Leave page blank without running head and folio

The Internet, rights and society

The impact of new information and communication technologies on privacy rights

Carlos G. Gregorio,

Silvana Greco and Javier Baliosian[1]

Introduction

The growing levels of information technology available to state agencies and individuals, and the exponential growth in access to sources of information over the Internet, are giving rise to situations that until a few years ago were unimaginable. In some cases, these applications can be abused by those so inclined to threaten some of our fundamental rights. Meanwhile, national legislation and international instruments governing the use of these applications may not be adequate: they are rapidly becoming out of date and are leaving potentially dangerous regulatory gaps. At the same time, both the content and the accessibility of information are being viewed in new ways and are being used, for example, as an instrument to make public policies more effective or to pursue private interests.

The situation is changing so fast that the conventional rules of ethics and law no longer seem effective, and the justice system has been little involved in the area of privacy violations. This means that the body of available case law (which is in fact a more dynamic way of establishing rules than the legislative route) is very limited.

On the Internet, as well as in the information systems of government and private parties, the growing capacity of search engines as well as increased storage capacity[2] are rendering the rights of privacy and intimacy ever more vulnerable. On the other hand, the ease of connectivity and the interactivity of data tend to blur the limits of information systems, and this is true not only of data that are stored electronically.

This research project attempts to assess the impact of information and communication technologies (ICTs), and in particular that of personal databases, on the rights to privacy and intimacy, with a view to developing legal, judicial and technical mechanisms for their protection. We also attempt to develop some paradigms for information systems that will meet the needs for which they were created (the principle of "end purpose") without posing a threat to privacy and intimacy.

We selected a group of countries (Argentina, Brazil, Costa Rica, Chile, Jamaica, Ecuador, Mexico, Dominican Republic, Trinidad and Tobago, Venezuela and Uruguay) in which we tried to identify situations, legislation and case law, if not in an exhaustive manner then at least ensuring that the information collected would provide a clear appreciation of violations and of approaches to guaranteeing those rights.[3]

The right to privacy, intimacy and personal data

The treatment of rights to intimacy and privacy has differed between the Common Law tradition of Anglo-Saxon countries and continental law, primarily that of Spain, France and Latin America. In the Anglo-Saxon tradition, privacy rights cover a broader field (Shepherd 2001):

(a) As a right that is fundamental to liberty
(b) As a means of preventing and protecting against totalitarianism
(c) As the "right to be left alone"[4]

In the United States, the right to privacy was established by a series of Supreme Court decisions defining a realm of personal decisions in which the state could not intervene. The legal precedents refer to acts of many different kinds: in *Pierce v. Society of Sisters*,[5] a law requiring initial instruction in English was struck down; in *Skinner v. Oklahoma*,[6] a law requiring the sterilization of certain kinds of criminals was overturned. In *Griswold v. Connecticut*,[7] which challenged a law prohibiting the use of contraceptives, the Court for the first time referred to the "right to privacy". The concept of privacy has since been extended to more controversial situations: *Cruzan v. Director, Missouri Department of Health*[8] (refusing medical treatment), *Roe v. Wade*[9] (abortion), and *Washington v. Glucksberg*[10] (assisted suicide).

Rubenfeld (1989) points to the identification of the right to privacy as a set of prohibitions and protections against totalitarianism. This view suggests that the protection of privacy and personal data constitutes rights that should be of concern not only to industrialized countries with strong democratic traditions. Some developing countries have suffered totalitarian regimes that were totally out of control. What kind of power would a deeper and more individualized knowledge of individuals give such regimes? Is not privacy the best protection against state persecution for minorities and dissidents?

In the continental tradition, the rights to intimacy and to one's own image are closely related to the concept of defending one's honour. The first clear reference to the protection of intimacy is found in the *Lex Cornelia de iniuris* (AD 81). Most current legislation considers the right to personality as a fundamental right (Peña González 1996).

Osvaldo Gozaíni (2001) offers some interesting thoughts about the history and process by which these rights took shape. "In current terms, the concern for intimacy is the result of a long historical process of the transformation of

conscience, beginning with the counter-reformation and on through the critique of religious conscience by the philosophers of the 18th century (Hobbes, Locke, Descartes, Spinoza), culminating in the construction of the moral conscience, begun by Thomasius and completed by Kant. It is man's freedom that allows him to judge his actions for himself and to determine his will on the basis of his innate inclination to morality. Juan Manuel Fernández López adds that this concept of man gives meaning to the current notion of intimacy as a necessary attribute of his new status of freedom–autonomy. The duality of the individual (as both internal and social being) is translated into a two-way intimacy that relates both to self (*ad se*) and to others (*ad alteros*). Intimacy, while it relates primarily to an individual's own, private space, acquires its full meaning only vis-à-vis others, against whom it is defended or with whom it is shared. Thus, intimacy is simultaneously a condition of the individual personality and of the social personality." Gozaíni maintains that while Europe pursues the defence of the individual through rules that specify the limits of the state and of individuals in the handling of data, the United States has essentially no constitutional policies on this issue: it has left it to the courts to review acts that may violate the right to privacy (for example, by including abortion within the intimate sphere of the woman), a process that led in 1994 to the Privacy Act. Similarly, the distinction that Europeans make between the data rights of individuals (ownership of data) and the rights of those who handle or administer those data (databases) seeks to expand the field of individual rights and limit the use of data in the possession of businesses, unless they have the owner's consent to use them for a specified purpose.

American jurisprudence, which is broad and generous in this area of fundamental rights, reveals a successive pattern of protections that began with the famous "right to be left alone", went on to address relations with the press and the communication media, and culminated with the protection of data that are compiled in computer format.

The work of Alberto Bianchi (1995) shows that in the United States the protection of the right of privacy embraces many cases and a large body of doctrine, although the problem always revolves around the concept to which Justice Louis Brandeis gave expression when he said that privacy signifies "the right to be left alone". Of course, Bianchi adds, if we go back to the origins of the right to privacy, we will find, in the first place, that it is a typically Anglo-American concept. Its history can be divided into four periods for methodological purposes. The first runs from the origins of the Common Law until 1890, when Warren and Brandeis published their celebrated article (1890). The second period extended to the essay published in 1960 by William Prosser and focused primarily on emerging issues of privacy and press. The third period, where the focus on privacy shifted from the United States to England, begins with the draft law prepared by Lord Mancroft and deals primarily with the conflict between privacy and the mass media. Finally, the fourth period begins in 1969 with the draft Walden Act, which for the first time raised the problem of ownership over personal data stored in computers.

In US legal history, the right to privacy is intended to protect individuals' feelings and sensitivities and not their property or their financial interests, and so it is seen as a personal right that ends with death.[11] It has been noted, for example, that criminal records for minors (which are protected) can be opened if a person dies under unexplained circumstances. This viewpoint is not shared in the continental system, where intimacy and privacy are linked to honour (Cifuentes 1995).

Another clear aspect of the continental tradition is that there is no privacy for "legal" or "moral" persons, i.e. corporations. The Supreme Court in Venezuela has repeatedly declared this (e.g. in *Inversora Bohemia II CA and Valores HB*). By contrast, in the case of *Collymore et al. v. General Attorney* in Trinidad and Tobago, the Privy Council maintained that this right did extend to *de facto* corporations, such as labour unions.[12]

Status of legislation in the region

International instruments

Table 1. International instruments relating to the rights of privacy and intimacy

1948	American Declaration on the Rights and Duties of Man (Articles II, III and XXII)
1948	Universal Declaration of Human Rights (Preamble, Articles 2.1, 16 and 18)
1948	Convention on the Prevention and Punishment of the Crime of Genocide (II)
1966	International Covenant on Economic, Social and Cultural Rights (Articles 2.1, 13.1, 13.3 and 17)
1966	International Covenant on Civil and Political Rights (Articles 2, 4 and 20).
1967	International Convention on the Elimination of All Forms of Racial Discrimination (Article 5)
1969	American Convention on Human Rights (Pact of San Jose) (Articles 1, 11, 12, 13.5, 16, 22.8 and 27
1980	Guidelines of the Organisation for Economic Co-operation and Development (OECD) on the Protection of Privacy and Transborder Flows of Personal Data
1989	Convention on the Rights of the Child (Preamble, Articles 2, 14, 16, 20, 29, 30 and 40.2.VII)
1990	United Nations Guidelines concerning Computerized Personal Data
1995	Directive 95/46/CE of the European Parliament
1998	Universal Declaration on the Human Genome and Human Rights (Articles 5 and 7)
2000	Optional Protocol to the Convention on the Rights of the Child concerning the sale of children, child prostitution and child pornography (Article 2.c)

Legislative trends

Some countries' legislation contemplates different systems of access, or limitations, to personal databases, depending on the type of file involved. However, the question is difficult and requires further debate. In surveying current trends in the protection of personal data, we start with Directive 95/46/EC of the European Parliament and the Council of Europe, of October 24, 1995, "on the protection of individuals with regard to the processing of personal data and on the free movement of such data", which reads:

> SECTION 1. PRINCIPLES RELATING TO DATA QUALITY
>
> Article 6.1. Member States shall provide that personal data must be:
>
> (a) processed fairly and lawfully;
> (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
> (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
> (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
> (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.
>
> 2. It shall be for the controller to ensure that paragraph 1 is complied with.

The rights of intimacy and privacy in the Americas

Some American countries have legislation of a general nature for protecting privacy and personal data. In Canada, the Privacy Act (1983) replaced an earlier set of rights contained in Part IV of the Canadian Human Rights Act. The objective of the Privacy Act was to provide better protection from the impact of new technologies and the growing tendency of government to create information systems. This law enhances transparency and gives Canadians greater control over personal data stored in government systems.

The regulations require the government to:

- limit the collection of personal information to that which relates directly to government programmes or activities
- collect information directly from the person to whom it relates, wherever possible
- inform the person why the information is requested and how it will be used
- not to use the information for any other purpose, except as permitted by law
- retain the information in such a way that the person to whom it refers has a reasonable opportunity to obtain access to it
- ensure that the information is accurate, up-to-date and as complete as possible
- not release personal information except where this is permitted by the Privacy Act or other legislation

In the United States, privacy rights are not spelled out in the Constitution but are considered to fall under its "penumbra", i.e. they are implicitly provided by constitutional principles.[13] In successive judgements, the Supreme Court has held that the Fourth and the Fourteenth Amendments protect individuals from certain kinds of invasion in their private life. Currently, there are many provisions regarding privacy scattered throughout the US Code.

The Constitutions of Colombia, Brazil, Argentina and Peru contain generic protection that in some cases is distilled in legislation or regulations. Article 5 of the 1988 Brazilian Constitution establishes the right of *habeas data*:

> TITLE II. FUNDAMENTAL RIGHTS AND GUARANTEES
>
> CHAPTER I. INDIVIDUAL AND COLLECTIVE RIGHTS AND DUTIES
>
> Article 5. All persons are equal before the law, without any distinction whatsoever, and Brazilians and foreigners resident in Brazil are assured of inviolability of the right of life, liberty, equality, security, and property, on the following terms:
>
> XXII. The right to habeas data is granted: a) to ensure knowledge of information relating to the person of the petitioner, contained in records or data banks of government entities or of public entities; b) for the correction of data, if the petitioner does not prefer to do so through confidential, judicial, or administrative proceedings.

Equivalent prescriptions are to be found in the 1991 Constitution of Colombia (Article 15), the 1993 Constitution of Peru (Article 200.3) and the 1994 Constitution of Argentina (Article 43).

