Case note **Colombia**

Case name. **Juan Carlos Samper Posada v Jaime Tapias, Hector Cediel and others**

Case No. **Decisión 73-624-40-89-002-2003-053-00**

Name and level of court **Municipal Court of Rovira, Tolima**

Member of court **Alexander Díaz García**

Date of verdict **21 July 2003**

Lawyer present **Alvaro Ramírez Bonilla (lawyer for Juan Carlos Samper)**

Available in electronic format: http://www.alfa-redi.org/upload/revista/80403--0-7-diaz082003.pdf; http://derechopublico.udenar.edu.co/S-2107_2003(Data).htm

Facts (as described by the attorney for the plaintiff)

Mr Samper owns the e-mail jcsamper@i-network.com and all other mails created in the i-network.com domain. Mr Tapias is a person who acts commercially as Virtual Card, that offers mailing, multimedia, databases, electronic newsletters and e-business consultancy services.

On July 21, 2002 Mr Samper received the first unsolicited e-mail from Virtual Card. He answered this e-mail, requesting to be removed from Virtual Card's mailing list, taking into account he had not signed up to any mailing list. Mr Tapias responded on the same day to Mr Samper as follows:

1. That Mr Samper was not in Virtual Card's mailing list.
2. That marketing techniques allow businessmen to look for customers through all means of communications, including the internet.
3. That he had no knowledge of any legislation regarding privacy that could in any way limit the activity of his company.

On July 22, 2002 Mr Samper sent a further request to be removed from the mailing list and argued that the problem was not the marketing strategy itself, but that customers were neither informed, nor previously requested an authorization to be included in mailing lists. Even though Mr Tapias, in his e-mail dated July 21,2002 assured Mr Samper that he had been removed from Virtual Card's mailing list, on September 2, 2002, he received a new e-mail from Virtual Card, reminding of the benefits of marketing through e-mails. On September 3, 2002, Mr Samper sent two new e-mails to Virtual Card insisting in the removal of his name from the mailing list and stating he had already tried to be removed from the list in every possible way.

One month later, on October 3, 2003, Mr Samper received a new e-mail from Hector Cediel and Consuelo Moreno informing him of the strategic alliance between Virtual Card, Okson Group, and Hector Cediel and requesting authorization to send marketing promotions to his e-mail address. Mr Samper replied on the same day, firmly requesting once again to be removed from the list. On October 5, 2002, Mr Samper received an e-mail from Time Seminarios, Virtual Card's client. Again, Mr Samper requested to be removed from the mailing list. On the same day, Time Seminarios answered his request by stating he had been removed from the mailing list. The efforts mentioned above to be removed from the list failed. On October 18, 2002, Mr Samper received an e-mail from Corporación Innovar, another client of Virtual Card.

On October 19, 2002, Mr Tapias, sent a new e-mail to Mr Samper in which he affirmed he knew Mr Samper disliked his working methods, and stated that the data bank in which Mr Samper was included would not be used anymore after November 2002. In addition to the above, Mr Tapias said he thought it was time to change the working method in which it was necessary to wait for authorization from clients, whom he knew he would never answer due to the problems with spam and opt in junk e-mail. The e-mail concluded with the following statement, "Mr. Samper, I don't mean to make you feel better but I receive daily more than 150 junk, porn, virus and publicity mails".

For a couple of months it seemed that Virtual Card had finally kept its word. However, on December 2, 2002, MrSamper received an e-mail from Lamy, Virtual Card's client. Finally, on December 27, 2003, Héctor Cediel, who identified himself as the person in charge of the data bank, sent an e-mail to Mr Samper. In conclusion, the defendants and their clients sent at least eight e-mails to Mr Samper, while the latter has sent them at least seven e-mails requesting to be removed from Virtual Card's mailing list.

