



ACCESS TO PUBLIC INFORMATION AND PERSONAL DATA PROTECTION

Huixquilucan (Mexico State), 4th November 2005

TABLE OF CONTENTS

- I. INTRODUCTION**
- II. PRINCIPLES OF ACCESS TO PUBLIC INFORMATION**
- III. PERSONAL DATA PROTECTION PRINCIPLES**
- IV. ACCESS TO INFORMATION AND THE PROTECTION OF PERSONAL DATA**
 - 1. THE BALANCE OF RIGHTS**
 - 2. PROOF OR BALANCE OF PUBLIC INTEREST**
 - 3. SPECIFIC CASES**
- V. CONCLUSIONS**



ACCESS TO PUBLIC INFORMATION AND PERSONAL DATA PROTECTION

Huixquilucan (Mexico State), 4th November 2005

I. INTRODUCTION

The right to access public information, that is, information in the possession of public sector entities in modern societies, constitutes a control mechanism that enables citizens to be aware of the actions taken by this sector and acts as a vehicle through which the sector can account for such actions. In this respect, access to public information has become a fundamental component of a democratic, transparent society.

However, the necessary transparency that must prevail in government activities must also be reconciled with the legal interests protected by law, such as other fundamental human rights, particularly the fundamental right to privacy. This reconciliation becomes even more evident if we take into account the effects of the fast progress of technology on the issue of privacy.

As the case in point encompasses two rights, certain conflicts may underlie particular cases of access to information and the protection of personal data, arising from the fact that both rights cannot be exercised absolutely in all cases.

The rights of all those affected must be respected, and no single right must prevail over others, except in clear and express circumstances. The laws governing access to information set out a clear, well-defined list of the matters that cannot be made public. Generally, there are two types of data envisaged as exceptions to access; the first usually refers to those matters limited only to the State in protection of the general public good, such as national security, damage to the national economy or international relations. In cases where governmental information is reserved, the relevant authorities must prove the damage that diffusion of certain information will effectively cause to the legal interests protected by law, so that the least amount of information possible is reserved to benefit the individual, thus facilitating assessment of governmental activities.

The other type of information held by the State is related to the personal data of both private citizens and legal entities. In the case of individuals, their personal data are protected by the laws of access to confidential data and by personal data protection legislation.



ACCESS TO PUBLIC INFORMATION AND PERSONAL DATA PROTECTION

Huixquilucan (Mexico State), 4th November 2005

Likewise, the exercise of the right to personal data protection has its limits, although such limits must meet the following criteria: a) they are permissible to the extent that there is a prevailing public interest; b) there is an express, precise, legal instrument that meets the requirements of the principle of proportionality; c) the doubt in question should be interpreted in a limited manner, as it is a matter of “guaranteeing and protecting public freedoms and the fundamental rights of individuals with respect to personal data processing, and in particular, their honour and personal and family privacy”, and d) the consideration of whether such limits not only violate the principles of consent and purpose established by personal data protection laws, but also the principle of quality, which provides that only the data that is absolutely necessary should be made available to attain the aforesaid purpose.

It may be said that there is no true *a priori* conflict between the right to information and the right to personal data protection, and therefore, no prior legal-philosophical scenario need occupy our attention. It is rather a question of seeing that the relevant authorities, or those with jurisdictional or quasi-jurisdictional powers, resolve the issues amicably as they arise, *ad casum*.

Furthermore, democratic societies must safeguard the protection of personal data. The most fully developed regime for such protection is envisaged in the European models, which are based primarily on Convention 108 of the European Council on the protection of individuals with regards to processing of personal data issued in 1981, and Directive 95/46/EC of the European Parliament and Council on the Protection of Personal Data.

The aforementioned legislation also establishes the rights to access, correction, cancellation and opposition as fundamental rights of all data subjects.

Thus, the present study is addressed at setting out the principles that govern access to public information on the one hand, and those regulating personal data protection on the other; the possible exceptions to those principles, and certain cases of conflicts of rights that may arise due to the diversity of the principles that apply to both issues.