Several countries already have specific legislation for protecting the rights of intimacy, privacy and personal data: Argentina (2000), Brazil (1997), Chile (1999), Ecuador (1997), Dominican Republic (1997) and Venezuela (1991). In most cases they are intended to regulate habeas data. In a few cases, such as Mexico and Uruguay, parliamentary initiatives are now under discussion.

Comparative analysis of national standards

Table 2: Legislation on privacy and intimacy

Argentina	
	Civil Code (Article 1071 bis)
1997	Financial Institutions Act (Law 21,526, Articles 39 and 40)
1997	Judicial Procedures Act (Law 11,683, Article 101 on Fiscal Secrecy)
1990	AIDS Prevention Act (Law 23,798)
1994	Constitution of Argentina (Articles 18, 19 and 43) and treaties incorporated into the National Constitution with the reforms of 1994, as they refer to the protection of private life
1995	Mediation and Conciliation Act (Article 11)
1998	Credit Cards Act (Law 25,065, Article 53)
1999	Ethics in the Exercise of Public Duties Act (Law 25,188, Articles 10 and 11)
2000	Personal Data Protection Act (Law 25,326)
2000	Alimony and Child Support Registration Act, Province of Neuquén
2001	Act Creating the National Registry of Haematopoietic Progenitor Cell Donors (Law 25,392)
Brazil	
1964	Law No. 4595 (Article 38)
1996	National Tax Code (Law No. 5172, Article 198)
1978	Constitution of the Federal Republic of Brazil (Article 5)
1990	Code of Consumer Protection and Defence (Articles 43, 44 and 45)
1990	Statute of the Child and the Adolescent (Articles 10.1, 17, 240, 241 and 247)
1996	Telephone Tapping Law (Law No. 9296)
1997	Law Regulating the Right to Access to Information and Governing Habeas Data Procedures
Chile	
1928	Decree 950 of 1928, Article 10, supplemented by Decree 516 of 1988, on the Commercial Information Bulletin
1967	Law 16,643 on Misleading Advertising
1980	Political Constitution of the Republic of Chile (Article 19, Paragraph 4).

Continued on the next page

Table 2 continued

1993	Law 19,223 on Computer Crimes
1994	Decree 1137, Regulating the National Disabilities Registry (Law 9284)
1999	Law 19,628, Protection of Personal Data
Costa Rica	
1929	Political Constitution of the Republic of Costa Rica (Articles 38 and 24)
1989	Constitutional Jurisdiction Act (Law 7135, Articles 2, 15, 29, 57 and 66).
1978	Criminal Code (Article 196).
1989	Constitutional Jurisdiction Act (Articles 2,15, 29, 57 and 66)
1995	Law Against Sexual Harassment in Employment and Education (Article 23).
1995	Creation of the 911 Emergency Call System (Law 7566, Article 13).
1996	Constitutional Reform (Article 24 and 26) (Law 7607, Article 1).
1996	Juvenile Criminal Justice Act (Articles 20, 21 and 99)
1996	Law on Equal Opportunities for Persons with Disabilities (Article 40).
1996	Code of Criminal Procedures (Articles 181, 196 and 295)
1998	National Statistics System (Law 7839, Article 10)
1998	Code of Childhood and Adolescence (Article 25)
Dominican Republic	
1962	Law on Freedom of Expression and Thought (Articles 41 to 45)
1965	Banking Act (Articles 31 to 34)
1994	Political Constitution of the Dominican Republic (Articles 8.9 and 8.10).
1994	Code for the Protection of Children and Adolescents (Articles 66, 67 and 237).
1997	Criminal Code (Articles 336 to 338, as amended by Law 24-97).
1998	Telecommunications Act (Articles 5 and 6)
2000	Resolution 36 of the Dominican Telecommunications Institute (INDOTEL) (Articles 1 to 9).
2001	Law No. 11-01 on the Enforcement of Tax Obligations (Article 3, Paragraph I).
Ecuador	
	Criminal Code (Articles 197 and 213)
1974	Judicial Functions Act (Article 201)
1992	Special Telecommunications Act (Law No. 184), Article 14.
1996	Minors Code (Article 168)
1997	Constitutional Control Act (Articles 24 and 45 on Habeas data)
1998	Political Constitution of the Republic of Ecuador (Article 23.8)
2000	Code of Criminal Procedures (Article 69.6 on the Rights of the Accused)

Continued on the next page

2000 Act to Reform the Disabilities Act (Article 14 on the National Registry of Disabilities and General Regulations to the Disabilities Act of February 4, 1994, Articles 51 and 52)
2001 Financial Institutions Act (Articles 88 to 94) Draft Law on Electronic Commerce, Electronic Signatures and Data Messages

El Salvador

1972 Labour Code, Article 406
1983 Constitution of the Republic of El Salvador (Articles 2 and 6)
1994 Code of Civil Procedures, Article 156 Notaries Public Act, Article 11.
1994 Young Offenders Act, Articles 5 and 30
1994 Family Court Act, Article 215.
1995 Transitional Law on the Registration of Family Status and Marriage Contracts, Articles 3 and 17
1997 Criminal Code, "Calumny and Injury" (Articles 177 to 183) and "Crimes relating to Intimacy" (Articles 184 to 191)

Jamaica

1962 Constitution of Jamaica (Chapter III, Titles 19 and 22)
1992 Banking Act (Title 45 and Table 4)

Mexico

1917 Federal Constitution (Articles 6 and 7)
1917 Law on Crimes relating to Printing (Articles 1 and 9)
1990 Credit Institutions Act (Articles 112 bis, 117 and 118)
1990 Financial Conglomerates Act (Article 33) Act to Protect and Defend Users of Financial Services (Articles 13, 14, 15)
2001 Draft Federal Law on the Protection of Personal Data, sponsored by Senator Antonio Garcia Torres, PRI

Trinidad and Tobago

1921 Act Establishing the Registrar General (Sections 4 to 6)
1925 Children's Act (Section 87)
1952 Statistics Act (Sections 8 and 9)
1955 Alcoholic Beverages Sale Permits Act (Section 57)
1960 Private Hospitals Act (Section 8)
1960 Food and Drugs Act (Table 2)
1965 Police Services Act (Sections 37 and 111)
1978 Firearms Act (Section 29)
1980 Constitution of the Republic of Trinidad and Tobago (Section 4(c))

Continued on the next page

Table 2 continued

1999	Freedom of Information Act (Section 29) and Freedom of Information Act (Amendment)
2000	Act Establishing the Registrar General (Amendment) (Section 3)
2000	Integrity in Public Life Act (Section 2 and Table)
2000	Computer Abuse Act (Part II, Sections 3 to 10)
2000	DNA Identification Act (Sections 39 and 40)
2000	Electronic Funds Transfer Crimes Act (Section 20)
2000	Draft Telecommunications Act (Sections 24, 65 and 80)
Uruguay	
1988	*Acción de Amparo* (Appeal for Constitutional Protection) (Law 16,011)
1997	Constitution of the Republic (Articles 7 and 29)
2000	Draft Law on the Right to Information and Habeas data
2000	Draft Law Creating the National Registry of Alimony Debtors
2000	Draft Law Regulating Credit Bureaus and Similar Information Databases
2000	Draft Law Regulating the Use of Databases
2000	Draft Law Creating a Special Form of Civic Registration for Persons with Physical Disabilities
2000	Draft Law on Individuals or Corporations Administering, Managing or Obtaining Information from Any Database
2000	Draft Child and Adolescents Code (Articles 11, 22 (f) and 211 to 215)
Venezuela	
1999	Constitution of the Republic of Venezuela (Articles 48, 60, 143 and 283.1)
1977	Transfusions and Blood Banks Act (Article 24)
1979	Criminal Records Act (Articles 2 and 6)
1991	Communications Privacy Act
1998	Resolution 2001-06-98 of the Superintendency of Banking
2000	Law on the Protection of Children and Adolescents (Articles 50, 65 to 68, 139, 227 and 228)
2000	Telecommunications Act (Article 190)
2001	Decree Law on Data Messages and Electronic Signatures
	Draft Public Defender Act

Conflict of rights

Most judicial cases involving violations of intimacy or privacy are decided by weighing the interests at stake. There are at least three possible scenarios:

- Conflict between fundamental rights.
- Weighing collective rights and interests.
- Weighing private rights and interests.

Conflict between fundamental rights: Freedom of expression

The most interesting example of a conflict between fundamental rights occurs with freedom of expression. In a recent Declaration of Principles on Freedom of Expression, the Inter-American Commission on Human Rights, during its 108th regular session, declared:

> Privacy laws should not inhibit or restrict investigation and dissemination of information of public interest. The protection of a person's reputation should only be guaranteed through civil sanctions in those cases in which the person offended is a public official, a public person or a private person who has voluntarily become involved in matters of public interest. In addition, in these cases, it must be proven that in disseminating the news, the social communicator had the specific intent to inflict harm, was fully aware that false news was disseminated, or acted with gross negligence in efforts to determine the truth or falsity of such news.

The question has been addressed in a number of judicial cases. Perhaps the most significant was that resulting from publication in Argentina of a book entitled *Impunidad diplomática* (Diplomatic impunity) (Martorell 1993). The book was banned in Chile, and that decision was "confirmed" by the Supreme Court.[14] The case was brought before the Inter-American Commission on Human Rights, which finally recommended to the government of Chile that it allow the book to be distributed and sold freely.[15] In its statement of reasons, it said: "The Commission considers that it is not for the Commission to examine the content of the book in question or the conduct of Mr Martorell, because it does not have competence in the matter and because the right to honour is duly protected under Chilean law. Moreover, as the proceedings in the instant case show, those persons who believe that their honour and dignity had been impugned have, in the Chilean courts, adequate remedies to settle the question. For that reason, the Commission cannot accept the Chilean government's argument that the right to honour would be higher than the right to freedom of expression" (Fuentes Torrijo 2000: 427).

Freedom of expression has been given a different connotation in recent years, thanks to the attitude that newspapers have adopted with respect to the Internet. The current tendency is for newspapers to post their daily headlines and lead stories on their web sites, and to offer facilities for searching their previous editions. The search engines can look for news on the basis of personal names, which means that any news story containing such a name becomes in effect indefinitely accessible.

For analyzing the situation, there are a number of judicial decisions in the United States examining the loss of privacy rights, in particular for individuals who are categorized as "public figures". The California courts have also held that "public figures" are entitled to a "zone of privacy".[16]

The US Supreme Court has pointed to the conflict between freedom of the press and privacy rights in two precedent-setting judgements: *Cox Broadcasting Corp. v. Cohn*[17] and *Florida Star v. BJF*.[18] In both cases, the Court held that the First Amendment does not allow states to claim privacy when the press publishes truthful information legitimately obtained from public documents or proceedings involving matters of public interest. In assessing a public figure's claim for damages resulting from invasion of privacy, the courts have ruled that a famous person has to some extent lost the right of privacy.[19]

Williams (1999) maintains that the standard of "newsworthiness" used by the courts to evaluate claims for invasion of privacy is not sufficiently clear for editors to be reasonably able to avoid lawsuit and argues that the courts should analyze: (i) the social value of the facts published; (ii) the extent to which the article ostensibly intrudes into private matters; and (iii) the degree to which the person involved has placed himself in a position of public notoriety.

