nuevas técnicas para evitarlo.

Estas medidas son necesarias para prevenir la captura de nuestras direcciones de correo. La distribución de spam sólo es posible si se dispone de muchas de estas direcciones. La captura de direcciones escaneando páginas Web es una técnica habitual para la distribución de spam. Existen numerosos programas de manejo sencillo y distribución pública que permiten este tipo de técnicas. Un diseño de páginas donde se tenga en cuenta evitar utilizar el *tag* **mailto:** será un primer paso para evitar capturar direcciones que acaben alimentando estas bases de datos y reducir el spam. La mejor alternativa al uso de estos *tag* es la implementación de formularios Web cuya información sea enviada por correo al buzón correspondiente para lectura.

Otra de las medidas preventivas que debería ser adoptada es la disponibilidad de un documento que defina la **Política de Uso Aceptable** del correo-e en la Empresa o en Proveedores. Básicamente este tipo de documentos deben definir los derechos y obligaciones del uso del servicio con recursos de la empresa o Proveedor. El uso del correo electrónico e Internet en las empresas ha abierto un nuevo capítulo en el debate sobre los límites de la privacidad y el control. Es claro que se minimizan los conflictos en una empresa por aspectos relacionados con el correo-e cuando las empresas disponen de Políticas de Uso sencillas, claras y conocidas por todos. En dicho documento la Empresa debería aceptar que las técnicas de spam no forma parte de su mecanismo de marketing y publicidad. Un tema muy importante a tener en cuenta es la labor de **formación** e **información** continua de los empleados en todos los aspectos relacionados con el correo: lo qué es, uso correcto, tipos de abuso, legislación relacionada y descripción del spam.

Evidentemente estas políticas de uso en un proveedor de servicios Internet (ISP) tendrían enfoques diferentes ya que no hay empleados sino usuarios/clientes que usarán los servicios. Los Servicios de los ISP son los que usan las empresas para distribuir spam por lo que deberían de disponer de una reglamentación contundente especificando claramente los tipos de abuso en el correo-e como la distribución masiva de correo así como sus penalizaciones. Este es un buen ejemplo de un extracto de la Política de Uso de Aceptable de un proveedor[29]:

---

[28] Centro de documentación Judicial del Consejo Superior de la Judicatura en Colombia. Mayor información www.ramajudicial.gov.co

[29] Tomado del trabajo denominado Evaluación de alternativas para reducir el spam, del profesor Jesús Sanz de las Heras (Coordinador del servicio de correo electrónico en la comunidad académica española, RedIRIS) Mayor ilustración en www.rediris.es

"Por esta razón, se entenderá que los clientes han infringido la política de usos aceptables de VERIO y el Contrato de servicios cuando los clientes realicen las siguientes acciones consideradas como prohibidas: ***Spamming*** *- Enviar correo no solicitado y/o mensajes comerciales no solicitados a través de Internet (llamado "spamming").*

No es solamente por el impacto negativo que pueda crear en el consumidor hacia VERIO, además puede sobrecargar la red de VERIO haciendo que el servicio que se ofrece al cliente no pueda ofrecerse en condiciones plenas de calidad. De la misma forma, el mantener una pasarela SMTP abierta está prohibido. Cuando una queja es recibida VERIO tiene la potestad de determinar si cumple o no las características que infringen las normas o determinan que se ha realizado Spamming."

Los ISP que ofrecen servicios de conectividad también deberían especificar en los contratos las condiciones de uso dejando claro que como responsables de las direcciones IP no se acepta la distribución de spam por sus líneas y por tanto cualquier denuncia recibida será canalizada convenientemente.

5.1.5. Regulando el spam.

La forma en que regulan las normas jurídicas según el sistema de precios sombra postulado por autores como POSNER[30]. 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.

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. Los precios constriñen nuestras posibilidades de viajar a la costa 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 reemplazados por plazas cercadas. Asimismo la arquitectura –o el **código** 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.

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

---

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

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.