ACCESS TO PUBLIC INFORMATION AND PERSONAL DATA PROTECTION

Huixquilucan (Mexico State), 4th November 2005

II. PRINCIPLES OF ACCESS TO PUBLIC INFORMATION

The regulation of access to public information is a relatively recent phenomenon. Three-quarters of the sixty countries that currently have legislation governing access to information approved these laws in the last 15 years. The aforesaid regulations vary in their structure; for example, some countries have laws that govern access to information at federal, state or provincial levels, with differing degrees of scope and content.

Access to the public information held by the government is an important concept for various reasons. Firstly, the true owner of the information is actually the individual. It is the people who elect a government and entrust it with the power to take decisions on public matters. The government collects information and takes decisions that are subsequently recorded in different documents. But, all of this is done on behalf of the people, as the people's representative. Therefore, the people are entitled to know and access all the information that the government has generated. Secondly, access to information is one of the foundations on which accountability is based, and accountability is an essential component of effective democracy. Accountability means that public servants are required to inform the public about government actions. Many regulations on access to information oblige governmental agencies to publish various types of information, which are actually another instrument for accountability. And thirdly, access to information is an effective mechanism for evaluating and controlling those in power. This type of legislation entitles individuals and organisations to request information that enables them to study the actions of their leaders in different matters. Public servants are aware that they are accountable for their actions, and this creates an incentive for them to act in accordance with their mandate and the legislation applicable to their sphere of responsibility.

Given the foregoing, legislation regulating access to public information must be viewed as a priority in all governments, particularly when endeavouring to open up a new relationship with society. Certain general principles must be taken into account in order to effectively legislate in this respect.¹ Firstly, the principle of maximum public access must be a priority. Many national regulations envisage this principle, which stipulates that all the information in the possession of the

¹ For a more in-depth discussion of the principles of the right of access to information, see Mendel, Toby. *Freedom of Information: A Comparative Legal Survey*. New Delhi: UNESCO, 2003.



ACCESS TO PUBLIC INFORMATION AND PERSONAL DATA PROTECTION

Huixquilucan (Mexico State), 4th November 2005

government is public, and that access to the same shall only be refused in exceptional cases. A further aspect of this principle establishes that individuals may access the information held by any government agency without having to prove any legal interest in the same. Of all the principles that typify laws regarding access to information, maximum public access should undoubtedly be the prevailing governing concept.

A second principle to be taken into account is the obligation to publish all relevant information without prior request from the public. In effect, government agencies must be required to publish information of public interest without the need for an express request for such publication. Certain national laws contemplate what are known as “transparency obligations”, also called “fundamental information”, which require entities (“subject individuals”) to publish information on the wages and salaries of public servants, the contracts entered into by the government, the budget, the goals and programmes undertaken by the department, entity or government body in question, amongst many other matters.

A third noteworthy principle is that exceptions to the access to information held by the government must be minimal. This is known as the “exception regime” in many laws. Of course, personal data must be confidential and access to the same must be limited (generally speaking, only available to the data subject). But there is another type of information to which government agencies may refuse access on the grounds that public knowledge of the same would have seriously adverse affects on the entity, or would give rise to risks in delicate matters of state, such as national security. The exception regime is one of the most complex aspects that legislation on access to information must contemplate. In addition to personal data, there must be certain parameters, such as the public good, that clearly establish the cases in which a government body may refuse access to information.

A fourth principle has to do with ease of access, which implies various issues. One of these is to stipulate the rapid processing of requests for information, preferably including the establishment of reasonable terms for its provision. Another relevant aspect is the existence of an independent and autonomous body to study the cases in which the applicant is refused information, as the mere existence of legislation on access to public information does not guarantee that this individual right may be effectively practised. In certain countries, the



ACCESS TO PUBLIC INFORMATION AND PERSONAL DATA PROTECTION

Huixquilucan (Mexico State), 4th November 2005

laws do not provide mechanisms to reinforce access to information, while in others, the government creates obstacles or takes advantage of legal vacuums to avoid having to make the information in its possession public.