Judicial proceedings

This lawsuit was filed by Juan Carlos Samper before the Municipal Courts by means of an e-mail adiazg@cendoj.ramajudicial.gov.co in compliance with the applicable regulation that sets forth that courts may use the internet and new technologies in order to solve and carry out proceedings. The plaintiff argued the defendant breached his fundamental rights to intimacy and habeas data, set forth in the Colombian Constitution. By writ of July 8,2003 the lawsuit was admitted and served to the defendant Jaime Tapias, Hector Cediel and others by e-mail. The defendants were given a term of three days in order to file their writ of defence in compliance with section 12 of Law 794 of 2003 and the Colombian Civil Procedure of Code. The proceeding was assigned to the Municipal Court of Rovira, Tolima.[1]

Considerations by the court

■ Venue of the court

The defendants argued that the Municipal Court of Rovira is not competent to carry out this proceeding taking into account the facts occurred in the city of Bogotá, and that the parties reside in Bogotá. The court however considered that the defendant has not understood that all behaviour based on information technology has a virtual component, and may not be uniquely limited to the material venue. The court expressed its surprised that a person somewhat familiar with the new technologies should argue that the venue may only be determined by the territorial element, taking into consideration the virtual element of information technologies.

Regarding this matter, the Council of State affirmed that the place where the violation or the threat to the rights of a person takes place is not only the place where the action occurs, but also the place where the effects of the action (or omission) has an effect. Even though the Council of State did not mention virtual effects, it is also true that the legal effects of the inappropriate use of new technologies have had an effect in the virtual domicile of the plaintiff. The fact that there is no regulation on this subject is not enough to conclude that the Municipal Court of Rovira is not the appropriate venue to solve this particular case.

The court considered that taking into consideration the characteristics of the new technologies and the services offered, the legal effects of the use of such technologies, as well as their venue, may not be materially limited to a physical and formal venue. Moreover the Colombian Statute of the Administration of Justice contemplates the use of the new technologies in the service of justice. Section 95 sets forth that Courts and judicial corporations are allowed to use any electronic or telematic method for the fulfillment of its functions. Section 95 of the Colombian Statute of the Administration of Justice (Law 270 of 1996) sets forth as follows:

"Los juzgados, tribunales y corporaciones judiciales podrán utilizar cualesquier medios técnicos, electrónicos, informáticos y telemáticos para el cumplimiento de sus funciones. Los documentos emitidos por los citados medios, cualquiera que sea su soporte, gozarán de la 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. Los procesos que se tramitan 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 contengan en los términos que establezca la ley"	"Judges, courts and other judicial corporations are allowed to use any technical, electronic, and telematic means in order to accomplish their duties. Every document issued by the mentioned means, whatever its support should be, will be considered as valid as an original document, as long as its authenticity, integrity and the fulfillment of procedural law´s requirements are guaranteed. Every procedure handled with technical supports, will guarantee the identification and the authorities´ jurisdictional duty, as the confidentiality, privacy and security of the personal data included, according to the terms set forth by the law"

[1] Rovira is a town in the region of Tolima. However, the events took place in Bogotá, capital of Colombia.

It also adds that the documents issued by such methods are as valid and efficient as an original document as long as its originality, authenticity and integrity are guaranteed, and that the procedural requirements set forth by the applicable regulations are met. The regulation also sets forth that all proceedings carried out based on electronic communications will guarantee the confidentiality, privacy and security of the parties involved and the matter under discussion.

The venue for Constitutional Judges comprises all the national territory and the applicable regulation does not exclude this court's venue in the cyberspace, taking into account the facts under discussion took place in cyberspace. Even though the defendants are trying to reduce the venue to a physical space, the court understands that a fundamental element of the matter being discussed is that it takes place in the virtual domicile of Mr Samper. In addition to this, Colombian Law 794 of 2003, Section 29 has granted the relevant legal protected to the virtual domicile and obliges businessmen to register their e-mails and sites before the Chamber of Commerce.

In Colombia, there are few persons who have studied and analyzed the issues regarding the legal venue, however, this issues has been studied more extensively in other Latin American countries. Among others, Professor Julio Nuñez Ponce has affirmed that the virtual domicile is directly related to the issues of venue and competence in the internet. Julio Núñez Ponce has published his opinion regarding the Peruvian regulation in light of the treatment that should be given to the virtual domicile regarding its legal, commercial and tax effects. According to Julio Núñez Ponce, the virtual domicile is the place where a citizen performs different virtual activities that may be carried out in any part of the world. Therefore the virtual domicile is not equivalent to the physical domicile.