5.1.6. Utilizando el derecho para regular el spam.

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[31]. 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. Según *Maza Gazmuri* 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 –es decir el receptor haya prestado su consentimiento sobre la recepción de correos- o bien exista una relación anterior entre el emisor y el receptor. La ventaja de este enfoque es evidente, por una parte reduce significativamente el número de correos enviados, y por otra, solo reciben correos quienes lo desean.

(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.

(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)

---

[31]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 NDOIBEROAMÉRICA . Editorial Temis S.A. 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

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 *enrutamiento* (routing) y el despliegue de información engañosa en la línea de asunto del correo electrónico. Ambas prácticas son utilizadas por spammers más avanzados para engañar a los servidores y a los usuarios sobre la fuente de los correos electrónicos.

(4) Utilización de bienes muebles sin autorización[32]. Cierta legislación basada en un nutrido contingente de casos resueltos por tribunales norteamericanos en los últimos años, 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 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 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. de los registros de opt-out, una de las principales críticas es que los mismos registros pueden ser utilizados para recolectar direcciones. En adición a lo anterior, un segundo problema –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.

La legitimidad de la 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[33].

---

[32]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

[33]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

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, sólo conocemos la ya referenciada española y el proyecto de ley colombiano. 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.

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

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 . 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

---

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.).

correo no deseado. 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 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.

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.

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 sancionatorias 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.

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. 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.

5.1.7 Cómo actuar frente al spam:

- No responder nunca un mensaje no solicitado. Lo único que hará es confirmar que su dirección está activa.
- No responda uno de estos mensajes con insultos y cosas por el estilo. Puede volverse en su contra.
- Quejarse al postmaster de la persona que realiza el spam.
- Configurar filtros o reglas de mensaje en el programa de correo para no recibir más mensajes de una dirección determinada.
- No dejar la dirección de mail en cualquier formulario o foro de Internet.

Si está recibiendo demasiado correo basura, tal vez lo mejor sea cambiar la dirección de correo.

6.2. Los Derechos Fundamentales Vulnerados

6.2.1 La sensibilidad del dato electrónico, la autodeterminación informática, el derecho a la intimidad y habeas data.

Actualmente, todos los individuos – voluntariamente - proporcionan sus datos personales a distintas instituciones públicas o privadas, por distintas razones. El apropiado tratamiento de los datos, permite convertirlos en información útil para el logro de determinados objetivos. Pero esos datos pueden amenazar la dignidad de los hombres por el uso arbitrario y malicioso de la informática. El peligro se concreta con la capacidad de almacenamiento en la memoria de los ordenadores, la celeridad de todo el proceso, el desarrollo de las disímiles técnicas reservadas para el manejo de volúmenes de información, etc.

El ordenador puede verificar los datos sobre un individuo introducidos en su memoria y cotejar la imagen real de los datos del individuo en cuestión. Todos esos datos deben ser protegidos contra el acceso de quienes no estén autorizados. Esta necesaria protección es un límite al manejo de la informática ante el temor de que pueda atentar la intimidad de los ciudadanos y que pueda restringir el ejercicio de sus derechos.

Una base de datos, esta compuesta por todo tipo de información aportados por las personas para determinados fines. Pero también existe una gran variedad de medios a través de los cuales se compila información de las personas sin su consentimiento, tal como sucede en algunos sitios de Internet que cruzan datos de las personas que las visitan y conforman un perfil del interesado.

La existencia de enormes bases de datos que contienen gran cantidad de información referida a las personas, es una consecuencia de la informática y sin la cual seria imposible su existencia.

Lo importante es la finalidad para el cual se usara la información allí almacenada para evitar que seamos discriminados debido a un uso desatinado de sus datos.

La cuestión es aun mas grave si especulamos que esas bases de datos pueden ser atacadas por crackers que son aquellos aficionados a la computación que obtienen accesos no autorizados a los sistemas de computación, robando o destruyendo datos, y que buscan información para si o para terceros.

La ambición para conseguir datos no es el mismo que para actualizarlos, rectificarlos, suprimirlos o modificarlos.