The fifth relevant principle refers to the provision of information free of cost, or the establishment of costs that make requests for information affordable by all. In general, this implies that the government body must keep the cost of reproducing the information to a minimum, even when such cost may be passed on to the party requesting it. Many other factors must also be included in laws governing access to public information. Penalties for non-compliance, for example, is one such factor, although the existing legislation varies considerably in this respect.

A sixth principle has to do with finding the institutional structure that envisages the persons responsible for handling requests for access within the government body and mechanisms for revising the decisions taken by such persons. These mechanisms may be implemented either in the government agency itself or through a body entrusted with overseeing observance of the law. The latter is one of the most solid principles on which effective access to public information in the possession of the State is based.

Furthermore, a key issue to be considered and for which there is no pre-established principle is the scope of application of the law. The majority of legislation on this matter stipulates that federal or national government agencies are subjects with obligations under the law, including those operating in decentralised regimes. Other countries establish a general law that governs this right over practically all the public bodies of the State, both at national and local levels. On the other hand, countries with unitary governments will probably set out generally or nationally applicable laws that govern access to information in practically every government body. The essential point here is that citizens have a government that is open in matters of access to information. That is, regardless of the type of government of the country in question, citizens have the legal mechanisms to enable them access to the public information held by their government, whether this is national, federal or local. Perhaps a federal state should have more than one law on access to information to be able to ensure access to all government documents. But it must be stressed that access to information is a fundamental right that guarantees the true exercise of democracy, and the type of government should not be an obstacle in making this right effective.



ACCESS TO PUBLIC INFORMATION AND PERSONAL DATA PROTECTION

Huixquilucan (Mexico State), 4th November 2005

III. PRINCIPLES OF PERSONAL DATA PROTECTION

The basic principle governing the processing of personal data must be consent, such that, on principle, personal data must be collected, processed or communicated to third parties with the data subject's consent.

However, the fundamental right to personal data protection is not absolute, but rather must find a balance when it converges with other fundamental rights, such as the right to information or effective legal protection, or constitutionally protected concepts such as transparency in government bodies, the protection of health, national security or other legally governed matters of the public good.

This implies that the principle of consent must give way to such matters of public good when envisaged by law, provided that the law is sufficiently specific and is not so far-reaching that it constitutes violation of this fundamental right.

This guiding principle must also seek a balance with other fundamental rights on the basis of proportionality that allows the resolution of those cases in which various rights conflict.

This assessment must be particularly rigorous in cases dealing with especially confidential personal information, such as data on ideology, labour affiliation, religious beliefs, ethnic origin or sexual preferences.

The principle of consent is closely linked to another basic principle, which is the right to information.

Individuals should be informed, even when the provision of their information is compulsory, as to who will process their personal data, the purpose of such processing, whether the data will be transmitted or accessed by third parties and the cases in which the provision of such data is compulsory.

Likewise, data subjects must be given the address of the controller of their data to enable them to exercise their rights of access, correction, cancellation or opposition.



ACCESS TO PUBLIC INFORMATION AND PERSONAL DATA PROTECTION

Huixquilucan (Mexico State), 4th November 2005

Moreover, the data requested must encompass only the information strictly necessary and appropriate for the purpose, such that unnecessary information is neither requested nor processed.

And, when the data is no longer necessary for such purpose, physical or other measures must be undertaken to prevent further processing of the information, except when justifiably required in the course of administrative or jurisdictional responsibilities related to the completed personal data processing.

A particularly relevant principle is limitation on the purpose for which the data is processed, as this enables legitimate consent, when required, and restriction of the processing of the data when such consent is excluded, especially in the case of government bodies.

In any case, the information processed must be accurate and updated, ensuring a suitable degree of quality.

Personal data processing must be subject to specific security and secrecy obligations.

The former require the definition and implementation of the suitable technical and organisational media to ensure that the data meets the requirements of integrity and to prevent, or at least allow detection of, unauthorised access to the same.

The latter must be addressed at the parties with access to personal data who, save very specific exceptions, may not disclose the data to which they have access to third parties and must be expressly advised of such obligation.