Therefore, the virtual domicile of a person is made up by his e-mail or site address, which is the permanent residence of the person in the world wide web. For example, those corporations or businessmen who have a registered homepage or e-mail address before the Chamber of Commerce may be notified of judicial decrees and notices by means of their virtual domicile. In addition to the above, the Court concluded that, taking into account the Colombian government has enacted laws 527 of 1999 and 794 of 2003, regarding e-commerce, data protection and the use of new technologies, there is a clear legal support regarding the virtual domicile and the venue of the Court in this case.

In light of the above, the following statement of David R Johnson and David G Post, regarding absence of territorial boundaries in the Internet seems appropriate:

> "The Cyberspace has no territorially-based boundaries, because the cost and speed of message transmission on the Net is almost entirely independent of physical location: Messages can be transmitted from any physical location to any other location without degradation, decay, or substantial delay, and without any physical cues or barriers that might otherwise keep certain geographically remote places and people separate from one another. The Net enables transactions between people who do not know, and in many cases cannot know, the physical location of the other party. Location remains vitally important, but only location within a virtual space consisting of the "addresses" of the machines between which messages and information are routed".[2]

■ Electronic Signature

The defendant has argued that the documents issued by the court based on electronic means are not valid, in the understanding that the signature of the court is not supported or certified by any certification entity, as regulated by the applicable regulation. Nonetheless, it is important to differentiate the electronic signature from the digital signature. According to Professor Rodolfo P. Ragioni, the digital signature is made up by the data expressed in a digital encrypted format and used to identify the content and person executing a digital document. The electronic signature instead is made up by the electronic data that identifies other electronic data, but that does not meet the criteria necessary to be considered a digital signature.[3]

In light of the above, seems that the defendant has misunderstood Law 527 of 1999 regarding the validity of an e-mail. According to Section 6 of the law:

[2] David R Johnson and David G Post, in *"Law and Borders – The Rise of Law in Cyberspace"* 48 Stanford Law Review 1367 (1996) available in electronic format at http://www.cli.org/X0025_LBFIN.html.
[3] Rodolfo P. Ragoni, *E-money, la importancia de definir el medio de pago en el e-commerce*, (Prentice-Hall, Buenos Aires, 2001) page 242.

"Artículo 6°. Escrito. 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. Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas prevén consecuencias en el caso de que la información no conste por escrito."	"Article 6th. Written. Whenever any regulation requires the information to be in writing, such requirement will be satisfied by a data message; if the information such message contains is accessible for its later consultation. The provisions in this article will apply both, if the requirement established in any regulation constitutes an obligation, and if the regulations anticipate consequences in case the information is not in writing."

In those cases when the regulation requires that the information be sent in writing, an e-mail will suffice, if the e-mail is accessible to the parties for further consultation.

In addition to the above, the law only sets forth the requirement for a digital signature in certain circumstances, and the consequences of its absence, and that, in those cases when the digital signature is not required, the law sets forth the requirements in order to assure the content of the message is the original one. This court in all communications sent during the proceeding has met the requirements set forth by law. The communications have not included a digital signature because the courts still do not have a registered certified digital signature.

■ Solution of the problem

The court considers that the lawsuit proceed on the understanding that the plaintiff is currently defenseless. Accordingly, the Colombian Constitution sets forth that those persons who are in state of defenselessness have the right to file a lawsuit for the protection of their constitution fundamental rights. The defenselessness is contended against the person who, by means of an action or an omission, breaches the fundamental right of another person and thus leaves him defenseless. In addition to this, the plaintiff in this particular case has proved he repeatedly requested the defendants to bring their behavior to an end and delete his name from their databases. Clearly, the means used by the defendant have the capacity to breach the plaintiff's rights even after he had repeatedly requested to be removed from the unsolicited mailing list. Nonetheless, the fact that the plaintiff continued receiving messages even after he had requested to be removed form the mailing list, prove that he was defenseless before the defendants and their behaviour.