These concepts suggest two categories of public persons. "Voluntarily public persons" are those who have placed or exposed themselves before the public's gaze through their activities or through assuming a prominent role in institutions or activities of general public interest. Such considerations have been applied to actors,[20] professional athletes,[21] politicians,,[22] musicians, performers and cartoonists,[23] to deem them "public figures". It is argued that the public has a legitimate interest in obtaining information on voluntarily public persons and that this information may extend to aspects that for other persons would be private. In contrast, "involuntarily public persons" are those who have not sought public attention but who have become "news" as a result of their involvement or association with some event of public notoriety. This category includes, for example, victims of crimes or accidents, persons on trial for crimes or persons who have performed heroic acts. A person may become involuntarily public, and therefore lose a portion of his privacy, simply by the fact of being related to a person who is voluntarily public.[24] One relevant case for the definition of this category is *Kapellas v. Kofman*,[25] in which a newspaper published an editorial critical of Ines Kapellas, a candidate for elected office, referring to the fact that her son had been arrested and that her daughter had been found wandering the streets on various occasions. The Supreme Court of California ruled that the children had lost their privacy as a result of their mother's candidacy. The courts have also held that those who lose their privacy can never retrieve it.[26]

It is obviously very difficult to establish who are public persons and, among them who are voluntarily or involuntarily public figures. Latin American legislation would seem more restrictive in the concept of involuntarily public persons. The Ethics in the Exercise of Public Duties Act (1999) of Argentina includes an exhaustive list of public persons who are required to reveal their assets.[27] In Trinidad and Tobago, the list of "persons in public life" contained in the Integrity in Public Life Act (2000), Section 2 and the final table, is highly restrictive.

In *R.M.F.G. v. D.A.*,[28] the court ruled that "the rights to honour and to freedom of expression are of the same hierarchical order as fundamental rights"; and in *H.V.P.*,[29] "when there is a conflict of rights. . . between the freedom of expression and information and the right to honour and intimacy, there must be a weighing of interests. . . interference in another person's honour can be justified in the public interest, in the general interest. . . ".[30]

In the Common Law, establishing liability for damages deriving from the disclosure of private information requires that the information have been widely published and not confined to a few persons or to limited circumstances. In 1972, the Constitution of California was amended to provide privacy as an inalienable right of citizens.[31] Before that amendment, in *Hill v. National Collegiate Athletic Association*[32] and later in *White v. Davis*,[33] the Supreme Court of California defined the criteria for deciding invasion of privacy claims. According to those rules, plaintiffs must: (i) identify a specific and legally protected privacy interest, (ii) prove that the plaintiff had a reasonable expectation of privacy, and (iii) prove a serious invasion of privacy.

The supremacy of the freedom of expression is under discussion at this time in relation to the case of *Free Speech Coalition v. Reno*. The Child Pornography Prevention Act of 1996 prohibits the publication of any image that "appears" to show explicit sexual conduct by a child. In this case, the argument is over whether the law (the purpose of which is to protect children) applies to images created by software, in which no child has participated.[34] This is another interesting example of the difficulties in adapting juridical norms to technological changes. The case was accepted for consideration by the US Supreme Court on January 22, 2001.[35]

Weighing the collective interest

In *Vernonia School District v. Wayne Acton et ux*,[36] the US Supreme Court evaluated the Student Athlete Drug Policy that was adopted by the Vernonia School following the discovery that athletes were leaders of the drug culture among students because of concern that the use of drugs increases the risk of injury during sporting activities. The policy authorizes the taking of random urine samples from students participating in athletic programmes. James Acton was banned from the school football programme when he and his parents (also parties in the proceedings) refused their consent for such a test. They went to court, seeking an injunction and a corrective order on the grounds that the policy violated the Fourth and Fourteenth Amendments and the Constitution of Oregon.

The Supreme Court held that the policy was constitutional under the Fourth and Fourteenth Amendments. Whether a search meets the reasonableness standard "is judged by balancing its intrusion in the individual's Fourth Amendment interests against its promotion of legitimate governmental interests". The first factor to be considered in establishing "reasonableness" is the nature of the privacy interest, on which opposition to

the examination was based. The subjects of the policy are children who have been committed to the temporary custody of the state. As the school authority, the state can exercise a greater degree of supervision and control than it could over competent adults. The requirement that children in a public school submit to physical examinations and vaccination indicates that they have a diminished expectation of privacy with respect to medical examinations and procedures than the rest of the population. Student athletes have even less legitimate expectation of privacy, since by participating in athletic activities they expose themselves implicitly to a kind of "communal undress" and, moreover, athletes are subject to pre-season physical examinations and rules of conduct. The Supreme Court held that the Fourth Amendment does not require the "least invasive" search or examination, and therefore the argument that the analysis to determine drug use could be based on the suspicion of such use, even if proven, would not be decisive; it also pointed out that such an alternative presents substantive difficulties of its own.[37]

The ruling in *CODEPU v. Gendarmería de Chile y otro* (Supreme Court 1995) confirmed that installing microphones in prisons falls within the security measures contemplated by Decree No. 353 (2) of the Ministry of Justice. In this case, the court confirmed indirectly that public security takes precedence over privacy rights. The decision has been the subject of international debate.[38]

Normally, legislation and case law recognize the possibility of personal and documentary inspections when there are reasonable grounds to suspect that a crime has been committed. In Jamaica, in the case of *King v. the Queen*[39] (Privy Council 1968), it was established that Title 18 of the Constabulary Force Act does not state the terms under which a personal search is to be conducted and that Article 22 does not give a justice of the peace the mandate to authorize a personal search. The evidence against the defendant (during a search of Mr Herman King without his consent, marijuana was found in his trouser pocket) was obtained illegally and must be excluded. On the contrary, in Trinidad and Tobago, in the case of *D. Davidson vs. R. Williams and the Attorney General*[40] (Supreme Court 1988), the police obtained two warrants to search the plaintiff's house and to seize the documents mentioned in the warrants, which provided evidence that Title 4 (2a) of the Falsification Act had been violated. The plaintiff went to court arguing that the procedure used was illegal and unconstitutional, and seeking damages. The court rejected the claim that the plaintiff's rights under Title 4 (c) of the Constitution were affected.

Banking secrecy is treated in some legislation as coincident with the right to personal data. In the case of *Douglas and Others v. Pindling*,[41] the court ruled that the right not to have banking information disclosed without consent, established in Section 10 of the Banks and Trust Companies Regulation (Amendment) Act of the Bahamas, was superseded by the public interest. A similar decision was rendered in the cases of *Troy Megill v. General Attorney and Others* and *George Mayne v. General Attorney and Others*.[42]

Weighing the private interest

Access to credit is seen as a private interest that contributes to economic development, which is a collective interest. For many years, obtaining a loan, either in cash or for the purchase of goods, was preceded by the posting of collateral (personal pledge or a mortgage on the goods). These requirements were in effect a barrier to obtaining loans for consumption, particularly for people with few resources. With the appearance of centralized information systems (credit bureaus), it was possible to develop databases on credit backgrounds. These databases contain personal information and allow access to credit both for persons who have no negative history and for those who have a positive history. Their defenders maintain that the existence of these credit bureaus does away with the inefficiency and ineffectiveness of resorting to the judicial system in suits to recover money. There is a generalized tendency in many countries that only an insignificant number of suits result in payment of the debt (directly or through auction), while in the remaining cases the debtor's insolvency or other circumstances will mean that the case concludes without resolution. Today, the risk of being reported to a credit bureau provides a disincentive to defaulting on payment, since the "sanction" for default is immediate, permanent and internationally known.

This situation is a source of debate: some argue that credit bureaus should be administered by the state, while others consider that this is a proper activity of the private sector. In the United States, for example, the borrower must give written authorization for the lender to consult the bureau, while in Latin America, at least in most cases, merchants can consult the bureau directly without even telling the borrower that his personal data are being checked. In some cases, debts that have been paid pursuant to legal proceedings are registered, while in other cases such data must be eliminated.[43]

Many of these problems are resolved through specific legislation – which is virtually non-existent in Latin America – and by recourse to habeas data.

Access to information

One relevant point in analyzing the impact of new ICTs has to do with access to information – essentially, whether information is publicly accessible or restricted, and whether a person is guaranteed the right of access to his own information, which may include the possibility of correcting it or suppressing it. It is also relevant for the person to know that his information is being used and who is using it and for what purpose. The mechanism designed to protect these rights is habeas data.

With respect to habeas data a distinction is made between the form that protects the right to informational self-determination and the set of principles (equality, dignity, freedom) and rights (honour, reputation, intimacy, image, etc.) that can be violated by the handling of information – called the proper habeas data – and the extensive form that protects the right of access to public

information as the right to be informed in accordance with the republican principle that government acts are public. This distinction is merely a question of classification of the juridical goods protected. Nevertheless, both forms translate into certain powers that subjects may exercise for a variety of objectives, claiming subjective private rights in each case. Thus, a number of types and subtypes have been identified in doctrine (Sagües 1995).[44]

Informational habeas data covers access to records in order to know what information is stored, and it may be limited to this. Argentina, Brazil, Ecuador, Colombia, Guatemala, Peru and Paraguay make express provision for this, as does the Constitution of Portugal. One subtype within this category would be for the sole purpose of knowing what personal data are recorded, which may also include knowing certain specific public information, and is generally defined as the right of free access to sources of information, sometimes including the right to freedom of the press or of expression. Generally, this is limited when there is a state right to security. It is considered basic because it is the source of any other right to correct, suppress or request confidentiality for the data. Other subtypes relate to knowing the purpose (why and for whom the information was obtained) and the agent (identity of the person who sought and obtained the data).

Associative habeas data has to do with including a piece of information which, if excluded, would affect its owner and with clarifying any information contained. As an example with respect to credit bureaus, a person may request that an explanation be entered to the effect that he is not the principal debtor of an obligation, but rather the guarantor. The legislation of Argentina, Brazil, Colombia, Ecuador and Paraguay, as well as that of Portugal, provides for this expressly.

Remedial habeas data seeks to correct false, inaccurate or imprecise information as well as any other type of information that is so vague or ambiguous as to lead the reader to misinterpret it. For example, some databases may use expressions with a particular meaning that does not correspond to generally accepted technical use of the term (e.g. “disqualified debtor” in the juridical sense). Legislation in Argentina, Brazil, Colombia, Ecuador, Guatemala and Paraguay, as well as in Portugal, regulates this expressly.

Protective habeas data seeks to ensure that information is kept confidential and not disclosed to anyone. It is usually used for sensitive data that have to be stored, or for components of secret state data. Argentina, Peru and Portugal have constitutional provisions to this effect.

Habeas data of deletion seeks to eliminate data from files and is applied when preservation or confidentiality cannot be adequately protected (sensitive data, dangerous forms) or when further storage of the information makes no sense because it offers no benefit to society. This type is regulated in the legislation of Argentina, Ecuador and Paraguay.

To this point, the types and subtypes discussed are constitutionally recognized, but case law has also recognized other forms of habeas data:

- That used for challenging a mistaken interpretation of the information or of the decision stored.
- That used on a pre-emptive basis, until it has been decided whether the data should be retained or definitively cancelled.
- That used to de-personalize data or make it anonymous so that the subject referred to cannot be recognized. The right to security of data is the prevailing principle in this area, to the point that regulations require the use of technical measures to prevent unauthorized leaks.
- Habeas data is at times used for "assurance of security" purposes, where the court evaluates whether the proper technical means were used to prevent use of the data by unauthorized persons.
- The term *compensatory* applies to habeas data when seeking a court award of damages; and together with the "anonymous" form, it is always associated with other purposes, such as having the data furnished or corrected, or both.

Another point on which regulations differ relates to who is the active subject, an individual or a legal person. Depending on whether they include both categories or only the first, we may analyze the appropriateness of protecting one right or the other. If it is intimacy or privacy that is being protected, legal persons are not recognized and are excluded: the only aspect of legal persons that is protected is generally the economic one. In Spain, Germany, France and Ireland, in fact, such persons are excluded from protection. On the other hand, Switzerland, Austria, Denmark, Luxembourg and Norway provide protection with respect to the economic aspect. The United Nations allows contracting states to apply protection to legal persons (Puccinelli 1999).