IV. ACCESS TO INFORMATION AND PERSONAL DATA PROTECTION

Although it is true that all democratic regimes must guarantee the right of access to public information, it is also true that they must safeguard the individual's right to privacy. In fact, both rights are often found at the same regulatory level. For example, both are established in the Universal Declaration of Human Rights. Article 19 of this document establishes that: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any



ACCESS TO PUBLIC INFORMATION AND PERSONAL DATA PROTECTION

Huixquilucan (Mexico State), 4th November 2005

media and regardless of frontiers”. Likewise, Article 12 of the aforementioned Declaration provides that, “no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks”.

The topic is particularly relevant, as at times it would seem that both rights are in conflict, while on other occasions they complement each other, for example, in the context of cases where government bodies or public entities must be accountable to the public. As observed by David Banisar, “These rights may be complementary in the case of request for access to personal data in the possession of a government body. Both rights may also be used to allow individuals to access their own data and thus promote governmental accountability”.²

One of the most common areas of conflict between access to information and privacy lies in personal data protection. This refers to a certain type of private information and consists of “the right of individuals to control the personal data in the possession of third parties, such as financial or medical data”, as well as the rules for their collection and processing.³ In effect, government agencies collect a large quantity of personal data, which may give rise to a number of conflicts related to access to the information. For instance, many governmental organisations may restrict access to a certain type of information, alleging that public knowledge of the same would violate the privacy of individuals. Of course, the first issue to be envisaged is the proper classification of such data. But there are situations where it is not totally clear whether the information should be classified as confidential simply because it contains personal data. In such cases, the law envisages certain tests that allow an assessment of the value of making the knowledge public for the general good, as compared to the individual need to protect it.

Thus, it is even more important that, given the regulations both of access to information and on personal data protection, the two be complementary, so that such points of conflict are minimal. In this way, individuals are guaranteed their right to access the information in the possession of the government, while at the

² Banisar, David. *Two Sides of the Same Coin: Conflicts and Complements Between Privacy and Freedom of Information Laws*. Manuscript, 2005, p. 1.

³ *Ibid.*, p. 2.



ACCESS TO PUBLIC INFORMATION AND PERSONAL DATA PROTECTION

Huixquilucan (Mexico State), 4th November 2005

same time the personal data held by such government may not be disclosed to third parties without the consent of the data subject.

1. THE BALANCE OF RIGHTS

A discussion of the right to access to information and the right to personal data protection obviously leads to a consideration of the limits on the exercise of these rights.

One of the most complex aspects in the philosophy behind fundamental rights is how to come to a reasonably fair solution in those cases where such rights appear to conflict or collide. Perhaps the best way to find a solution in cases of conflict is to seek a different viewpoint, which first entails acceptance that the fundamental rights – and the obligations to which they give rise – are amicably interrelated or correlated.

We might say that the fundamental rights have points of contact between them, rather than conflicts *per se*. The key is to seek out interpretational approaches to bring them together, so that conflicts are not insurmountable and controversy, therefore, inevitable. Oppositional positions can lead inexorably to confrontations that can only be overcome by choosing one of the rights and ignoring the other. However, the principle of equality establishes that no rights shall be sacrificed for others.

Specifically within the scope of access to information and personal data protection, there are points of conflict that merit exhaustive study and an individualised interpretation in each specific case.

2. PROOF OF BALANCE OR PUBLIC INTEREST

Both the right to access public information and the right to personal data protection allow the establishment of certain limits, expressed in legal provisions



ACCESS TO PUBLIC INFORMATION AND PERSONAL DATA PROTECTION

Huixquilucan (Mexico State), 4th November 2005

that contain the specific rationales against their diffusion in the former and in pro of their disclosure in the latter.

In this respect, and in the case of governmental information, access may be limited for reasons of State (secret) or because it refers to data on individuals (confidentiality).

The main limitation on access to the personal data obtained by public bodies in the exercise of their respective duties lies in the rights of third parties, particularly in protection of the privacy of such parties (individuals). In other words, the confidentiality of the data is addressed at protecting the individual's sphere of activity from undue interference from authorities and other individuals.

