



LEGAL REPORT

ELECTRONIC PRIVACY EXPECTATIONS IN THE WORKPLACE UNDER VENEZUELAN LAW

Francisco M. Castillo G.

Partner

Patrick Petzall K.

Consultant

Hoet Pelaez Castillo & Duque

INTRODUCTION

As corporations rely more on ubiquitous information technologies (computers, intranets, the internet and, most importantly, electronic mail) and make those tools readily available to their employees in the workplace, the issue of control over these information tools becomes poignant as employees utilize them for personal ends, both for the storage of personal data and to engage in private communications. However, these instruments, comprising both hardware and software are the property of the employer and, as such, the employer seeks to restrict their non-official use, to control the flow of sensitive corporate information and to protect the security of its assets.

This conflict between privacy and ownership that has always loomed within the workplace has resurfaced in Venezuela with added vigour due to

the drastic changes coursing through the Venezuelan legal framework during the last two years, starting from the enactment of the 2000 Constitution, continuing with certain laws passed during this period and concluding with package of Decrees drafted by the Executive based on the enabling law which directly address issues of privacy and communications.

By attempting to resolve the conflict between property and privacy we hope to respond the primary question: What are the electronic privacy expectations in the workplace?

First we will define the essential characteristics of property rights, as they are relevant from an employer's perspective; then we shall review regulations pertaining the labor relationship, the workplace and the safeguarding of work tools, focusing on the Organic Labor Law. Third: We will outline the new privacy rights regulations offered by the Constitution and their development in specific legislation like Law for the Protection of Personal Communications and the Special Law on Information Crimes. Finally we shall link these lines of analysis to ascertain what, if any, limitations can be placed on the privacy expectations of an employee with regard to the use of computer systems owned or provided by the employer for storing personal data and engaging in personal communications.

Private Property Principles:

Starting from the basic premise that the information systems used by the employee in the workplace to store personal data and engage in personal

communications are the property of the employer, we will review the basic elements of the property right as it is stated first in the Constitution and in the Civil Code.

The Constitution¹ states in its article 115:

"The Property right is guaranteed. All persons have the right to use, enjoy and dispose of their property. Property shall be subject to the contributions, restrictions and obligations set by law for purposes of the social good or of general interest."

The Civil Code², in its article 545, repeats the constitutional precept:

"Property is the right to use, enjoy and dispose of a thing in an exclusive manner, with the restrictions and obligations set by the Law."

Note that the Code adds the element of exclusivity to the property right, thus granting the owner the *sole* right to use, enjoy and dispose. Moreover, in article 547, the Code clarifies this even further when it states that

"No one can be forced to transfer his property, nor to allow others to make use of it but for reasons of public or social interest, mediating the due process and previous indemnification."

Here the Code offers us an essential factor to be included in our response to the basic question posed in this article: That an employer, due to his

¹ Official Gazette (Extraordinary) N° 5453, March 24th, 2000.

² Official Gazette N° 2.990 (Extraordinary) July 26th, 1982.

property rights can restrict and limit an employee's use of the employer's computer systems.

Labor Regulations, the workplace and work conditions.

The Venezuelan Labor legal regime makes virtually no mention to privacy and communications *per se*. Yet, it does contain several rules pertinent to our analysis, mainly those regarding agreements on working conditions and causes for justified termination of the employee.

The Organic Labor Law³ establishes on its article 186 that

"The workers and the employers may freely agree on the conditions under which labor will be provided..."

And, in its article 68 the Law enshrines the enforceability of the express provisions agreed upon in the labor contract:

"The labor contract shall be binding with respect to its express agreements and shall carry the consequences that derive from it in accordance with the Law, custom, local usages and equity."

Contractual freedom is severely limited under the Venezuelan Labor Regime, however those limitations derive from Constitutional and legal protection to labor stability, restricting the employer's power to terminate unilaterally the labor relationship with a worker. Also, both the Constitution and the Law require that labor legislation must be interpreted in favor of the worker. We will not engage in an analysis of these contracting limitations, since that is

not the main thrust of this paper, but we can state confidently that there are no specific provisions, neither in the Constitution nor in the Organic Labor Law, openly restricting an employer's power to establish conditions and rules for the use of its information systems. In fact, we find several provisions that offer the employer justifiable reasons to indeed restrict and control access and usage of the company's information systems by the employee. First, the Organic Labor Law includes among the causes for justifiable termination the following (Article 102):

- a) Lack of probity or immoral behavior at work;
- b) Material harm caused intentionally or by gross negligence on machines, work tools, furniture, raw materials or products (manufactured or being processed), plantations or other belongings;
- c) Disclosure of manufacturing, fabrication or procedural secrets.

In each of these scenarios we find justifications for limiting access and usage of information systems. In fact, by setting these limits, the employer is protecting the employee's own interests by reducing the likelihood of engaging in actions that could trigger a justified termination.

- a) Immoral behavior: The employer limits internet access and monitors messages thus avoiding transmission, exhibition and storage of lewd or pornographic material that is too easily available through the internet.

³ Official Gazette (Extraordinary) N° 5152, June 19, 1997.

- b) Material harm to work tools: Again, by restricting access and usage of electronic mail and by monitoring software/information downloads the employer seeks to prevent the damaging effects of computer viruses, Trojan horses, worms and the like. These harmful agents could infiltrate and seriously damage information systems through the negligence of an employee.
- c) Company Secrets: By controlling information flows the employer not only protects its own intangible assets, but also reduces the chances for negligent disclosure.