La doctrina especialista en el tema, se refiere al amparo debido a los ciudadanos contra la posible utilización por terceros de sus datos personales susceptibles de tratamiento automatizado para confeccionar una información que afecte a su entorno personal, social o profesional en los límites de su intimidad.

La protección de datos esta prevista por las innovadoras legislaciones mediante el derecho a la intimidad y su transmisión telemática cuando aparece una nueva relación entre datos y personas que necesitan ser protegidos mas allá de las normas referentes a la intimidad.

Lo primordial es que los datos no generen situaciones de segregación por cuestiones de salud, raza, ideas, costumbres y datos que pudieran llegar a limitar nuestras posibilidades.

Son base de datos privadas los datos que tienen regulados situaciones o circunstancias en que la persona se ve obligada a darlos o ponerlos en conocimiento de un tercero, debiendo impedir su difusión y respetar la voluntad de secreto sobre ellos, de su titular. A su vez, dentro de los privados encontramos los datos personales íntimos, que son aquellos que el individuo puede proteger su difusión frente a cualquiera y que, de acuerdo con un fin determinado, esta obligado a dar, salvo algunas excepciones. Estos

datos secretos son los denominados datos sensibles, definidos por la Constitución Nacional en su artículo 15 que en su tenor literal dice: "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer a actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas"

Y como datos personales que requieren una protección especial, tales como ideas políticas, creencias religiosas, salud física o mental, comportamiento sexual de los individuos y la autodeterminación informática. Este es el derecho conocido como habeas data, considerado hoy como uno de los más importantes derechos fundamentales, especialmente dado el desarrollo de la cibernética, la informática y la telemática y en general de la información y las comunicaciones[34] en la actualidad.

En forma errada el demandado constitucional alega que el derecho de habeas data sólo es viable para cuando se refiere a datos financieros, precisamente sobre el tópico el Dr. Nelson Remolina[35] en conferencia ofrecida en el Hotel Ambalá, en la ciudad de Ibagué, se refería que el habeas data se establece el manejo de cualquier dato sensible, de ahí el porque se torna viable una acción de tutela para cuando, v/gratia en un centro asistencial se le diagnostica a un paciente erradamente una enfermedad terminal y se publican sus datos. Compartimos la tesis del Dr. Remolina, porque no puede ser excluida en ninguna ley, la viabilidad de la acción de amparo para cuando se manejan datos diferentes a los financieros como los que usualmente manipulan la mayoría de las empresas que conservan bases de este tipo.

Podríamos decir que una de las mas frecuentes violaciones de los derechos humanos en el presente la constituyen las actuaciones de entidades particulares o públicas que tienen por objeto recopilar información confidencial o personal de los individuos, sin que el dato sea verificado, ni conocido por la persona afectada por el mismo o ilegalmente manipulado. Igualmente este manejo informático del dato impide la actualización y el olvido con que la persona está sujeta irredimiblemente a soportar la carga de su pasado o de un uso impropio de la información confidencial o de sus registros informáticos, para ser utilizada como medio de presión para alcanzar fines desleales o propósitos ilícitos.

Para una mayor ilustración analizaremos el término de Intimidad: según el diccionario Jurídico Espasa[36] es un derecho constitucionalmente reconocido y protegido, es objeto de tutela en la diversas ramas del ordenamiento jurídico, entre ellas la penal, según el Diccionario de la Academia de la Lengua Española, es la zona espiritual y reservada de un grupo de personas; esta definición coincide con la llamada "doctrina de la autodeterminación informativa", creada por el Tribunal Constitucional Alemán en un fallo del 15 de diciembre de 1983, donde se instituye que es titular de los datos personales la propia persona y debe ser requerido su consentimiento por parte de terceros que deseen almacenarlos, cederlos o publicarlos; el Diccionario Jurídico de Ossorio y Gallardo, define al derecho a la intimidad como el derecho que tienen las personas a que su vida intima sea respetada, que nadie se entrometa en la existencia ajena