However, there may be circumstances in which the public good must prevail over individual interests; that is, the good sought by the State in opening up such information is greater than the harm that would be done to the individual in question by violating his/her right to privacy. This necessitates careful and in-depth analysis by the authorities of the interests in conflict before allowing the possible disclosure of certain personal data in exceptional circumstances.

Such a decision cannot be subjective, and must be strictly founded on the goals pursued by the laws themselves when, for instance, the issue at hand is transparency and accountability. Likewise, procedural conditions must be envisaged to guarantee the holders of the conflicting rights due hearing.

Finally, this type of decision, known in comparative law as proof of public interest, should only be undertaken when requested by a party thereto. The applicant is thus responsible for providing all the elements of proof that allow the authority to establish unequivocally that the public interest envisaged in the law should prevail over the specific cases of individual interests.

In view of the foregoing, proof or balance of public interest may be said to exist when:

1. The authority that resolves the conflict issues a well-founded and causal ruling, based on express legal provisions;



ACCESS TO PUBLIC INFORMATION AND PERSONAL DATA PROTECTION

Huixquilucan (Mexico State), 4th November 2005

2. Procedural conditions are established to ensure the holders of the conflicting rights due hearing, and
3. It is only undertaken at the request of an affected party.

3. SPECIFIC CASES

a) Environmental information

Information related to the quality of the environment is deemed to be of public interest, given the scope of its effects on the public and on the life and health of populated areas. Should information be requested about a certain person who, through his/her business activity, pollutes a river or the air, if knowledge of such personal data becomes an essential factor in proving cause of the damage to the ecosystem, public access to such data could be justifiable. In this case, the actions that could be taken to reverse the damage or prevent its progress would revert in benefit of the affected communities.

Proof of public interest would necessarily lead to public disclosure of such individual's personal data and his/her consent to their disclosure in this case would be limited. In tests of proof or balance of public interest, the public good generated by access to the information in question would have greater weight than the damage caused to the individual.⁴

b) Information about government employees.

When the public requests information about a public servant, a distinction must be made between the personal data inherent to the position and those that are not, and therefore affect only his/her private life. This task sounds like a simple one, but although it may be validly stated that the generalised consensus on this matter supports the protection of the public servant's personal data as an individual, provided that such protection does not prevent due accountability, there are also those who argue that public servants must effectively waive the right to privacy in favour of transparency.

⁴ This proof of public good or balance is a very developed concept in countries such as Ireland and the United States of America.



ACCESS TO PUBLIC INFORMATION AND PERSONAL DATA PROTECTION

Huixquilucan (Mexico State), 4th November 2005

Certain bodies of law containing provisions on access to public information establish that individuals may have access to the personal data of public servants even without express request and, in the absence of specific regulations, some governments have even opted to publish their organisational charts and the salaries of their employees.⁵

The above notwithstanding, a key issue in this matter is that the fundamental rights of the public servant are not lost or diminished by virtue of his/her position. However, the data related to the public servant that must be made public are envisaged as exceptions, and in the event of legal vacuums, the criteria of public duties or exercise of a public position should be applicable in clarifying any doubts.

Therefore, if public access to the files or personal data systems containing photographs of all public servants, their dates of birth, *curriculum vitae*, tax rolls or tax identification numbers is requested, criteria must be drawn up *ad-casum* by each of the relevant authorities, taking into account: i) if any precedents exist in favour of making such data public in the respective laws, ii) if the disclosure of the personal data may be linked to or provide knowledge of the proper performance of the duties and tasks assigned to the public servant in any specific case; iii) if such data is deemed to comprise the individual's private information, not related to his/her position in the organisational structure, and, iv) if disclosure will furnish the information required to establish accountability or transparency in the use of public resources

c) Medical records

In the case of access to health-related personal data contained in medical records, the basic premise is that the patient is entitled to be aware of the information on his/her state of physical and mental health. However, certain regulations require that access to medical data may only be obtained through health-care professionals, or that the patient is only entitled to a summary of his/her medical file, which does not contain, for example, the case notes made by the physician.