■ Rights breached

■ Means used: spam

The attorney of the plaintiff argues that by means of spam the defendants breached the plaintiff's rights of habeas data, informative self- determination, and intimacy. The court considers it necessary to further explain spam before analyzing the breach of the plaintiff's rights. According to Professor Iñigo de la Maza Gazmuri the word "spam" comes from the canned spiced ham produced by Hormel Foods since 1926. Taking into account this spiced ham did not need refrigeration, it was widely used during World War II. Nonetheless, according to different studies, the expression "spam" was first related to electronic communications in the 1980s, when a person involved in a MUSH (a type of MUD, where users can create things that remain for other users to see and use once the user has left) created an image that repeatedly typed the word Spam and interrupted others by interfering their possibility to participate in the MUD.

It is very probable that the creator of this macro was inspired in a sketch realized by the Monty Python Flying Circus in which the word spam was used repeatedly in the menu. Nowadays, spam is used to describe those unsolicited e-mails that are sent in massive volumes. However, the expression spam is also used with regards to all those unsolicited communications, not necessarily e-mails.

The sending of unsolicited e-mails generates additional cost for internet users and Internet service providers. In addition to this, spam has no physical territorial boundaries that make no difference between rich or poor, or advanced or non-advanced countries or persons. A practice like spam had never been seen

before in the history of humanity. Spam does not have a generally accepted definition. Nonetheless, the two most accepted definitions for Spam are: (i) unsolicited commercial e-mail (UCE); and (ii) unsolicited bulk e-mail (UBE). To define spam as unsolicited mail is not enough, taking into account that in order to enact a regulation to prevent spam, the fact that it is unsolicited or solicited is just one part of the problem. The main issue is to define when the sending of unsolicited e-mail is legal and when it is not. Once this issue is solved, then it will be possible to set forth a regulation in order to prevent and fight against spam.

The common elements of the definitions of spam is that is unsolicited by the recipient. Generally, e-mail is unsolicited when the sender and the recipient have no previous relation and the recipient has not consented to the sending of the message. E-mails may also be unsolicited when a party has tried to stop their sending and has obtained no result. However, in order to be spam, it also needs to be commercial and it also depends on the amounts sent. Even though the definition for commercial varies in many legislations throughout the world, usually something is commercial when it promotes goods and services.[4]

Regarding the amounts sent, there are many doubts regarding this issue. It may be one message that is sent massively or it may be different but very similar messages sent massively. However, there is a doubt on how many messages or times the message needs to be sent in order to be massive. Regulators need to define it if regulation should entail a fixed amount or if it should be open and decided in each case. However, and once issues like the commercial and massive elements are defined, regulators have to decide between UCE or UBE. Even though there are arguments in favor of both definitions, it is our understanding that UBE may be a better choice. This, taking into consideration UBE does not limit the content of the e-mails considered as spam to a commercial content. Spam is a strong business that invades our e-mail inboxes. The improvement of the internet access has increased the volume of spam for both the sender and the recipient. Spam is a reflection of the actual society where publicity invades everything. The contents of spam vary and are difficult to classify, however it is true that there are some, which are illegal and rigged.

Differences between spam and other unsolicited e-mails

It is evident that the sending of unsolicited publicity as a marketing mechanism is a direct phenomenon that helps improve and increase the use of the internet and spam. Daily, houses and apartments are invaded with letters and pamphlets that offer services, which have not been requested. Likewise, it is normal to receive undesired calls over the telephone offering certain products and other services. Why not treat these like spam? There are many answers. Before examining them with more caution, a general approximation would be that while the unsolicited commercial advertisements have been used for many years, they had never threatened the viability of an entire communication network.

The economics of spam

The advantage of direct marketing mechanisms is that they allow the sender to send information to consumers directly, contrary to other mechanisms such as television or street advertisement. However, direct marketing mechanisms are expensive. For example the sending of publicity through postal mail implies that the sender has to pay for all mailing expenses. However, in when using spam, the costs are minimum and there is direct customer and consumer approach. The cost for sending one more e-mail is nonexistent; therefore, the sender will encounter no problem in sending as many e-mails as possible. The insignificant costs of sending an e-mail justifies the sending of massive e-mails, since the sender will increase the possibility of getting more clients depending on the quantity of e-mails sent. The sending of 10,000,000 e-mails provides results that are more economically reasonable.