Does protection cover only "sensitive data" or does it apply to all data? In some countries' legislation and case law, what must be protected is personal information referring to ideology, religion, colour, beliefs, etc., deemed to be "sensitive data" that if taken into account could imply discrimination and the violation of human rights. In other countries, however, it is considered that, with the cross-referencing of data and the absence of security as to their use, the speed with which computers can process information makes all data sensitive and therefore in need of protection.[45] Some countries' legislation enshrines the right to oppose the release of data (France) and may require consent to disclosure by the person involved (Spain). In the case of credit information, the debt must be certain, unpaid and already demanded by the creditor. In the case of private records, they must be registered and there must be proof that the data recorded there are accurate.[46]

Some countries, for example Argentina, Chile, Spain and Bolivia, have a specific law on habeas data. Others do not, although doctrine and case law generally apply other constitutional, legislative or regulatory norms to the same effect. Sometimes resort to constitutional protection is used, and on other occasions habeas data is sought (Pierini, Lorences and Tornabene 1999; Sosa 2000; Antik and Ramunno 2000; Slaibe and Gabot 2000).

Risks and violations

The most relevant disputes relate not so much to the accumulation of information in paper format, as the civil registries of nearly all countries have been doing without entailing violations, but rather to the automated processing of those databases and the power of search engines. In this respect, legislation has progressed furthest in Europe.

DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF EUROPE

SECTION II
CRITERIA FOR MAKING DATA PROCESSING LEGITIMATE

Article 7
Member States shall provide that personal data may be processed if:
(a) the data subject has unambiguously given his consent; or
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
(d) processing is necessary in order to protect the vital interests of the data subject; or
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

SECTION III
SPECIAL CATEGORIES OF PROCESSING

Article 18 The processing of special categories of data
1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.
2. Paragraph 1 shall not apply where:
   (a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or

(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or
(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or
(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or
(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.
4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.
5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority. Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority.
6. Derogations from paragraph 1 provided for in paragraphs 4 and 5 shall be notified to the Commission.
7. Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.

For purposes of classifying risks and violations, it is interesting to distinguish those that arise as a consequence of a database.

Primary generation of databases

Non-computerized archives are slow-moving and permanent, and errors in the data they contain can be recognized and corrected. Information processing systems – computerized databases – are swift, interconnected and impermanent, which means that errors cannot readily be corrected, a situation made all the worse by the speed with which they are disseminated and duplicated.

The generation of databases brings great benefits but also poses risks. To avoid these risks, a number of countries have established defence systems or protection models: (i) the judicial system (e.g. in the United States) which repairs damages after the fact – in these systems the role of surveillance bodies is merely supplementary; (ii) the administrative approach, in which the jurisdictional functions are given to government, is much used in Europe (Spain, Sweden, Germany), where specialized and independent bodies have been established with powers of sanction; and (iii) a mixed approach that seeks to strike a balance between the administrative and the judicial models. Here, control and protection mechanisms can be both preventive and repressive.

We must distinguish public records from private records. Public databases are those kept by government agencies and are normally reserved or secret. Examples of laws that govern such databases are Argentina's Law 11,801 on the Registry of Real Property; Law 22,617 on the Registry of Recidivism and Criminal Statistics; and Law 17,622 on INDEC (National Statistics and Census Institute), which refers to secret information collected for statistical purposes.

This raises the question: Who are the persons who are bound to fulfil the requirements imposed by law, and against whom the protective mechanisms (preventive or penalizing, i.e. establishing liability for damages) are applied? Brazilian and Guatemalan regulations restrict such application to public databanks or registries, while Colombia, Argentina, Peru and Ecuador extend it to private databases.

When it comes to defining and administering an information system, the fundamental principle is that of the end or purpose. Any information system has a purpose, and it must be designed to achieve that purpose and not to be used for any other. That purpose must be explicit. For example, the 1980 Liquor Licenses Act of Trinidad and Tobago reads: "For the purposes of this Act, every holder of a hotel spirit license or special hotel license under this Act shall keep a register in which . . ." There must be time limits (5, 7, 10 years) set for keeping the information in the database for that purpose.

The rights protected by these regulations, which are sometimes mentioned by the law and in other cases are deduced by judicial interpretation, are very broad. In some countries they apply to all personal rights: the right to life, intimacy, privacy, name, dignity, honour, integrity, freedom of conscience, virtual personality, personal data, informational self-determination. The Council of the European Union speaks of "protection of freedoms and. . . of the right to intimacy as regards the processing of personal data". This is also

known as the "right of domain over personal data" and is beginning to be considered as an autonomous and very personal right. In Argentina, several rulings and doctrines, regarded as innovative, consider this right to derive from human dignity, mentioning that it goes beyond intimacy or image alone to embrace honour and identity. "It derives from a technological and social phenomenon".[47] It may be called "a highly personal right to personal data", "a right to informational self-determination", "to information processing freedom", "a highly personal right of domain over personal data".

Administration of justice

The point of departure is that the administration of justice must be transparent. Indeed, the publication of proceedings and decisions is one of the pillars of the system, and the knowledge of precedents ensures respect for the principle of equality before the law (Cadoux 1994). In this sense, the information that originates or is processed judicially or administratively may differ in identity and value. Nevertheless, the information that is normally included in information systems can be distinguished as to procedural or jurisprudential.

Systems for monitoring legal cases are strictly necessary for the efficient administration of justice. The books of registry of the courts have gradually been replaced by computerized systems that are increasingly centralized. These systems not only record great quantities of personal data but also make it possible to relate individuals acts, conflicts of interest or crimes. There is also a growing tendency to create electronic files that can record virtually all the information relating to the case (including victims, witnesses, attorneys and experts). This is clearly a way to ensure the universally desired prompt and efficient administration of justice. All computerized court records (except judgements) should be considered confidential, and their purpose must be restricted to the administration of justice. Justice systems must therefore provide a secure guarantee that the data will not be manipulated or deleted. The visual inspection of files and hardcopy documents must not be restricted, except as the law may provide.

Court records have been used for certain purposes that may constitute violations:

- Companies that sell information on credit histories may obtain and use records from commercial rulings.
- Job recruiters may petitition the labour courts to reveal whether a candidate for employment has brought labour claims.
- Petitions of a similar nature may be filed to the civil courts, for example to verify whether a potential tenant has a record of past evictions.

In all these cases, the intent is to predict future conduct, on the assumption that a person who was party to a dispute or who exercised his rights in the

past is likely to do so in the future (Cappelletti and Garth 1988). While judicial information is public, information systems created for the purpose of facilitating the administration of justice should not be used to serve the interests of third parties unrelated to the case in question.

The situation with judicial rulings and access to case law is different. Public knowledge of precedents guarantees the principle of equality for all citizens before the law. For this reason, and except where the law determines otherwise, judicial decisions must be public and all possible measures must be taken to make them accessible (Rotunda 1995).

This issue poses some difficulties. Court rulings contain a great deal of personal information and reveal facts that fall within the private sphere. The aim of guaranteeing equality before the law does not require that data be accessible through a search engine, but it is desirable that decisions be exposed to public scrutiny – for example in the press – and that they be appraised or criticized. Many law reviews and web sites quoting judgements have begun to take precautions. Certain personal data will be selectively removed (generally the names of the parties to the dispute and those of the witnesses, attorneys and perhaps the judge), the assumption being that what is important is to reveal the rationale and the essentials of the decision and not to identify the parties to the dispute. In the end, once a ruling is identified by its juridical content (i.e. of fact or of law), the personal data can nearly always be accessed by applying to the court and requesting the record of proceedings. The kind of search that should be avoided is one that seeks to identify court cases in which a specific individual is involved.

The tendency to suppress personal data reflects a balance between the rights of intimacy and privacy and those of equality before the law: in some cases, personal names are replaced by initials, and in other cases portions of the ruling are suppressed if they are not part of the fundamental decision (e.g. the fees paid for attorneys and experts). Nevertheless, the fact of suppressing personal data carries a significant additional cost. Online reviews and case law providers are divided on this point. Some eliminate names only in certain cases, others in all cases (e.g. *Aranzadi* in Spain). There are also providers who eliminate only those names that the law specifically prohibits and who allow the use of names in search engines (e.g. the Court of Justice of the Federal District and Territories in Brazil, the Costa Rican Juridical Information System, and in the United States the publishers Lexis and West Law). On March 8, 2001, a motion was brought before the Court of Appeals of Santiago relating to the search function of a recently inaugurated web site <http://www.poderjudicial.cl>, where upon introducing her name in the search system (for checking the status of pending cases) the person found that it produced data on a paternity suit she had brought with respect to her daughter.[48]

Health information

In the health field, the creation of databases or information systems containing medical prescriptions or facilitating access to personal clinical data could be considered a risk. Access to such information has sparked controversy, particularly because it may be based on discriminatory notions or attitudes. Justice W. Brennan of the US Supreme Court, in an opinion in the case of *Whalen v. Roe*, 429 US 589,607 (1977), where the plaintiff challenged the constitutionality of a New York State law requiring the compulsory registration of all medical prescriptions in a centralized database, wrote: "The central storage and easy accessibility of computerized data vastly increase the potential for abuse of the information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology." The situation has not changed much. The recent Health Security Act in the United States recognizes the need for strict rules to administer information without harming privacy. It sets forth the following principles: (i) defined and limited circumstances under which consultation of medical records is authorized; (ii) "minimum necessary disclosure" of medical records; (iii) the "right to know" who has information on a person; and (iv) the "right of access" to that information, and to be notified of any corrections or modifications (Shapiro and Annas 1994).

It has also been noted that marketing firms will purchase used medical prescription forms from pharmacies and enter them in databases for use in statistical analysis of drug use trends. While the names of patients are not recorded, the names of their physicians are, and the list showing their preferences will be used for calls by drug salesmen. The clients for this service are large pharmaceutical laboratories.

Databases of clinical histories, blood donors[49] and vaccinations have become commonplace in recent years, although the information is sensitive and should be protected. Many hospitals have also begun to post clinical histories on the Internet.

A person's condition as a carrier of HIV, the AIDS virus, may require special privacy protection. In Argentina, the AIDS Prevention Act (Law 23,798 of 1990) provides that "in no case may individuals be identifiable through forms, records or stored data, which must to this end be kept in codified form", and "the system used must be limited to the initials of the person's name and surname, and the day and year of birth". For example, when judicial records make mention of an HIV carrier, that person's name is replaced by a number, and this is true for paper records as well. By reason of this law, the legal review *El Derecho* publishes judicial cases without revealing even the HIV carrier's initials, using instead the letters N.N. The Supreme Court of Venezuela has defined its position on AIDS and privacy in *N.A. and Others*".[50]

In *N.N. v. the State*,[51] moral damages for discrimination were awarded a public employee suffering from AIDS, even though the results of the test were not disclosed, because the state, his employer, had failed to fulfil its

duty of maintaining confidentiality. The amount of damages was set at US$14,000, certainly the highest such award that we found during our research on Latin America.

Chile has presented a case that was difficult to remedy legally. Vivo Positivo is a self-help organization for HIV carriers. The list of its members fell into the hands of a funeral parlour, which sent out letters to every member inviting them to use its services. To prove that the law had been violated, the plaintiffs would have to show that the firm sent letters of this kind to HIV carriers more frequently than to other persons. Statistical evidence of this kind is non-existent in Latin American courts.

