Vera Abogados, S.C.

Mexico: The Current Legal Framework Of The Data Privacy And Personal Information Protection In Mexico

11 January 2007

By: Luis Vera Vallejo, © 2006 [(1)]

I. INTRODUCTION

Since the enactment of the Federal Constitution in 1917, the post government administrations show no particular interest to implement neither a formal nor a comprehensive legislation and policies, regarding the protection of Personal Data of the citizens in Mexico.

This situation partially changed during the administration of President Fox (2000-2006), when bills governing the access and protection of personal data in credit bureaus and public government files, were introduced and passed by the Federal Congress.

The purpose of this paper is to describe the current legal framework of the Data Privacy provisions, established in an array of pieces of federal legislation, which will be analyzed hereinafter.

As will be noted, new federal legislation has also covered broader protection to consumers, both "on line" and "off line", as established in the recent amendments to the Federal Consumer Protection Act.

In spite of the opposing voices to the approval of data protection legislation, our conclusion is that in our globalized world, companies in Mexico, should implement corporate data privacy policies and procedures, in order to comply with foreign recommendations and local laws and regulations.

As follows, we will briefly describe a summary of the most relevant Mexican Federal legislation on this matter.

II. CURRENT RELATED LEGISLATION

1. Constitutional Provisions.

The bill of rights guarantees the privacy of private communications including PTT´s communications (post, telegraph and telephone). Likewise, the Constitution also protects the due process of law regarding to search and seizure procedures.

2. PTT´s Confidentiality Related Provisions.

The Federal Communications Act, establishes in Articles 383, 576, 577 and 578 that government and private citizens must keep in strict confidentiality the content of any

messages, except by order of competent court. Severe fines and imprisonment can be imposed to infractors. Likewise, Article 49 of the Federal Telecommunications Act, establishes that any information transmitted through telecommunication networks, shall be confidential, except the information in public domain or by resolution of competent authorities.

3. Statistical - Census Information.

Under Article 5 of the law governing Geographical and Statistical Information (the Census Act), all statistical information collected as well as the data of the informants must be kept in strict confidentiality.

4. Federal Tax Records.

As per Article 69 of the Federal Tax Code, all employees and officers of the Mexican IRS (SAT), must keep in strict confidence all data concerning tax returns, tax payments, tax audits, etc.

Violations to the above will be sanctioned with fines which will run from USDLLS$4,500.00 to USDLLS$6,000.00 per event.

5. The Federal Government Procedures Act.

Under Article 33, petitioners or any interested party, in any governmental matter, shall have the right to be informed about the content of the related and pertinent files, which otherwise must be kept in confidentiality. However, any information regarding to the national defense and security, or any other matter protected by industrial or trade secrets or by any other law, will be also kept in confidentiality.

6. Banking Secrecy.

The Credit Institutions Act, establishes in Article 117 the "Bank Secrecy", wherefore the financial institutions can not disclose any information related to the deposits or any other banking services of their customers to any person, except to the tax authorities or by judicial resolution issued by competent court.

Violation to the above shall be punished by imprisonment from 3 to 9 years, as per the provision of Article 112 Bis of the same law.

7. Insurance and Medical Records.

As per Articles 136, 137 and 138 of the General Health Act, patients have the right that all medical information and clinical records be kept in strict confidentiality and that such information must not be disclosed without his or her authorization, except in those cases under which doctors and hospitals have the obligation to report to the Health Authorities.

The same obligation is established in Article 36 of the law governing Professional Practice.

8. Foreign Investment Law and its Regulations.

It is provided that all information that must be disclosed under the law, by foreign investors, should be kept in confidentiality and the authorities shall not allow the access to any third party to the files and records in the Foreign Investment Office or in the Registry of Foreign Investment.

9. Copyright Law.

It protects the confidentiality of software products and data bases. Files at the Copyright Office regarding to software products should be kept in confidentiality and the access to such files will not be permitted, but only to the copyright-holders. Severe fines may be imposed by the Mexican Institute of Industrial Property.

10. Industrial Property Law.

Regarding to this law, it should be noted that disclosure of trade secrets or the unlawful access or the acquisition of such information by third parties shall be considered a crime and sanctioned with imprisonment up to 10 years.