---

34 Módulo sobre la Acción de Tutela. Escuela Judicial Rodrigo Lara Bonilla Pág. 46

35 Nelson Remolina Angarita. Abogado y especialista en Derecho Comercial de la Universidad de los Andes. Master en Leyes the London School of Economics and Political Sciences, con énfasis en derecho informático y económico (information Technology Law; Electronic Bancking Law; International Economic Law; International Trade Low). Director de Pregrado y profesor de la Facultad de Derecho de la Universidad de los Andes. Profesor de postgrados de las Facultades de Ingeniería y Administración de la Universidad de los Andes. Autor de los temas DATA PROTECTION E INFORMATICA EL DOCUMENTO ELECTRÓNICO y DATA PROTECTION Panorama nacional e internacional, publicado en el libro INTERNET COMERCIO ELECTRÓNICO & TELECOMUNICACIONES por la Universidad de los Andes en asocio con Legis. 2002

36 Diccionario Jurídico ESPASA. Espasa Siglo XXI. Edi.1998. Pág. 534

publicando retratos, divulgando secretos, difundiendo correspondencia, mortificando a otros en sus costumbres y perturbando de cualquier otro modo su intimidad.

Por su parte nuestra Corte Constitucional ya se ha referido al respecto sobre el derecho de la intimidad afirmando que: "Es un derecho entonces, personalísimo, según inspiración constitucional relativa a la dignidad humana, que debe ser tutelado cuando, por la acción de terceros, se produce una intromisión indebida en el ámbito personal o familiar del sujeto que conlleva la revelación de asuntos privados, el empleo de su imagen o de su nombre, o la perturbación de sus afectos o asuntos más particulares e íntimos relativos a su sexualidad o salud, con o sin divulgación en los medios de comunicación.

Se ha considerado doctrinariamente, que constituyen aspectos de la órbita privada, los asuntos circunscritos a las relaciones familiares de la persona, sus costumbres y prácticas sexuales, su salud, su domicilio, sus comunicaciones personales, los espacios limitados y legales para la utilización de datos a nivel informático, las creencias religiosas, los secretos profesionales y en general todo "comportamiento del sujeto que no es conocido por los extraños y que de ser conocido originaría críticas o desmejoraría la apreciación" que éstos tienen de aquel. [37]

El avance de este derecho no es reciente, ya que podemos remontarnos al año 1890 donde una publicación en el diario "Harward Law Review" salvaguardaba la propiedad de cada individuo sobre la propia privacidad, como el derecho de estar solo (*to be let alone*); pero en el siglo XX, el derecho a la intimidad adquiere un predominio especial ya que actualmente cubre un cúmulo de relaciones que el individuo mantiene sobre otros y que deben ser preservados como de su reserva personal. El derecho a la intimidad es el derecho de toda persona a que se le respete en su vida privada y familiar, y a evitar injerencias arbitrarias en la zona espiritual íntima y reservada de una persona.

El nuevo derecho a la intimidad posee una faz preventiva y una faz reparadora: preventiva por la facultad de conocer los datos personales que constan en registros automatizados, de exigir la rectificación, actualización y cancelación de la información; y reparadora por al posibilidad de resarcimiento de daños y perjuicios por parte de quien lo padece.

En nuestro derecho positivo, que posee un rango constitucional, la evolución de este derecho puede resumirse desde el "secreto" al "control" de la información que se tiene de uno mismo en los bancos de datos.

Este derecho a la intimidad se encuentra por estos días seriamente amenazado por la capacidad que posee tanto el sector público como el privado, de acumular gran cantidad de información sobre los individuos en forma digital. Con el desarrollo constante e ininterrumpido de la informática y las telecomunicaciones, se permite a tales entidades a manipular, alterar e intercambiar datos personales a gran velocidad y bajo costo. Así obtenemos sociedades altamente informatizadas en la que nuestras conductas y acciones son observadas y registradas y será imposible evitar la estigmatización y encasillamiento.