In the insurance field, health information can be used to assess the risk of contracting diseases or for predicting life expectancy. For this reason, such information could be used by insurance companies to refuse coverage for life insurance, medical assistance or retirement benefits.[52]

Genetic databases are sure to pose a problem for the future (Annas 1999; Roche 1996). Trinidad and Tobago passed the DNA Identification Act in 2000 for creating a personal genetic database, compulsory for persons who have been convicted by a court of appeals[53] and for those agreeing to register.

Information related to children

There is a strong tradition in Latin American legislation to protect the names and images of children and adolescents from publication in the press, especially if they are victims or perpetrators of crime.[54] Yet some countries have deemed it advantageous to equip their child protection agencies with information systems to store personal data on health, violations or situations of risk for children in their care. The rationale for such records is that they allow for individual monitoring, which is certainly of benefit to the children, and can be used for statistical studies and research for planning and designing policies.[55] Nevertheless, the systems have failed to strike a proper balance between such objectives and the need for protection of personal data (Gregorio 1999). Nor has sufficient attention been given to the security of those systems, and there are no clear criminal penalties for persons who violate data security and confidentiality.[56]

In *S., V. v. M., D.A.*,[57] the court ruled that, when there is a conflict between a child's right to intimacy and the right to freedom of expression, judicial protection of the child's higher interest must be strictly limited to what is indispensable, so as to avoid unjust restriction on freedom of the press, since that freedom, which allows the publication of news of concern to the community as a social and cultural body, requires that restrictions, sanctions and limitations be imposed only by law and in accordance with a restrictive interpretation.

Adoption procedures are generally secret and in some countries documents relating to biological parentage are destroyed, yet the Internet has sites devoted to tracing biological links.[58]

School records also present the possibility for discrimination. In the United

States, disciplinary measures for violating school rules are considered a part of school records and are protected by the Family Educational Right to Privacy Act.[59]

There are generally few disputes over violations of children's privacy by their parents, yet the state telephone company in Uruguay (ANTEL) published an advertisement in which it highlighted, as one use of the caller identification feature, the possibility of "controlling the friendships of an adolescent child". Several countries, including France, have legislation establishing an age beyond which children have a degree of privacy from parental supervision. The Venezuelan Child and Adolescent Protection Act establishes rules on the confidentiality of correspondence. In the United States, there are web sites offering the possibility of detecting drug consumption on the basis of a hair sample, which is generally taken by the parents without the adolescent's consent.[60]

Other databases compile information on adults that is related to children. In the United States, there are national databases with personal data on "deadbeat dads", fathers who have shirked their child support obligations. These databases interact with banking institutions to restrict such persons' transactions. This practice has been sharply criticized (Schwartz 1992). In Argentina, legislation is under consideration to create a National Registry of Alimony Debtors, something that already exists in some provinces.[61] In the United States, several states have databases on suspected child molesters.[62]

Other state records

The civil registries, perhaps the oldest form of public records, were generally based on "indexes" that were annexed to each registry book (typically covering one calendar year). This system offered an efficient search mechanism, but it was limited in the sense that the user had to know the year and the place of the event (e.g. a birth, marriage, death). The conversion of the civil registries into computerized, centralized databases would allow for searches into parentage, homonyms and other areas that could violate or threaten privacy.

Voters' lists contain personal data, including some that are extremely sensitive, such as affiliation with a political party (as in Argentina). We also found that some countries (e.g. the Dominican Republic and Venezuela) have created web sites that can display personal information for a specific identification card number.

Criminal records hold data on confirmed judgements and are governed by specific rules in most countries, where they are administered by the state and treated as confidential. Nevertheless, this information is highly sensitive and there is a risk that these records could be replaced by police records of arrests. In El Salvador, juvenile delinquency legislation prohibits the police from keeping records of this kind on children and adolescents.

People's international movements are increasingly being recorded. The old paper forms are being replaced by new optical recognition devices and passports and other personal identification can now be read automatically.

Border-crossing records contain sensitive personal data and information on private life. The "purpose" of maintaining these databases is not clear.

In Ecuador, the National Narcotics and Psychotropic Substances Control Council (CONSEP) keeps a database of crimes under the Narcotics and Psychotropic Substances Act.[63]

A decision of the Venezuelan Supreme Court in the case of *R.C.M. y otros v. Consejo Nacional Electoral* (2000) is highly significant, as it establishes a limit on the concept of transparency in state information and on the concept of habeas data: "What the plaintiffs are seeking is not access to administrative files and records, but the provision of computerized electoral information complete with the results obtained at each and every polling station, broken down station by station." This decision means that transparency and the right to information do not imply the right to access or search computerized state records, since the purpose for which they were developed relates solely to state functions. Thus, there is no right to obtain copies of public records. The 1999 Freedom of Information Act of Trinidad and Tobago and the US Freedom of Information Act of 1996 give citizens the right (with some exceptions) to access official documents. Section 30 of the Trinidad and Tobago law excludes documents that could affect personal privacy, as well as other documents for *raisons d'état*. In *Bruno F. Villaseñor*,[64] the court ruled that the right to information enshrined in the last part of Article 6 of the Federal Constitution is not absolute but is limited by national interests and those of society, as well as by the rights of other parties (e.g. to privacy).

Records on persons with disabilities and their families

Some countries (e.g. Chile, Ecuador, Mexico, Uruguay) maintain records on persons with some form of disability. In some cases these are official and in others they are kept by self-help associations (e.g. the Down's Association of Uruguay). Inclusion in these registries implies eligibility for certain social benefits or subsidies. Yet such databases can also be used for purposes of discrimination, or to restrict eligibility for life insurance or private pension systems (as in El Salvador).

Personal identification systems

Personal identification (ID) systems are now able to store great quantities of information that far exceed what is needed for identification purposes, and the owner of the ID document may not even be aware that such information exists. In Venezuela, the government is about to introduce a new system of ID documents. While the details have not yet been announced, the government's call for tenders included provisions for an enormous database of fingerprints and a remote-readable chip to be inserted in the ID documents. A document of this kind will be issued to newborns in Malaysia, with a memory chip that includes an ID number, name, name of parents and citizenship status.[65]

Information that is illegible to the document's owner is found in the form of bar codes on the ID documents of Costa Rica and the Dominican Republic. In the Philippines, the so-called social security ID card has not only a bar code that includes fingerprints but also a magnetic device that allows the owner's social security contributions to be read in "information kiosks" and that in future will allow transactions at automated teller machines.[66]

Credit risk information systems

The lack of clear legislation to regulate this activity no doubt translates into violations of the rights to privacy and intimacy. The ideal rule would be to require credit bureaus to verify every piece of data entered in their records, but this information is normally received informally from their clients, with no substantiating documentation. On this point, it is interesting to analyze the case of *Hoffman Fuenzalida, Luis v. Boletín de Informaciones Comerciales*, which raises a very important point.[67] By releasing the credit bureau from any form of civil liability for erroneous information, and transferring that liability to the institution that provided the data, the court was in effect removing all incentive for the bureau to concern itself with the quality of information. It would certainly seem contradictory that the Supreme Court of Costa Rica, in *Félix Przedborski v. Mauricio Herrera y La Nación* (2001), should insist that the truthfulness of a source in Belgium be verified and that links to a site in that country be eliminated (thereby limiting freedom of expression) and yet it should not be a requirement for a credit bureau to verify the truthfulness of information, in light of the rights to privacy and intimacy. This situation should surely be rectified.

Another situation of risk arises in the lack of effective control over the information contained in credit bureaus' databases. We noted that several of these databases not only contained credit information but also other kinds of data that were not necessarily obtained in a legitimate way (criminal records, labour judgements, traffic violations, consumption profiles, etc.), and we also found cases of personal vendettas involving the entry of false information in the victim's database (del Villar, Díaz de León and Gil Hubert 2000; Miller, 2000).

Workplace monitoring

In the workplace, the employer can monitor his employees' telephone conversations with clients for reasons of quality control. In some cases, there must be a recorded message or special tone indicating that the conversation is being recorded or monitored. In the United States, the Electronic Communications Privacy Act, 18 US Code 2510 et seq. (the federal law that regulates interstate communications), allows for the unannounced monitoring of calls. Internal calls between employees can also be monitored. The employer can have access to the record of telephone calls made from a specific extension. Magnetic disks, e-mail and voicemail can be monitored, and video

cameras can be stationed at selected places.[68] Privacy in the workplace is thereby substantially reduced, with the justification that all this monitoring will enhance productivity, prevent theft, avoid civil liability for employees' acts and prevent industrial or commercial espionage. One of the few exceptions is to be found in the Employee Polygraph Protection Act of 1988, which prohibits lie detector tests.

It is difficult to draw a clear line between the private information of the employee and that of the employer, but in extreme cases these practices may amount to violations of intimacy and privacy. To prevent such conflicts, some employers have established their own internal rules.

There is also debate as to whether an employer can require an employee to submit to medical tests (e.g. for HIV) or psychological examinations. In many cases, the employer insists that these are justified on grounds of security.

Nevertheless, the Supreme Court of the Dominican Republic, in *Agromán Empresa Constructora SA v. BP*,[69] held that there can be facts of a personal nature that relate exclusively to an employee's private life and not to his work.

Database by-products

Telephone services

Telephone companies keep a list of calls received and calls made for individual telephones. These data can be processed and can provide information on a person's private life. While there is no record of violations or complaints relating to these databases, they have been used pursuant to a court order in criminal investigations (as in the investigation of the murder of José Luis Cabezas in Argentina).

Caller identification systems do not represent a direct invasion of privacy. Nevertheless, if the owner of the telephone uses that system to identify calls received by other people (e.g. in hotels or by parents with respect to their children), this could possibly be considered a violation. As well, we noted that some companies that receive service requests by telephone use the caller identification system to generate databases on their clients. For example, radio taxi firms keep historical files on the date, time and destination of trips.

In some countries (e.g. Jamaica and Uruguay) the debt status (service billings) of a telephone company's customer can be obtained simply by knowing his telephone number. In Jamaica there is an automated service for this purpose, available by dialling 1-919-1919 (Roxborough 1999); and in Uruguay the owner of a telephone line can be identified at public terminals in the telephone company's offices.

As a result of the Communications Assistance for Law Enforcement Act, telephone companies in the United States will have to equip their mobile phones with geographic positioning systems accurate to within 50 metres, for intelligence purposes (by the Federal Bureau of Investigation or FBI) and

for tracking emergency (911) calls. Even without such devices, it is possible to locate a cellular phone to a fair degree of accuracy in densely populated areas, by identifying the nearest antenna: in large cities antennas are placed at distances of a few tens or hundreds of metres.

Credit cards

Companies that issue credit cards have databases that can not only reveal a person's purchasing profile but also locate him in time and space. Some of them use this information in real time to prevent fraud. We have not detected any violations with respect to these databases, presumably because those companies maintain adequate security and confidentiality. In terms of legislation, we may cite the Credit Cards Act of Argentina (Law 25,065 of 1998), which prohibits the provision of information to credit bureaus.[70]

Consumer profiles

Many businesses regularly request personal data for compiling a "customer profile". Such information can even be requested for cash sales. These databases are shared and combined with those generated by other businesses, and they can result in invasions of privacy, such as new-product offers by mail, telephone, e-mail, etc.

There is now widespread use of lotteries and competitions for which entrants must complete a coupon with personal data. Those data are stored and processed and can be used or sold to telephone marketers.

Risks not related to databases

Communications

Telephone eavesdropping in many countries constitutes a violation of the rights to intimacy and privacy. There is an important distinction to be made here, depending on whether the wiretap is ordered by a judge or is conducted by the police or other security forces, or is requested by private individuals.