Another economic reason for which spam is justified is the following: in the case of normal mail publicity the conversion ratio is between 0.5-2 per cent, in the case of marketing via e-mail this ratio increases between 5-15 per cent. In a few words the issuing of undesired commercial e-mails in a massive way is less expensive and has better results.

Methods for capturing e-mail addresses to send spam

The most useful ways in order to collect e-mail addresses are:

[4] Please see Section 2 f) of Directive 2000/31/EC of the Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (L178/1 OJ 17.7.2000).

- **Buying databases.** These databases are composed by e-mail addresses classified under the interest matter.
- **Opt-In lists.** These are services to which anyone could subscribe by their own will. Most of the time clicking on the "Do not send me more offers" option does not work and messages will still be sent.
- **Web Pages.** These are capable of searching e-mail addresses throughout the internet and people undertake sweepings in various places in order to obtain massive e-mail addresses. Spammers use this method constantly.
- **E-mail Servers.** These robots extract e-mail addresses from the mail servers, imitating a SMTP transaction and questioning if the user is or not correct. These robots do automatic sweeps of user names with dictionaries.
- **Viruses and Codes.** These viruses spread through e-mails searching and capturing information.

Distribution methods of spam

The distribution of a spam e-mail to a thousand destinies is not a hard or expensive task. The only thing, which is necessary, is to know the dialogue of the SMTP (Simple Mail Transfer Protocol) described in RFC2822. The important elements for distribution are:

- Simple software, which can reproduce an SMP dialogue.
- Data Base of addresses to which the e-mails will be sent.
- Machine that serves to establish the SMTP dialogue.

Cataloging of spam

After defining spam, as any not desired e-mail, spam can be classified under two categories:

- **Legal Spam:** The spam delivered by corporations from their own machines and own marketing campaigns or the one that is sent by ISPs on behalf of users of corporations that do not have their own massive distribution mechanisms.
- **Illegal Spam:** The spam sent from wrongly configured open relay servers. The illegal spam is usually written in the English language.

Effects of spam

Some negative effects and problems of spam include:

- It overwhelms inboxes filling the maximum capacity of the inboxes, therefore provoking the loss of useful and important e-mails.
- Reduces the effectiveness of the e-mail.
- Affects the resources of the servers and the ISP.
- Affects broadband capacity.
- Users waste time erasing and cleaning their mails.
- It may be used to introduce virus to computers.

Measures against spam

What is there to be solved? The trash mail in the user inboxes? Or reduce the impact on mail servers and the communications network? Or in general spam wants to be destroyed since it is a problem for the internet.

The solutions to stop spam are classified as follows:

- **Cautious:** Measures that prevent receiving and distributing spam from or in the corporations or ISPs. This would entail the deletion of the tag html "mailto" on Web pages, Guidelines and policies for the correct use of mails, and other preventative measures.
- **Reactive:** Measures taken after spam has arrived to the servers and e-mail boxes. These measures may be content-Filter type for servers as well as e-mail clients.
- **Proactive:** Measures taken before spam arrives to the servers. These measures are described as black lists.

None of these measures will bring spam to an end, however they will reduce it. This does not suggest that one must not take these measures, since every time a measure is taken spam is reduced. The spammer techniques change constantly as well as all the measures to prevent and stop it.

Controlling spam by means of law

Actually there are many laws that control the treatment of personal data, and spam throughout

many countries in the world. According to Iñigo de la Maza Gazmuri, the Director Programa de Derecho y Tecnologías de al Información at Universidad Diego Portales, there are five options to be considered in order to control spam:

1. The prohibitive option consists in proscribing every type of commercial publicity. A more accepted version consists in banning the sending of commercial publicity via e-mail when the recipient has not authorized it.
2. The cataloguing of spam as spam consists in describing fully the subject of the e-mail in the "Subject" thus permitting recipients to identify the content of the messages.
3. The anti-fraud option consists in penalizing those massive e-mails when they use the name of a third person without its authorization, or they hide the real origin of the e-mail or they have false information in their subject.
4. The trespass to chattels option is based on legislation previously used in the United States in order to confront spam and is based in the case of *CompuServe Incorporated, v Cyber Promotions, Inc. and Sanford Wallace*,[5] in which Compuserve argued that the massive e-mails sent by Cyberpromotions physically damaged their equipment.
5. The opt-out option. The legislations with the opt-out option allow the sending of unsolicited massive e-mails unless the receipient has requested to be removed from the mailing list by any means.