11. Moral Damage - Civil Remedies.

When collecting, disclosing, transferring, marketing, publishing, disseminating or the use personal data and in particular "Sensitive Data", if one person might suffer or be affected in his feelings, affections, beliefs, honor, reputation, private life, etc., which damages are protected by Article 1916 of the Federal Civil Code, a civil action can be instituted allowing to the affected party to claim the payment of damages, whether contractual or in tort. The amount of the damages shall be determined by the Judge, depending upon the injury caused, the degree of the liability or any other circumstances related to the case.

12. The Federal Criminal Code.

Post and Communications.

- Anyone who deciphers or decodes telecommunications signals or is engaged in the marketing or in the use of apparatus, devices or instruments permitting such activities, shall be punished by imprisonment up to 2 years, as per the provisions of Article 168-Bis of said Code.

- Anyone who opens or intercept any written communication without a legal reason, shall be punished with up to 380 of community working days.

- Anyone who trespass or obtain undue access to private communications without the proper judicial court authorization shall be punished with up to 12 years of imprisonment.

Child Pornography

- Child Pornography is punished with up to 16 years of imprisonment, including transmission by electronic means such as the Internet.

Trade secrets disclosure and unlawful access to data processing equipment and systems.

- Disclosure of confidential information which is known as a consequence of the employment or labor relationship shall be punished with up to 200 of community working days.
- In the event of disclosure by a person rendering professional or technical services or in the event that the nature of the information disclosed is a confidential trade secret, then, the punishment will be imprisonment up to 5 years.
- Access, disclosure or use of information or images obtained from a private communication shall be punished with imprisonment up to 12 years.
- Anyone who access or copy information contained in data processing equipment or systems, shall be imprisoned up to 1 year.

13. Workplace Environment.

The Federal Labor Law was enacted in 1931. Since then and as up to date, labor courts continue resolving claims in the most favorable manner to employees.

The employer must respect the dignity of employee´s labor conditions at the workplace as established in Articles 3 and 56 of the Labor Law. Such principle can not be matter of a waiver by the employees. Any pact in contrary, shall be considered null and void.

As per Article 133 – VII, employers are forbidden to perform any act which restrains the labor rights of the employees.

In view of the foregoing, when implementing any employment data privacy or any surveillance procedures at the working place, including the access and search through electronic and computer technology, to collect, analyze, reproduce and disseminate information about employees, the above provisions must be taken into consideration. Likewise, it is important to point out that any of the above practices including monitoring e-mails or the company´s intranets, should be clearly specified in both, the employment agreement and in the interior working regulations, as well. A clear written consent by employee to any company policy must be implemented.

III. THE PERSONAL DATA PROTECTION PENDING BILLS.

Since January 2001, several legislators have sponsored in Congress, bills governing the protection of personal data privacy, in particular regarding to personal data stored and disseminated by the private sector, including private corporations, advertising and other direct marketing organizations. Most of these bills were strongly opposed and lobyied by the private sector and industry chambers which finally obtained to stop the approval of said bills within the Congress.

However, it is quite foreseeable that the new Congress (2006-2012) will take again the initiative to promote the approval of this kind of legislation. Some sectors including several NGO´s promoting the protection of data privacy, will encourage legislators to approve data privacy laws covering the creation of a data privacy authority to protect and enforce the following ("habeas data") rights:

- The right to access.
- The right to be informed.
- The right to oppose to data collection.
- The right to oppose to the disclosure, transfer or dissemination of personal and in particular "sensitive" information.
- The right to correct and update.
- The prohibition or restrictions to transborder data flows.

Private sector main opposition to the various introduced bills on this subject matter, argued:

- That the creation of a Data Privacy Agency, would generate more bureaucracy and unnecessary burden and costs to private companies.
- The imposition of fines and criminal sanctions by the Data Privacy Agency.
- Frivolous complaints by angry current or dismissed employees.
- The impact and effects of prohibition or restrictions to the free transborder data flows.

In addition to the above, direct marketing companies, advertising call centers, credit cards and other similar marketing organizations strongly opposed to the "opt-in" concept instead of the "opt-out" procedure, which was a bargaining condition to the acceptance of the proposed bills.

The current trend is to expect that a data privacy legislation will pass, hoping that its provisions satisfy both public and private interests as well.

IV. THE RECENT DATA PRIVACY LEGISLATION.

As indicated in the beginning of this paper, it was only in recent years when specific data privacy legislation was proposed by the Executive Branch and/or sponsored by Congress.