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

---

37 Sentencia SU 089 de 1995 del Dr. Jorge Arango Mejía. Sentencia citada por la Corte Constitucional en la T-411 de 13 de Septiembre de 1995. MP. Alejandro Martínez Caballero. 13 de Septiembre de 1995 S. U - 089 de 1995.

deben ser superados al momento de legislar sobre el tema o aplicar la legislación vigente.

En Colombia se tramita el proyecto de Ley No. 166[38] de 2003, el que " Por el cual se regulan las comunicaciones Vía Internet y mediante el uso de Fax " y en lo que se refiere al spam los legisladores consignaron el siguiente tipo: "Articulo 5. Queda prohibido el envío de comunicaciones publicitarias o promociónales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas". Igualmente se consagró una sanción dentro del parágrafo único del artículo 3°, que reza: "Parágrafo: Cuando por el mal uso del Internet o Fax se atente contra el patrimonio moral de las personas, se ponga en riesgo su vida o atente contra la seguridad y la estabilidad económica de las empresas, cualquiera que fuese su actividad, las autoridades competentes pueden, con fundamento en los libros de registro, aplicar a los responsables el rigor de las leyes preexistentes en materia civil, comercial o penal para castigar a dichas personas".

Esteremos atentos del futuro legislativo que atañe la atención de este Despacho en el día de hoy, por lo pronto resulta oportuno acotar que España es de los pocos estados que prohíbe absolutamente esta técnica gracias a dos leyes: LSSICE y LORTAD (la primera regularía la utilización del spam y la 2º el origen de los datos ilícitos sin autorización del propietario), que imponen en ambos casos severas sanciones a los responsables.

6.2.2. La vulneración de los derechos fundamentales

Alega el demandado JAIME LEONARDO TAPIAS GONZÁLEZ, que se le vulneró el derecho al debido proceso, en razón a la distancia no se practicaron las pruebas que se deberían hacer en la ciudad de Bogotá, y poder probar que no había vulnerado ningún derecho constitucional. Consideramos que dichas pruebas no eran necesarias precisamente por la confesión que el mismo ciudadano demandado hace en su libelo, porque reconoce que sí le ha enviado correspondencia no solicitada al actor del que conservaba la dirección de su correo electrónico en su base de datos.

Extrañamente no refiere el ciudadano TAPIAS tener vinculación alguna con su compañero de demanda, esto es, el señor HÉCTOR CEDIEL, pese a qué éste en el traslado de la demanda constitucional acepta haber contratado los servicios del señor TAPIAS GONZALEZ en el manejo de su e-marketing.

El señor TAPIAS GONZÁLEZ, en toda la extensión de su escrito de traslado, ha intentado derrumbar por todos los medios la competencia del Estrado, pero se despreocupó de desvirtuar los cargos; no aportó prueba alguna que nos indicará que los argumentos del actor no eran verdad, esto es, que desvirtuara los cargos de haber vulnerado los derechos constitucionales del señor SAMPER, como hubiera sido a guisa de ejemplo, que nos hubiera aportado algún contrato virtual que nos enseñara que contaba con la anuencia de éste para recibir mensajes comerciales, como también de manipular su dirección electrónica, lo que en el medio se llama, e-marketing de permiso, en donde se invita al presunto o potencial cliente a recibir los catálogos de productos o servicios ofertados virtualmente, de esta manera una vez contando con la aprobación

---

38 PROYECTO DE LEY No. 166-02 "Por el cual se regulan las comunicaciones Vía Internet y mediante el uso de Fax " Ponente ALVARO ASHTON GIRALDO Representante a la Cámara Departamento del Atlántico

del futuro cliente, se le remitiría hasta cuando el quiera recibir, los mensajes comerciales[39]. Así es como se debe manejar el mercado virtual, con principios éticos[40].

Aquella consigna que se agrega a todo spam de que si no quiere recibir más mensajes comerciales, sólo es remitir al postmaster su deseo de no querer recibirlos, es inconstitucional, puesto que se le pide una exclamación sobre un hecho no consentido.