How to act toward spam

Σ

- Never answer an unsolicited message. The only thing you will do is confirm that your e-mail account is active.
- Do not answer one of these messages with verbal abuse. This could turn against you.
- Complain to the postmaster of the person who is sending spam.
- Configure filters and message rules in the mail program so you would not receive more e-mails from the determined address.
- Do not leave the e-mail address in any forum in the internet
- If you are receiving numerous spam messages, you must take to consideration changing your e-mail address to a new one.

■ Violation of fundamental rights

Presently, many individuals voluntarily give their personal data to public and private institutions. Some of the institutions use this information in a useful way. However, others use it for threatening reasons. The danger is basically placed in the fact that the computers have such big memories in that they can save all data and addresses as well as extremely high volumes of information. Computers may also verify the data of an individual once the information is introduced in the memory and compare it with the data of another individual. All this information must be protected from those who do not have authorization. This protection is necessary in order to protect the intimacy and the personal information of the citizens.

A database is composed of various kinds of information from different persons acquired for different reasons. There are also a variety of sources by which information from citizens is compiled without their consent. The existence of large databases that contain information of individuals is an informative consequence of the modern world. However, the importance is the final purpose for the use of the information that is stored. This fact is more severe if we hypothesize that crackers could attack the databases and obtain unauthorized access and steal or destroy information. The ambition to find information is not the same as to actualize, rectify, modify and suppress them.

Legislation therefore seeks to protect personal information by means of the right of intimacy. However, the regulation also seeks to avoid the creation of any difference among the citizens based on private personal information. Even though some personal information is public due to the fact that it is necessary for the day-to-day life of citizens (identification number) other information belongs to their intimacy and in no way are they obliged to disclose it. The Colombian Constitution catalogues such information as sensitive data that require a special protection because such information is fundamental to every human being. Such sensitive data needs to be handled with the utmost care by both public and private entities. Constantly, the management of this information is not careful enough and citizens are exposed to an illegal disclosure of their information or to their breach to their right of intimacy regarding personal sensitive information.

Based on the right of intimacy, Colombian citizens may:

All this information must be protected from those who do not have authorization. This protection is necessary in order to protect the intimacy and the personal information of the citizens

[5] United States District Court for the Southern District of Ohio, Eastern Division, 962 F. Supp. 1015; 1997 U.S. Dist. LEXIS 1997; 25 Media L. Rep. 1545, Case No. C2-96-1070.

1. be informed of their personal information contained in data bases and demand the information is updated or corrected when wrongly registered as well as cancelled when not applicable; and
2. demand the indemnification of damages for the breach of their right to intimacy.

The right to intimacy is constantly threatened by the information society and the new technologies that may have access to personal information by means that were never considered before. Regulators need to consider the development of technologies and communications in order to enact regulations that will effectively protect citizens right to their intimacy and the use of their personal data.

■ The breach of fundamental rights

The court considers that the behavior of the defendants constituted a breach of the fundamental rights of intimacy of Mr Samper. Clearly, Mr Samper requested to be deleted from the mailing list several times, instruction that was not followed by the defendants. Therefore, Mr Samper's right to modify or cancel his personal information form public or private data bases as an expression of the right to intimacy was breached.

Decision

The judge ordered Jaime Leonardo Tapias and Héctor Cediel, not to send any more spam to Juan Carlos Samper´s e-mail address (jcsamper@network.com). Additionally, he ordered them to erase his details from their e-marketing management database, the e-mail address and any other mail addresses created under the domain name i-network.com.

Translation by Ms Valeria Frigeri and Manuel F. Quinche

http://www.brigardurrutia.com.co