⁵ Certain laws on access to information establish so-called transparency obligations, amongst which is information related to a directory of public servants, their positions, level in the organisational structure, institutional telephone number, address for correspondence and, if the case may be, fax and e-mail address.



ACCESS TO PUBLIC INFORMATION AND PERSONAL DATA PROTECTION

Huixquilucan (Mexico State), 4th November 2005

It is important to remember that a medical record contains both objective and subjective data, and the latter are comprised of the physician's opinions drawn from the patient's objective data. In this respect, it is important to base the concept on the premise that all the information related to the physical or mental health of a data subject constitutes personal data, to which the data subject is entitled access. Thus, both the objective and the subjective data are regarded as personal data.

In consequence, the data subject is clearly entitled to access the objective information without any restriction. However, there may be certain variations in this interpretation with regards to the subjective data. A possibly valid approach to this issue is that the patient's right to informed self-determination, which attributes the individual the power to control and dispose of his/her personal data, would be of greater weight. On the other hand, a case-by-case analysis could also determine the situations in which certain information should be held back, because, although it constitutes personal patient data, knowledge of the same at any given time could cause injury to the life, safety or health of the data subject. The physicians' notes could fall into this category, in which case the following two questions must be analysed: *i)* how to determine whether the medical information is objective, taken from clinical findings, or subjective?, and *ii)* whether knowledge of the information contained in the aforesaid subjective notes is part of a process of deliberation, and/or as such, could put the life, safety or health of the patient at risk, and if not, whether such data must be made accessible, given that it encompasses *in fine* personal data (even when it is comprised of speculation, deliberations or testing, the result of these practises is actually information related to an identified individual).

V. CONCLUSIONS

Based on the preceding analysis, the following conclusions may be drawn.

1. There is a diversity of models and vast differences between the systems that guarantee and protect the rights of access to information and of personal data, which affect the actual and effective safeguard



ACCESS TO PUBLIC INFORMATION AND PERSONAL DATA PROTECTION

Huixquilucan (Mexico State), 4th November 2005

of such rights. Thus, there is an apparent need not only for the legal instruments specifically envisaging each right, but also for the suitable institutional and procedural mechanisms to this effect. This leads to our belief in the advisability of independent supervisory authorities;

2. The definition of concepts such as privacy, public information and confidentiality contain many vacuums. These terms must be defined with greater precision in order to limit the range of discretion allowed bodies that take decisions on requests for access to public information;
3. The foregoing indicates that the existing laws on access to public information tend to follow the criteria described below:
 - a) The right of the data subject to access to administrative documents generated or obtained by the State in the exercise of its powers. (without proof of legal capacity or interest);
 - b) The determination of subjects obligated by law does not follow uniform criteria, as these, at times, cover the public administration and, at others, legislative and judicial bodies;
 - c) An expeditious procedure for access and appeal in the event of refusal, which may be exercised before different authorities, depending on the model in question. These procedures may be addressed at the persons on the next higher level of the organisation, an administrative committee created to this effect or may be submitted directly before the Courts.
4. On the other hand, data protection laws should follow a model, a series of principles and recognised rights of the data subject that originate in the concept of personal data as all information concerning an identified and identifiable individual.

The basic principles recognised in personal data protection laws may be summarised as follows:

- i) The legitimacy of the processing;



ACCESS TO PUBLIC INFORMATION AND PERSONAL DATA PROTECTION

Huixquilucan (Mexico State), 4th November 2005

- ii) information;
- iii) quality of the data;
- iv) purpose;
- v) security; and
- vi) supervision by an independent authority.

5. In cases of conflict between the right to access governmental information and personal data protection, a test of proof or balance of public interest with clear and precise rules should be drawn up to determine which of the protected rights – the right to knowledge or the right to privacy – should prevail according to the existing circumstances.

Huixquilucan (Mexico State), 4th November 2005*

* The *Dirección Nacional de Protección de Datos* (National Directorate of Data Protection) of the Republic of Argentina has not issued an opinion on this document.