Sabemos que el Spam es el envío indiscriminado de mails no solicitados. Si yo recibo un mail que no solicité de una persona que no conozco, y que al mismo tiempo es enviada a una cantidad de personas que tampoco lo solicitaron, eso es spam. No debería tener necesidad de enviar un mail para que me borren de una lista ya que no deberían agregar mi dirección a ninguna de ellas, puesto que no he autorizado a estar incluido, es ahí en donde se me vulnera mi derecho constitucional y continúa la vulneración cuando comienzan a comercializar mi dirección electrónica, que tampoco he autorizado. Esta advertencia sólo se torna viable si el titular de la cuenta de correo electrónico ha autorizado recibir dichos mensajes, como cuando aceptamos recibir noticias o catálogos al cargar un software en nuestros equipos que ha sido bajado de la Internet.

Además, la mayoría de las veces, al responder el mail pidiendo ser removidos de la lista, lo único que estamos haciendo es confirmar que nuestra dirección existe, con lo cual, en lugar de dejar de recibir mensajes, comenzamos a recibir más.

Recibir spam, es como cuando encuentro a un mismo vendedor golpeando insistentemente en mi casa, para ofertarme sus productos que vende, de los cuales no necesito, yo le replico no quiero nada suyo y le suplico a su vez no insistir ya que no me interesa su genero de productos. Nuevamente el mismo señor u otro personaje, me vuelven a ofrecer los mismos productos, los que no me interesan.

El Habeas Data brinda el derecho a toda persona de conocer qué datos propios han sido incluidos en registros y bancos de datos o en registros privados, destinados a proveer de informes, para pedir su supresión, rectificación, confidencialidad o actualización en caso de falsedad o discriminación.

Los riesgos a los cuáles esta expuesta la vida privada de las personas en la sociedad de la información, en particular, aquellos derivados del tratamiento de datos personales a consecuencia de la utilización de las nuevas tecnologías de la información y de la comunicación, nos hacen cuestionar cual debe ser el rol del derecho ante la referida problemática.

En relación con el derecho a la intimidad, este hace referencia al ámbito personalísimo de cada individuo o familia, es decir, a aquellos fenómenos, comportamientos, datos y situaciones que normalmente están sustraídos a la injerencia o al conocimiento de extraños. Lo íntimo, lo realmente privado y personalísimo de las personas es, como lo ha señalado en múltiples oportunidades la Corte, un derecho fundamental del ser humano, y debe mantener esa condición, es decir, pertenecer a una esfera o a un ámbito reservado, no conocido, no sabido, no promulgado, a menos que los hechos o circunstancias relevantes concernientes a dicha intimidad sean conocidos por terceros por voluntad del titular del derecho a por que han trascendido al dominio de la opinión

---

[39] Mayor ilustración en www.comovender.com

[40] Mayor ilustración en www.ispo.cec.be/Ecommerce/legal.html#legal

pública.

El derecho a la información expresa la propensión innata del hombre hacia el conocimiento de los seres humanos con los cuales se interrelaciona y de su entorno físico, social, cultural y económico, lo cual le permite reflexionar, razonar sobre la realidad, adquirir experiencias, e incluso transmitir a terceros la información y el conocimiento recibidos.

La Libertad Informática o Autodeterminación Informativa, ha sido denominada por la doctrina española y colombiana[41] como "un nuevo derecho fundamental que tiene por objeto garantizar la facultad de las personas, para conocer y acceder a las informaciones que les conciernen, archivadas en bancos de datos y controlar su calidad, lo que implica la posibilidad de corregir o cancelar datos indebidamente procesados y disponer sobre su transmisión". Esta facultad, es lo que se conoce como Habeas Data que constituye, en suma, un cauce procesal para salvaguardar la libertad de la persona en la esfera informática.