Legislation dealing with such violations has been adopted in Ecuador (Special Telecommunications Act, Law 184 of 1992, Article 14); in Venezuela (Telecommunications Act, 2000, Article 190); and in the Dominican Republic, where Supreme Court Resolution 80 of 2001 instructs judges, in cases relating to Resolution 36-00 of the Dominican Telecommunications Institute (INDOTEL), to "consider as illegal telephone interception any direct or indirect interference, interception, intervention, reception, ordering, permission, espionage, listening and provision of means, for one's own account or that of another, without prior warrant of a court". In Mexico the Supreme Court ruled, in the case of *Fernando Koram Valle y otro, amparo directo*,[71] that "if the telephone interception was not preceded by a court order, it is an unconstitutional act

and it and the fruits thereof are automatically null and void". In Jamaica[72] the legality of a police wiretap in the course of investigating a crime is considered to be regulated by the precedent of *Malone v. Commissioner for the Metropolitan Police* (No. 2).[73]

Decisional law also tends to reject evidence (from telephone wiretaps) that has been obtained illegally. In the Argentine case *In re Sergio F. Lazica*,[74] the court ruled that the transcription of a telephone conversation had no validity or effectiveness because it was spurious evidence obtained surreptitiously and therefore represented a direct violation of the guarantee of privacy enshrined in Articles 18 and 19 of the Argentine Constitution.

When it comes to intercepting communications by persons deprived of their liberty, the situation may differ: in Brazil it is considered illegitimate and a violation of the right of defence, while in Chile it is considered legal to place microphones in prison cells for security purposes.

Internet

In the context of the Internet, there are certain techniques and practices that violate privacy, even though in principle they may appear inoffensive (Vibes 2000). "Spam" consists in sending e-mail messages to a long list of persons, generally for advertising purposes, but can also involve circulating chain letters, petitions, etc. Some e-mail providers have introduced spam filters, although this could itself be seen as a further intrusion.

"Cookies" consist of pieces of information that a web server can store on the user's computer in order to record "favourites", for example. The user is generally unaware of the presence of these cookies and of the fact that his visits to a certain site or, thanks to browser errors, his Internet activity as a whole may be tracked.

There are no clear or universal rules on the allocation of domain names, and so we find cases of "cyber squatters" who make a practice of registering the names of celebrities or companies as domain names, for the purpose of selling them or discrediting the person or company. In some countries, the courts deal with these situations on a case-by-case basis, while in others (e.g. Uruguay) the company that allocates domain names reserves the right to withdraw them if it considers that they are being abused in this way.

The web sites of some government agencies allow access to personal information by simply entering an identification number. Examples are the sites of the Central Bank of Argentina <http://www.bcra.gov.ar/sesfaaaa.htm>, the Internal Revenue Service of Ecuador <http://www.sri.gov.ec/html/ruc_consulta.html>, the National Elections Council of Venezuela <http://www.cne.ve/donde.asp>, and the Central Elections Board of the Dominican Republic <http://www.jce.do/consultas/index.asp>.

Other forms of invasion of privacy

In many countries we found that the information contained on automobile licence plates bore no strict relation to the purpose for which they were created. For example, including the owner's place of residence is excessive information and reveals a personal fact that could generate an additional risk (e.g. becoming the target of a robbery). This is a problem in Brazil, Mexico and Uruguay.

There are also other violations that show that the concept of intimacy and privacy has broader implications. In *Szwec, Andrés v. Carrefour Argentina SA*,[75] the court ruled that Carrefour had violated the privacy of the plaintiff because an error on its billing and receipt documents, which reproduced his telephone number, caused him to be disturbed at home by calls from people trying to reach the supermarket. He was awarded damages of US$3,500. In *João Rodrigues v.Viernes Entretenimiento CA*,[76] the court declared that "an environment with significant noise levels is prejudicial to health and disruptive of intimacy". In *Julia Vanessa Castro Sánchez v.Tercera Comisaria y otros*,[77] the court said that "the fact of photographing a person passing along the public way, even without that person's consent, does not constitute a crime; although the court considers that, pursuant to Articles 29 and 30 of the Civil Code and Article 24 of the Constitution, it would be a violation of that person's constitutional rights to personality and privacy if the photographs were published, reproduced, exhibited or sold without that person's consent, except in the cases listed therein relating to public notoriety or the needs of justice or the police". In *Rischmani Grinblatt, Francisca v. Consorcio Periodistico de Chile SA*,[78] the court found that "the fact of attending a public place does not imply consent for the release of a photograph taken in that place".

Devices and technologies that invade privacy

Current technology, supported in large part by the constant increase in computer power and information storage capacity, is giving rise to extremely powerful surveillance devices and procedures. The following are some of the best known.

The FBI admitted that it was using a product called Carnivore,[79] developed for the purpose of "bugging" e-mail traffic within the United States (incoming and outgoing), which automatically selects messages that appear suspicious.

Global positioning systems (GPS, GLONASS) allow the position of an object or a person to be located within a few metres anywhere on the planet.[80] This makes it possible not only to conduct accurate land surveys but also to determine the exact position of an escaped prisoner or a lost child. Bracelets are now in use that integrate GPS with cellular phone networks or radio

receivers for relaying positions. Thus, it is possible to track a fugitive or to confirm whether a house arrest or a restriction order is being observed. The company Digital Angel <http://www.digitalangel.net> developed technology for implanting a device of this kind in the human body: body heat generates the needed electricity, and the device allows the wearer's pulse and temperature to be monitored. Although the company presented it as an excellent way of supervising children and the elderly, its market studies showed that the public is still leery of this kind of implant, and so the company decided to postpone its launch until the market is more receptive. Meanwhile, it is working to develop externally-carried versions of the device.

For the March 12, 2001, elections in Uganda, the government decided to use face recognition technology to combat electoral fraud. The task was undertaken by the US company Viisage Technology Inc. <http://www.viisage.com>, which was awarded a contract by the Ugandan government to record the faces of approximately 10 million persons eligible to vote in the country. Recording the faces involved converting photographs into 128 vectors representing facial characteristics, including nose profile, lip thickness and the distance between the eyes. This task was conducted during the voting process.

The US government will pay US$500 million[81] to the digital telephone industry to introduce "back doors" to facilitate intelligence work. This and other initiatives, such as adding tracking functions to cellcular phones, are being undertaken in accordance with a law approved by the US Congress in 1994, known as the Communications Assistance for Law Enforcement Act .[82]

The Dutch government recently carried out an investigation for the European Parliament to confirm the existence of Echelon. This is a massive espionage organization run by the United States, Great Britain and other Commonwealth countries that can overhear and filter communications of all kinds (voice, data, etc.) by intercepting microwave and satellite transmissions, using powerful information extraction tools and a vast network of satellites and antennas, at least in the United Kingdom and the United States. The European Parliament formed a special committee to study this case, on the basis of numerous complaints and demonstrations of its existence. Apparently this organization has been used to conduct industrial espionage against countries of the European Union.[83]

In a study published in April 2000,[84] the American Management Association found that the proportion of US companies engaged in some kind of active surveillance over their employees rose from 45 percent in 1998 to 74 percent in 1999. E-mail monitoring rose from 27 percent to 30 percent over the same period.

The International Data Corp. (IDC) estimates that, worldwide, corporations spend some US$62 million on Internet monitoring and filtering software. One study by IDC predicts that such spending will reach US$561 million by 2005.

Reordering ideas

The evolution of rights (legislation) has often gone hand-in-hand with technological development. Automobiles have become steadily more powerful and more widely used since they were first introduced. And since their invention (and that of the railway), there has been conflict between the benefits they offer and the consequences or risks that they present. Although the rights to life and personal integrity were sufficiently established before the invention of the automobile, accidents began to increase significantly.

It is important to note that, despite the severe criticism and the apocalyptic forecasts that were made about the risks inherent in the automobile, the first changes in legislation were to adjust and expand the scope of legislation on damages. The intent was to provide financial compensation for violations of the rights to life and to personal integrity. While legal rules governing automobile traffic were being developed, such policies alone were incapable of reducing the number of accidents and of deaths and injuries. In fact, legislation introducing vehicle safety and performance standards probably had more to do with this. And yet, more than any laws and traffic regulations, it was liability lawsuits against manufacturers (e.g. the Ford Pinto case) that finally forced them to come up with safer automobile designs.[85]

This analogy shows once again the tardiness or failure of legislation in creating effective protection for rights and its inability to control or hold back technological developments. We may say that safety improvements were due more to technological solutions (safer designs) than to any laws or regulations protecting rights. Swiftly changing liability legislation and the ability of the courts to deal with new situations were strong incentives for regulating the automotive market.

There may be a certain analogy with the protection of privacy and intimacy rights. But in this case, is it sufficient to leave it to civil liability to provide the incentives that will bring order to the new ICTs? We must remember that the automotive industry developed first in countries that had very strong civil liability systems. Today, information systems are making the fastest progress in developing countries, where there are virtually no established systems of civil liability nor any tradition of suing for damages and, in those cases that reach the courts, the amounts of compensation are insignificant compared to the profits to be made from marketing personal data. We need only mention that in Latin America punitive damages do not exist – or they are not provided for in existing legislation – while in the United States awards for such damages amount to billions of dollars (Alterini and Filippini 1986).

Rethinking personal data

In analyzing the purpose of an information system and evaluating the risks of invasion of intimacy and privacy, we need to identify some data categories.

Statistical data

Information that is used only to compile statistics and to conduct research or monitoring, does not have to reveal the names of the parties involved (except perhaps for the government or parties on which multiple files are kept). The most important consequence is that the information that is included for these purposes alone can be protected by "statistical secrecy". The rules governing statistical information usually impose certain obligations on individuals and legal persons to provide data. As a counterpart, they are guaranteed a degree of confidentiality, meaning that no individual's data will be disclosed or published that could be used to identify that individual. Publication of the data will be limited to conventional statistical techniques.

Reference data

Reference information contained in the system makes it possible to access or process documentary and personal identification for management purposes.

Documentary data

Information of documentary value is used to support sound decision-making. If the parties, for example, can obtain information on a court decision or a notification by consulting the information system, that information must have documentary value. For all data classified as documentary, there must be an assurance that the information cannot be modified, or that any change to the data will leave a trail identifying who modified it and when.

Registration data

The most important characteristic of this information is its legal effects and its completeness: in a registration system, the absence of information has documentary value. The principles governing registration and the management of registries are: (i) rogation: the registry does not act of its own accord but at the request of the interested party, through intervention by the administrative authorities or pursuant to a court order; (ii) any document registered can be contested; (iii) there is a presumption of truth in registered information; (iv) the registry must examine documents diligently and ensure that those registered meet the applicable legal standards.

Little has been said about the role that information plays in decision-making. On this point, we may cite France's Law on Data Processing, Data Files and Individual Liberties.[86]

> LAW 78-17 OF JANUARY 6, 1978, ON DATA PROCESSING, DATA FILES AND INDIVIDUAL LIBERTIES
>
> Article 1: Data processing must be at the service of each citizen. Its development must be pursued within the realm of international cooperation. It must not infringe either on human identity, or on human rights, or on private life, or on freedom whether individual or public.

> Article 2**:** No judicial decision involving an appreciation of human behaviour may be based on automatically processed information purporting to define the profile or the personality of the interested party. No administrative or private decision involving an appreciation of human behaviour may be based solely on automatically processed information purporting to define the profile or the personality of the interested party.