Privacy Rights under the 1999 Constitution:

The Constitution states the essential rights to privacy in two articles:

"Article 47: The domestic home, the domicile and any private place are inviolable. They can not be searched unless judicially ordered in order to prevent commission of a crime or to comply, in accordance with the law, with decisions issued by the courts, always respecting the dignity of the human being."

"Article 60: All persons are entitled to the protection of their honor, private life, intimacy, their own image, confidentiality and reputation.

The law shall limit the use of information systems to guarantee the honor and both the personal and family intimacy of the citizens and the full exercise of their rights."

However, the Constitution does not offer a clear definition of private place ("recinto" or enclosure) allowing the interpreter to wonder whether the employee can have a private abode within the workplace. However, this question can become moot upon further examination of the Constitution as it develops these rights along the two paths of personal data privacy and communications protection:

"Article 28: Any person has the right to access the information and data that, over himself or his property may be kept in official or private registries, with the exceptions set by the law, as well as learn of their [the information or data] use and of their purpose, and to request before a competent tribunal their update, correction or destruction if they were erroneous or were to illegimitally affect his rights."

"Article 48: The secrecy and inviolability of private communications in all their forms are guaranteed. They can not be tampered with unless so ordered by a competent tribunal, in accordance with legal provisions and preserving the secrecy of what is private that bears no relation to the corresponding procedure."

It would seem then that, by protecting data and communications without regards to where they are located or were to take place as long as

they are private, the issue of private place would not limit an employee's right to privacy even within the workplace.

However, what makes a communication *private*? Not an easy question as the Constitution offers little guidance. However, we will find an answer to that question through the analysis of the Organic Telecommunications Law, the Law for the Protection of Personal Communications and the Law on Information Systems Crimes.

Legal Development of the Privacy and Communications Protection Rights

The Organic Telecommunications Law⁴ enshrines communications privacy protection, as a fundamental user's right on its article 12 when it states that

" In its condition of an user of a telecommunication service, every person is entitled to...

... The privacy and inviolability of their telecommunications, save for those cases expressly authorized by the Constitution or that, due to their very nature, have a public character."

Note that the law provides broad protection to communications and only excludes those communications that are not inherently public.

Communications privacy was also protected in the 1991 Law for the Protection of Personal Communications⁵, which states in articles 1 and 2 that:

"Article 1: The purpose of this Law is to protect the privacy, confidentiality, inviolability and secrecy of communications that take place between two or more persons."

"Article 2: He that in an arbitrary, clandestine or fraudulent manner records or imposes himself on a communication between persons, interrupts or impedes it, shall be punished with prison for three (3) to five (5) years."

Note that the Law did not delve either on the *means* of communication nor on their nature (personal or not) and offers protection *without regard to the means* used to carry out said communication and it also sidesteps the issue of "personal" or "private" communications by privileging those that simply occur *between persons*.

In 2001, the National Assembly passed the Special Law against Information System Crimes⁶ that punishes unlawful activities performed through and on information systems. This law materializes the personal data privacy protection set forth in the Constitution:

"Article 20: Any person that intentionally takes over, utilizes, modifies or eliminates through any means, without their consent, another's data or personal information of or over which said other person has a legitimate interest, that are incorporated in a computer or system that utilizes information

⁴ Official Gazette N° 36970, June 12th 2000.

⁵ Official Gazette N° 34863, December 16th, 1991.

technology, shall be punished with two to six years in prison and fined between two hundred and six hundred tax units.

The penalty shall be increased from a third up to a half if, as a consequence of the aforementioned actions, either third parties or the owner of the data or information suffer any damages.”

The Law also punishes communication privacy crimes in its article 21:

"Any person that, through the use of information technologies, accesses, captures, intercepts, interferes, reproduces, modifies, deviates or eliminates any data message or transmission signal or communication of another person, shall be punished with two to six years in prison and fined from two hundred to six hundred tax units."

Note that the law does not take into consideration who is the owner of the computer or communication systems themselves. That issue is irrelevant since the purpose of the law is to protect any individual's data, personal information or communications.

CONCLUSIONS AND SUGGESTIONS

We have seen how the property rights entitle the employer to dictate the manner in which his information systems can be used by the employee and how, in principle, the employer should be able to monitor

⁶ Official Gazette N° 37.313, October 30th, 2001.

and control any and all information that is stored, received and transmitted by those information systems of the workplace.

We find that the Venezuelan labor law not only permits placing severe restrictions on information systems and computing tools (contractual freedom), but also provides the employer with ample justification to do so.

Yet, the privacy and communications regime sidesteps the issue of ownership and strives to protect (quite severely) both personal information and private communications thus limiting, in fact, the ability of an employer to unilaterally access and monitor data and communications carried out by the employee through the employer's information systems.

Then it would seem that, in principle and lacking any express agreements or provisions to the contrary, the employee may have a very broad expectation of electronic privacy in the workplace.

However, since the employer can require in the labor contract that the employee comply with policies and procedures that define access and usage of information systems; and since the parties can also agree expressly in the labor contract (or even through an incorporation by reference to the aforementioned policies) on a broad authorization from the employee to the employer and its representatives to monitor, access, reproduce, modify and eliminate any and all information that could reside in said information systems, including communications and any personal

information. Then the electronic privacy expectation in the workplace can indeed be narrowed, even to the point of rendering it nonexistent.

In order to avoid potential claims of violation of privacy rights by employees, the employer should issue clear and precise policies stating the limitations to privacy in the computer or information systems provided in the workplace, the right to monitor electronic mail and the acceptance by the employee by reference in the work contract or an implied authorization by virtue of using the information systems subject to the terms and conditions established by the employer.