La Libertad Informática forma parte del núcleo de derechos denominados de tercera generación, debido a que el derecho a la intimidad adquiere una nueva dimensión al verse amenazado por el uso abusivo de la informática. El mismo, bajo la forma de libertad informática, aúna la noción clásica de los derechos de primera generación, la libertad, en cuanto define las posibilidades reales de autonomía y de participación en la sociedad contemporánea, que pueden verse amenazadas por el mal uso que se haga de determinados datos personales; la igualdad, valor guía de los derechos de segunda generación, en cuanto en informática se concibe como un instrumento de control que puede introducir asimetrías entre quien controla ese poder y quienes no tiene acceso a él. A éstos dos valores han de sumársele al hablar de derechos de tercera generación, el de la solidaridad ya que éstos derechos tienen una incidencia universal en la vida de los hombres, y con ella se apunta a garantizar su pleno disfrute, mediante un esfuerzo no egoísta de toda la comunidad.

En el art. 20 de la Constitución Política se garantiza a toda persona la libertad de expresar y difundir sus pensamientos y opiniones, la de informar y recibir información veraz e imparcial, es decir, se trata de una libertad que opera en doble vía, porque de un lado se reconoce la facultad de la libre expresión y difusión de las ideas, conocimientos, juicios u opiniones y de otro se proclama el derecho de acceder o recepcionar una información ajustada a la verdad objetiva y desprovista de toda deformación.

En corolario de lo anterior, el Estrado tutelará los derechos de habeas data, autodeterminación informática y el de intimidad al ciudadano JUAN CARLOS SAMPER POSADA, por habérsele violado en las circunstancias que arriba se anotaron.

Por lo anteriormente expuesto, el Juzgado Segundo Promiscuo Municipal de Rovira Tolima, administrando Justicia en nombre de la República de Colombia y por autoridad de la Ley,

---

41 Entre otras sentencia del CONSEJO DE ESTADO SALA DE LO CONTENCIOSO ADMINISTRATIVO SECCIÓN TERCERA Consejera ponente: MARIA ELENA GIRALDO GÓMEZ Bogotá D. C., treinta y uno (31) de octubre de dos mil uno (2001) Radicación número: 25000-23-24-000-2001-1338-01(AC-1529) Actor: Amparo Barajas García Referencia: Acción de Tutela.
Y de la Corte Constitucional las siguientes, entre otras: T-157/94, T-164/94, T-094/95, T-096A/95, T-097/95, T-199/95)

F A L L A

PRIMERO: TUTELAR como en efecto se hace los derechos a: HABEAS DATA, AUTODETERMINACIÓN INFORMÁTICA y a la INTIMIDAD, del ciudadano JUAN CARLOS SAMPER POSADA.

SEGUNDO: ORDENAR a los señores JAIME LEONARDO TAPIAS GONZALEZ representante de la firma VIRTUAL CARD y HÉCTOR CEDIEL, una vez en firme esta providencia no remitir mas correo no solicitado (spam o ace) al señor JUAN CARLOS SAMPER POSADA a su cuenta de correo electrónico jcsamper@network.com y todos los demás correos creados bajo el nombre de dominio i-network.com.

TERCERO: ORDENAR a los señores JAIME LEONARDO TAPIAS GONZALEZ y HÉCTOR CEDIEL una vez en firme esta decisión, borrar la dirección de correo electrónico jcsamper@network.com y todos los demás correos creados bajo el nombre de dominio i-network.com, cuyo titular es el ciudadano JUAN CARLOS SAMPER POSADA, de sus respectivas bases de datos para el manejo de e-marketing en sus empresas.

CUARTO: Se procede a notificar a los demandados en sus corroeos electrónicos **(jtapia@virtualcard.d2g.co; jaime@virtualcard.dns2go.com y hcediel@virtualcard.d2g.com)** surtiéndose la fórmula señalada en el artículo 29 de la Ley 794 de 2003, que modificó el artículo 315 del Código de Procedimiento Civil. El presente documento electrónico está amparado en los preceptos de los artículos 6°,7° y 8° de la Ley 527/99 que se refiere al mensaje de datos.

QUINTO : Contra la presente decisión procede el recurso de impugnación consagrado en el art. 31 Decreto 2591 de noviembre 19 de 1991.

COPIESE, NOTIFÍQUESE Y CÚMPLASE

ALEXÁNDER DÍAZ GARCÍA

Juez