The following pieces of legislation were approved by Congress:

- The Credit Bureaus Act.
- The Federal Law for the Access to the Governmental Public Records and Information.
- The Revised Federal Consumer Protection Act.

The first two above mentioned bills were approved by Congress in the year of 2002 and the last one in 2004.

As follows we will briefly discuss the above mentioned enacted statutes:

- **The Credit Bureaus Act.**

  This law permits consumers or users of the banking system and credit applicants, to obtain access to their own credit records and also to request and or to claim the pertinent corrections and information updates as relevant, including the elimination of their personal data from the data bases of the credit bureaus, when applicable, as per the provisions of this law.

- **The Federal Law for the Access to the Governmental Public Records and Information.**

  This law was published on June 11, 2002. It was widely advertised by the Presidency of the Republic, as an outstanding achievement of the new democracy promised by President Fox. Under this law, all citizens are entitled and government officers are obligated to permit citizens the access to the federal government agencies records and files and also to be informed about other data such as remunerations of public servants, government projects, government services, etc. This information may be accessed also by electronic means such as the Internet. However, under Article 13 of the law, certain information which is considered reserved, classified or which affects the national security or the national defense shall remain confidential.

  Likewise, government officers are obligated to keep in confidentiality personal data of the citizens contained in public records. Citizens are entitled to access to their own information and to request correction, modification and updating of the individual´s personal data.

  Government officers are forbidden to disclose, distribute, disseminate or marketing the citizen´s personal data both "on line" or "off line", without express written consent of the corresponding individual, with certain exceptions, including when such disclosure is decreed by resolution of competent courts.

  It is created a new governmental body called the Federal Institute for the Access to Public Information, in order to handle and perform the proper compliance of the provisions of this law and to grant remedies and impose sanctions in the event of violation to its provisions.

V.- CONSUMER PROTECTION.

We will now focus our attention to the Federal Consumer Protection Act, revised in February 4, 2004. Also, we will refer to the consumers protection in "on line" transactions, previously introduced in this law in the year of 2000.

Consumers "On Line" Protection provisions:

- The vendor is obligated to keep confidential the information provided by the Consumer, wherefore such information can not be disclosed, transferred or disseminated to other vendors, unless previous authorization is granted by the consumer.
- The vendor must inform to the consumer the technology used to assure the safety and confidentiality of the information provided by the consumer.
- Before any transaction is concluded, the vendor must inform to the consumer its physical domicile, telephone numbers and pertinent information regarding its policies concerning warranties and the instructions to make effective such warranties.
- Vendor shall avoid deceptive marketing and advertisement practices.
- Vendors must clearly inform to the consumer whenever the products or services are addressed to the elderly, children or ill people.

The 2004 Amendment.

Regarding to the new scope of the law, it is emphasized that it protect consumers in both, "on line" and "off line" transactions.

- The concept of consumer is modified to include corporations and not only individuals, wherever the transaction involved is not higher than USDLLS$ 30,000. Accordingly, now corporations which execute transactions with vendors, not exceeding the amount above mentioned, are entitled to file complaints before the Federal Consumers Protection Agency (FCPA).
- The FCPA is also entitled to monitor web sites in order to verify the proper fulfillment to the provisions of this law.
- Vendors and companies which collect, gather and use consumer´s information are obligated to report to any person what information they keep and to provide a report on such information, including to mention if said information has been shared with any third party, identifying such third party. Consumers have the right to request corrections if appropriate and vendors or the third party must comply with such petition within the following 30 days.
- All advertising sent to consumers, both "on line" or "off line", should indicate the name, address, telephone and the e-mail of the vendor.

Consumers are entitled to request to vendors not to be annoyed whether in their domiciles, working place or e-mails with advertising (SPAM).

- Consumers may request to vendors and advertising companies that the consumers information may not be transferred or assigned to any third party.
- The FCPA shall keep a public registry of consumers in which will be listed the names and telephone numbers of the consumers which have decided not to receive information or advertising materials, both "off or on-line", including a "do not call" registry. Prior to send any marketing or advertising messages to consumers, vendors must consult the list of the consumers which have requested not to receive SPAM. The same applies to marketing call centers.
- Regarding to contract formation, it is established that any contract will be considered as concluded after five (5) days of the delivery of the merchandise or the execution of the agreement, whichever is later. During this five days period, consumer is entitled to revoke its consent without any liability.
- Vendors engaged in the repair or maintenance must use "new spare parts" unless written authorization of the consumer.
- Standard agreements (adhesion contracts), whether "on line" or "off line" in order to be valid, must be in Spanish language and in a clear and conspicuous manner.
- The FCPA is entitled to declare which standard agreements must be registered and approved by the FCPA. Article 90 establishes that certain contractual provisions can not be included such as the submission to foreign courts. The forbidden clauses shall be null and void.