Government policies

Historically, the law has created mechanisms not to limit technological developments but to regulate them, to establish a system of incentives, and to create criminal and civil liabilities. This was the case with the automobile, which gave rise to acceptance of the inherent social risk and the payment of personal damages. Disputes of this kind are rarely resolved by legislation. In most cases, the result is a set of rules based on precedents.

Nevertheless, there is a need for a coherent set of public policies to govern the generation of information systems and the protection of personal data. General legislation should establish that the creation of any information system for storing personal data must be preceded by a needs analysis, a risk analysis and an explicit statement of purpose. The personal information stored must be the minimum necessary to that purpose.

There is also a requirement for public policies to control the processing of personal data, in both the public and private spheres. The control authority function may be exercised by a specific official or body (e.g. Spain's Data Protection Agency), or it may be assigned to the public defender or ombudsman.[87]

Explicit public policies must be defined relating to the need for information systems containing personal data and to their storage, transfer and accessibility. These policies must be dynamic and must be based on an analysis of new developments and new violations. The objective of these policies should be to overcome the incapacity of general legislation to resolve unforeseen situations.

The supervisory body must investigate complaints and violations, and it must verify that information systems have an explicit purpose, that the information collected is the minimum required to meet that purpose, that the systems respect security standards proportionate to the risks involved, and that in the case of private systems they are covered by civil liability insurance.

Services offered over the Internet must be carefully analyzed, and search mechanisms should be developed that make it possible to exclude personal data.

Technological solutions

Security in the Internet environment

The Internet's construction as an open communication system not only makes it interoperable but also renders it vulnerable to certain risks, including surreptitious intrusion, such as hacking, and human error. We may identify three kinds of inherent risks. Programming errors or "bugs" and problems caused by configuration errors on web servers that allow unauthorized remote users to steal documents and to obtain information on the computer providing the web server function so that the system can be penetrated. There are also risks in navigator or browser programs that may result in improper use of personal information provided with or without the knowledge of the user. Using traffic "eavesdropping" techniques, data sent between the browser and the server can be intercepted.

These weaknesses may be exploited innocently or deliberately. Recent incidents have included the penetration of the database of an electronic commerce company and the theft of thousands of credit card numbers (Ward 1997). A recent survey published in the United States indicates that there are five serious attacks every month on electronic commerce web sites.[88]

The US Department of Defense reported that 80 percent of its sites had been penetrated and that in 1996 alone there were 250,000 attempted intrusions into its computers.[89] Such vulnerability suggests that critical information should not be exposed over the World Wide Web. In other words, the kinds of information stored in equipment that is accessible over the Internet should be kept to a minimum, and critical data should be strictly segregated from the rest. This could include horizontal selection of information, such as removing a certain class of cases from a judgements database, or vertical selection, such as removing the names of the parties from all cases or from a certain class of cases.

Some possible techniques for enforcing privacy on the Web[90]

Labelling and licensing technologies

Labelling technologies license the use of symbols called *trustmarks* to online merchants through an ongoing programme of certification and auditing. Auditing conducted by well-respected firms will ensure the integrity of the trustmarks and strengthen consumer confidence. By clicking on the trustmark symbol, the individual can read the web site's privacy statement. At a minimum, the site should reveal what type of information it collects, how the site uses that data, with whom the site shares that information, whether the individual can opt out of having the data used by that site or a third party, whether the data can be changed or updated by the individual, and whether one can delete or deactivate one's data from the web site database. One example of this type of firm is TRUSTe <http://www.truste.com>.

Blocking technologies

A technology known as PICS, or the Platform for Internet Content Selection, developed by Massachusettts Institute of Technology's World Wide Web Consortium (W3C), will attach labels to describe any document on the Internet or any web site. In browsing the Web, an individual will not be able to enter those sites which he or she has set as being undesirable. In addition to labelling offensive material, the technology can also describe a web site's information practices, such as what personal information it collects and whether that information is reused or resold.[91]

Data exchange technologies

An example of this type of approach is the project developed by W3C, called P3P, short for Platform for Privacy Preferences.[92] Once implemented, P3P would permit web sites to state their privacy practices, based on a specified set of statements about how they would use, transfer, disclose and allow access to personal data collected by them. The user would also create a set of privacy preferences. If the web site's practices and the user's preferences matched, there would be seamless access to that web site. However, if a match could not be achieved, the user could negotiate with the web site (though the possibility exists that a user could be denied entry if not enough personal data was volunteered to the site).

Anonymous profiling

An alternative approach to collecting personal data over the Internet is anonymous profiling. While demographic information would still be released under this scheme, personally identifying data would not. In other words, the data would not be linked to a subject or associated with a particular name.

Encryption

Although many of these technologies and applications are still in the developmental stage, what can be said with some assurance is that there is a growing consensus that digital signatures and encryption will form the basic tools for electronic transactions. Encryption is needed to ensure security, including authentication,[93] confidentiality, data integrity and non-repudiation.[94] Several forms of electronic encryption exist, with public key encryption being strongly favoured, often in conjunction with the use of single-key systems.

The most extensive use of this system is PGP, "Pretty Good Privacy" <http://www.pgp.com>. The system encrypts the message using a single key that is generated at random for each procedure and is in turn encrypted with a public–private key mechanism. In other words, the public key is used only to encrypt and the private key only to decrypt the message. In this way, the decryption key remains in the sole possession of the information addressee. This type of encryption uses keys with up to 2,056 characters that would take thousands of years of processing time to break, given the current state of the art.

Digital signatures

Digital signatures are needed to authenticate the parties to an online transaction, just as handwritten signatures affixed to paper documents authenticate the identity of the individuals involved. Unlike handwritten signatures, however, digital signatures are transferable, and that transferability needs to be managed and contained to retain the system's reliability.

A digital signature resembles a pseudonym more closely than a real name because it is a secret piece of information that one possesses, which is then linked to an individual's name. This leads to two central risks associated with its use: (1) initial impersonation at the time of certification of the digital signature (the risk of false attestation); and (2) the "secret" information, namely the digital signature, being duplicated outside of the control of the bona fide individual (the risk of theft, misuse or loss).

The existence of these risks has sparked the development of new authentication technologies: biometric authentication (such as by fingerprints, voiceprints, retinal scans, iris scans, hand geometry, facial thermograms, etc.). Paradoxically, these techniques create a whole new world of possible violations of privacy.

Secure transmission

These applications provide secure transfer of information between a browser and a server through the use of encryption. Two competing standards exist: Secure HTTP and Secure Sockets Layer (SSL). The drawback to these technologies is that they allow the web site to decrypt the transmitted information, opening the door to the possibility of fraudulent use.

Credit card transaction protocols

Using public key cryptographic techniques and digital signatures, the Secure Electronic Transactions (SET) protocol, developed by Visa and MasterCard, mimics the current credit card processing system. Its advantage is that it does not permit the online merchant to read the credit card information. In any case, the entity issuing the card knows and certifies movements.

Electronic cash or virtual money

Electronic money or e-cash is predicated on a different strategy in order to be used over an open network like the Internet. The strategy is to avoid sending personal data, as is the case with credit card information, but rather to send electronic cash or tokens, with the individual providing no identifiable personal data over the Internet. With one form of this technology developed by David Chaum (Chaum, et al. n.d.: 319–27), the individual remains completely anonymous.

There are various versions that embody this idea, but they fall essentially under two systems: (1) hardware-based stored-value cards or smart cards and (2) software-based stored-value or prepaid payment systems for executing payments over open networks. The former are hardware or card-based

systems that permit individuals to use plastic cards with a magnetic strip or a smart card embedded with a computer chip; the latter are software- or network-based systems that work with installed software through a personal computer connected to a network.

There are two basic ways to represent the value of the funds stored: balance-based, in which a single balance is stored and updated with each transaction, and note-based, in which electronic notes, each with a fixed value and serial number (comparable, for example, to a real banknote), are transferred from one device to another. These values are encrypted when transmitted in order to ensure confidentiality and data integrity. In one instance, a note-based technology developed by eCash Technologies Inc. <http://www.digicash.com> uses a "blind signature" where the process ensures that no identifying information may be traced back to the individual.

Security at computer centres and other physical elements

Although great stress is placed on protecting communication between remote computers, most thefts of information in fact are done in "the old way", i.e. by directly accessing the equipment where the records are stored. This means that attention must be devoted to preventing intrusion, theft and tampering of the equipment, as well as to installations and activities such as those involved in computer centres, information transport, backup information, extractable storage devices (floppy disks, CD ROM, etc.), notebooks, printers and desks.

Royal Decree No. 994/1999[95] of the Spanish government offers sound criteria for the security of physical elements, classified by the level of security.

Technology for controlling the use and handling of data

Distributed information systems

A distributed information system consists of two or more distinct information subsystems that cooperate with each other. Each subsystem is capable of processing locally stored data. Data stored for remote access or for centralized maintenance purposes must be stored in accordance with a global conceptual scheme, on which a common database scheme is designed. According to Date 86, it is helpful to think of a distributed system as a partnership among a set of independent but cooperating centralized systems.[96]

Distributed systems contribute to the protection of privacy and offer the capacity to apply different levels of security to personal information on the same individual. In this way, for example, a database with demographic and identification data can be vertically partitioned and the two parts physically separated so that identity data are stored under extremely strict security conditions while demographic data, with a lower level of security, are available, for example, for research.

The main risk to individual privacy lies in the high degree of integration of information systems today. In other words, it is possible to monitor an individual's behaviour in different areas, thanks to the capacity to cross

information of all types: what the person is buying, to whom he calls or writes, whether or not he is in debt, whether he is ill, etc. It is the high degree of integration of all this information that provides real power. Dispersing it effectively will facilitate the erection of barriers that determine which subsystems can collaborate and what information can be crossed, for purposes of protecting privacy.

Authentication technologies

A key principle, and one that must be observed for any security policy, is that of responsibility. In other words, it must be possible to identify who is responsible for each action conducted in digital space. This calls for correct identification, which in turn requires proper authentication. There are three conventional types of authentication: (i) something that the user knows (a password), (ii) something that the user has (a key, a smart card), and (iii) something that the user "is" or "does" (biometrics). Although it is simple and widely accepted, knowledge-based authentication is vulnerable to dictionary-based intrusion and "brute force" attack by trying all possible character combinations.

Biometrics narrows the line that separates identification methods from authentication methods. There are two main phases in biometric authentication. In the enrolment phase, a certain characteristic of the user is measured. This may be a physical characteristic such as his fingerprints, his hand geometry, the configuration of veins in his retina, the pattern of the iris, facial geometry or DNA, or it may be a behavioural characteristic such as his voice or the dynamics of signing his name. In any of these cases, current technology makes it possible to analyze and extract a numerical representation (e.g. in the form of vectors) of the characteristic. This can be so refined as to express the differences between any two faces. To authenticate the person, the characteristic must be measured again and the numerical result compared with that stored in the first phase. The person is then authenticated, depending on how close the newly calculated value is to the stored value.

While these authentication systems are highly advanced and accurate, it must be noted that biometric identifiers are not keys. For example, they cannot be hidden, changed or destroyed. The uniqueness of biometric identifiers, the fact that they cannot be transferred and cannot be lost or forgotten, gives them an advantage over knowledge-based systems. But, as noted earlier, they pose a new risk to privacy, so they must be handled and stored with great care and used only for purposes authorized by the individual involved.