Consumer Remedies

Consumers shall have the right at its choice, to the replacement of the merchandise or the refund of the price paid, if the goods or services do not meet with the quantity or quality requested, the trademark or any other specifications of the products or in the event of services, the equipment is not properly repaired. In such cases, additionally consumers will be entitled to a compensation in an amount not less to the equivalent of 20% of the paid price, regardless of the following additional statutory damages:

- If the consumer has paid the price in full, it will be entitled to collect 30% of such price.
- If the consumer has paid more than 50% of the price, then he will be entitled to a compensation equivalent to the 25% of the price.
- If the consumer has paid up to the 50% of the price, he will receive a compensation equivalent to 20% of the contractual consideration.

In any other cases, such compensation will be no less than 20% of the total amount established in the contract.

In addition to the above, the FCPA will impose very expensive fines to the vendor depending upon the violation incurred. Such fines now has been increased to an average of USDLLS$ 50,000.00 to USDLLS$ 500,000.00, being the FCPA also empowered to shut down the premises of the vendor.

VI.- CORPORATE DATA PRIVACY PRACTICES

Although the Mexican Department of Commerce is trying to encourage industrial chambers and trade associations to formalize Ethic Codes and to promote self-industry regulations, as far as we know, such policy has not been successfully implemented. Accordingly, very few industry organizations have Ethic Codes such as the Mexican IT Association, the Mexican Internet Industry Association, the Mexican Advertising Council, the Bankers Association, among others.

Probably, the above is due to the fact that there is no formal enacted law governing Data Privacy in the private sector.

Due to the global nature of Internet, several multinational subsidiaries based in Mexico, have implemented their own Ethic Codes and Data Privacy procedures, in order to comply with parent global policies.

At this point in time, is difficult to ascertain whether or not the Personal Data Privacy and Information Protection Bills would be revived. However and under the likelihood of the near approval of legislation on this matter, industry needs to be prepared to comply with Data Privacy Policies and Procedures. In any case, since the impact of privacy is now a part of the corporate culture, Mexican companies and foreign local subsidiaries need to know how to avoid privacy risks and legal exposures.

For instance, it is highly recommended that such procedures include[(2)]:

- Website privacy policies (and the extensive internal due diligence and procedures necessary to implement them);
- Online information collection, use, and dissemination practices;
- Cookies and other tracking technologies;
- Online profiling;
- Third-party databases and publicly available personal information;
- Privacy issues associated with digital signatures, smart cards, and other key technologies;
- Crossing virtual borders in transmitting data;
- Collecting and using certain types of sensitive information (e.g., financial, medical, from children);
- Privacy and data protection issues in the electronic workplace; and
- New laws and pending legislation on privacy at both the federal and state level.

VII.- CONCLUSIONS AND RECOMMENDATIONS

As described in this paper, Mexico has enacted and put in force a variety of Federal Data Privacy statutes which were listed herein. The most important ones for the private sector, are those related to data privacy policies and procedures in the work place environment and also the newly revised Federal Consumer Protection regulations. Other statutes might also apply, in particular the provisions regarding to the access to the telecommunications facilities, labor and criminal legislation.

When implementing corporate policies, local companies need to take care on how to implement such policies in order to adapt them to the Mexican environment and current legislation, and also thinking in the near future possibility of new legislation protecting the treatment of privacy of data stored, managed and disseminated by the private sector.

Footnotes

* This paper is "CONFIDENTIAL" and can not be copied without authorization of the author.

(1) Mr. Luis Vera Vallejo is the Senior Partner of the Mexican Law Firm VERA ABOGADOS, S.C.

(2) Excerpts from the Article "E-Privacy Law Committee Targets the E-Commerce Legal Issue Facing Every Client", written by Ruth Hill Bro – The ABA E-Privacy Law Committee.