Handling notifications

After taking all security measures deemed necessary and applying authorization and authentication policies as appropriate to the classification of the information being handled, we must consider the possibility that these precautions will be evaded. It is very important, then, to minimize the time during which an intrusion goes undetected. To achieve this, records must be

kept of all activities involving the system conducted by any of the users who have a right to the information. These records, besides providing a means of tracking damage, can be inspected automatically so as to detect patterns that suggest a possible intrusion into the system, for example successive failed attempts at authentication. The system administrator or the security officer must then be notified, so that he can investigate what may be a serious situation. As well, the system must provide warning of especially delicate or suspicious transactions, such as copying, downloading or massive modifications of information.

Conclusion

Whenever the protection of privacy and personal data is sacrificed, the rationale is based on resolving a conflict of interests: public safety, combating drugs, freedom of the press (Budano Roig 1998), where the balance is tipped against privacy and intimacy. It is clear that there are no general rules that can be established by the legislative route: the issue falls clearly in the terrain of the courts, which are asked to dispense justice in individual cases.

What we have at the moment is a number of disparate criteria applied within state organs with respect to the access that should be given to information collected in the course of their activities or contained in private databanks. It is certain, as well, that the volume of such information and the means of accessing it will continue to grow, as will the demand for information, whether for legitimate or other purposes. It is highly advisable, therefore, to consider legislation to cover the situations discussed here and to define general principles that would apply to the computerization process.

Such legislation must be compatible with and supplementary to laws that determine the scope of habeas data, which is still not regulated in some countries, since in principle nearly all information in the public sphere is publicly accessible. Guidelines are needed, however, to strengthen the position of the citizen, who currently finds himself defenceless in terms of the use that may be made of this information. Data collection should be subject to limits in the form of some standard rules that require demonstration of the need for the data and the purpose for which it is to be used, as well as the identification of those who are entitled to request such information.

The process of creating data processing systems should be transparent and accessible to all. Government agencies working with databases should maintain contact with independent institutions and non-governmental organizations that can provide expert advisory services and convey the opinion of specific sectors. Risk analysis should examine the effects and consequences that data processing systems can have on society.

Legislation should prevent stored information from generating or permitting any form of discrimination or prejudice, for example the compiling of data on religious beliefs, political opinions, sexual attitudes, ethnic origin, disabilities, etc. Time limits should be set on how long the data are to be

kept, and procedures for deleting them should be defined. Freedom of information does not imply or excuse the indiscriminate disclosure of data, nor does it mean converting the public administration into an information service. Legislation should establish those cases where information on an individual can be supplied to third persons.

There is a need for some policy decisions in this area, either to open state information to any user while allowing individuals to place reservations on their information or, on the contrary, to restrict access to those who can demonstrate a legitimate interest. Clear definitions in this area are needed for the proper development and efficiency of information systems, as well as for public information services and government registries and, in particular, for the statistical processing of data.

Search engines facilitate the task of obtaining information and for this reason they are recognized as very useful; yet they are the principal technological weapon that can be wielded against privacy rights. However difficult this may be to arrange, search engines should be designed to "jump over" personal data: this will mean segregating information that relates unequivocally to a given person within a computerized registry (either textual or structured).

Self-regulation has proven successful in similar areas, and therefore, we feel in light of the cases described and until there are explicit rules or policies in place that the design of information systems should seek to maintain the balance between, on one hand, publicity and transparency in state activities and the legitimacy of private activities that involve the accumulation of personal data, and on the other hand the protection of privacy and intimacy for individuals (and in particular for those in the most vulnerable groups).

Today, this balance is assured by recent trends in the protection of personal data:

- The principle of "end purpose"
- The principle of proportionality (the data must be adequate, relevant and not excessive)
- The requirement that data must be obtained and handled legally and legitimately
- Right of access to the information (the right to know, before it is processed, what personal information is involved and how it is to be processed, transmitted and transferred to other people)
- The right to know to whom one's personal data have been transferred
- The right to oppose the processing of one's data, on legitimate grounds
- The right of rectification of personal data
- Specific action to enforce habeas data
- Deletion of records when they have ceased to be necessary or relevant to their purpose
- Statistical secrecy
- Existence of an authority to supervise and protect personal data

- Strict control over organizations that market personal data
- Severe penalties for those who violate the rules and those who steal information

A number of different policies are needed to strike the desired balance. The growing tendency of the state, and frequently the legislature itself, to create databases and registries is the source of many of the violations that occur today. There should be a set of rules establishing requirements for their creation and conditions for their operation, including measures to ensure confidentiality and security. In the words of Leggiere (1998), many risks or violations are the result of "ignorance" about the power of these new technologies.[97] Nor should we forget that the protection of privacy is a protection against totalitarian systems.[98]

In the private sector, there is a need for laws to govern specific activities, such as credit bureaus, credit cards, banks, telephones, and clinical records. These laws must seek to balance economic interests against the rights of privacy and intimacy. Among their key elements are that: (i) the assignment of civil liability must be designed as an incentive to protect fundamental rights; (ii) there must be suitable watchdog agencies; and (iii) database managers should be required to adopt strict security measures. In regulating these activities, it is essential that the courts keep abreast of new technological developments and that they offer ready and effective access to habeas data.

The most difficult problem relates to the Internet, particularly when freedom of expression is involved, as in online newspapers. The Internet today is governed by the laws of the market,[99] and in fact it has subverted some of the conventional market disciplines. This makes it very difficult to enforce respect for human rights on the Internet. It will be important to analyze the evolution of the right to freedom of expression,[100] in particular the decision that the US Supreme Court is to render in the case of *Free Speech Coalition v. Reno*.[101] While there may be a growing move to self-regulation on the Internet, the web sites that pose the greatest risk are those that manage to evade all regulation.

Notes

1. Camille Sutton also took part in the preliminary research and in the preparation of this paper. The authors are also grateful to Nuria Castañer, Francina Díaz, Elena Highton and Nelson A. Vaquerano for their help in revising the paper and for the country studies they contributed.
2. This process may be seen as a new and qualitative leap in the expansion of the human memory. For centuries, human beings have sought to extend and protect their memory. The earliest cave paintings, icons, oral transmission, printing and (to some extent) art and history – all were mechanisms of memory support. Man has created countless systems for keeping records, but his main problem has been to find mechanisms for searching those records. Thus,

indexes could be used to search paper records. But there are other procedures, as well: for example, in agrarian communities of Bolivia, when an agreement was reached on the boundaries of a farm, it was indicated with stone walls, but this symbolic delineation was not considered sufficient, and a powerful system of recording the event was added: small children were brought to the place and beaten with the boundary stakes – they would thus retain for many years a vivid memory of the place where the markers had been set. It is in fact the search mechanisms that signify the expansion of memory. Perhaps the most interesting innovation in the creation of search engines was that developed by Sigmund Freud. The psychoanalyst can be seen as a search engine, allowing an individual to dig deep into his own memory. It is search engines that are transforming the concept of memory and that have made individuals more vulnerable.

3. We also examined some situations in Canada, Spain, the United States, France and other countries of the Americas, including El Salvador and the Bahamas.
4. It was Justice Louis Brandeis who coined the expression "the right to be left alone", in *Olmstead v. US*, 277 US 438.
5. 268 US 510 (1925).
6. 316 US 535 (1942).
7. 381 US 479 (1965).
8. 497 US 261 (1990).
9. 410 US 113 (1973).
10. 521 US 702 (1997).
11. See 62A American Jurisprudence 2nd Privacy 25. An exception in common law would be Section 30 of the Freedom of Information Act of 1999 of Trinidad and Tobago, which protects the privacy of dead persons.
12. 12 WIR 5 and 15 WIR 229.
13. *Griswold v. Connecticut*, 381 US 479 (1965).
14. *Luksic Craig, Andróico v. Editorial Planeta*, Supreme Court, June 15, 1993. "The author of the book 'Diplomatic Impunity' has committed an arbitrary and illegal act that has signified deprivation, disturbance and threat pursuant to Article 19 (4) of the Constitution, by revealing facts that belong to the private and intimate life of individuals. The appeal for protection was accepted and the book was banned from entry and distribution in Chile." On the issue of censorship, see Article 19 (12) and Article 1 of the Constitution.
15. *Francisco Martorell v. Chile*, Case 11,230, Report No. 11/96, Inter-Am. C.H.R., OEA/Ser.L/V/II.95.Doc. 7 rev. p. 234 (1997). "The Government of Chile has pointed out that the rights to honour and dignity often conflict with freedom of expression, that the State must endeavour to balance these rights with the guarantees inherent in freedom of expression, and that a right may be sacrificed for the sake of what is considered to be a higher right."
16. See *Diaz v. Oakland Tribune Inc.*, 188 Cal. Rptr. 762, 772-73 (Cal. Ct. App. 1983).
17. 420 US 469 (1975).
18. 491 US 524 (1989).

19. *Carlisle v. Fawcett Publication Inc.*, 20 Cal. Rptr. 405, 414 (Cal. Ct. App. 1962).
20. *O'Hilderbrandt v. Colombia Broad. Sys.*, 114 Cal. Rptr. 826, 830 (Cal. Ct. App., 1974).
21. *Cepeda v. Cowles Magazines and Broad.*, 393 F. 2d 417, 419 (9th Cir. 1968).
22. *Miller v. Bakersfield News-Bulletin*, 1919 Cal. Rptr. 92, 94 (Cal. Ct. App. 1975); *Yorty v. Chandler*, 91 Cal. Rptr. 709, 712 (Cal. Ct. App. 1970).
23. *Star Editorial v. United States District Court*, 7 F. 3d 856, 861 (9th Cir. 1993); *Montandon v. Triangle Publication*, 120 Cal. Rptr. 186, 191 (Cal. Ct. App. 1975).
24. As defined in *Carlisle*, note 19.
25. 459 P. 2d 912 (Cal. 1969).
26. In *Sidis v. F-R Publishing Corp.*, 113 F. 2d 806 (2d Cir. 1940), the plaintiff was a child prodigy who had gained notoriety by graduating from university at the age of 17. Twenty years later, a magazine published a story contrasting those early achievements with his current life. The court ruled that the article did not violate his privacy because he continued to be a public figure.
27. For example, a former Vice President of Argentina, Carlos Alvarez, has declared his assets on his web site <http://www.chachoalvarez.com>.
28. Ruling of March 2, 1993, of the Criminal Court of Appeals of Uruguay, 107 *La Justicia Uruguaya* No. 12,338.
29. Ruling of March 13, 1999, of the Criminal Court of Appeals of Uruguay, 107 *La Justicia Uruguaya* No. 13,724.
30. See also *Movimiento al Socialism MAS v. Governador del Estado Apure*, ruling No. 1155 of May 18, 1999, of the Supreme Court of Venezuela.
31. California Constitution Article I (1) reads: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing and protecting property, and pursuing and obtaining safety, happiness and privacy."
32. 865 P. 2d 633 (Cal. 1994).
33. 533 P. 2d 222 (Cal. 1975).
34. See Optional Protocol to the Convention on the Rights of the Child concerning the sale of children, child prostitution and child pornography, Article 2c.
35. Compare "PC peep show: Computers, privacy and child pornography", *John Marshall Law Review* 27 (1989): 989–1013.
36. 000 US u10263, ruling of June 26, 1995. In general terms, the content of this paragraph is based on the opinion of Justice Antonin Scalia.
37. According to Traband (1995), this ruling reverses the burden of proof, violates the presumption of innocence, and sows mistrust between students and teachers. See Also *AVP v. Ministerio de Education y Cultura y Comité Olímpico Uruguayo* (Civil Court of Appeals, 5th Cir. 1998), in which the court held that journalistic reporting on doping issues, naming those involved, helps to eradicate this harmful practice while keeping the public informed on a matter of evident public interest, in this case the conduct of the country's athletes and the reasons why they were not invited to join the national team (118 *La Justicia Uruguaya* No. 13,590).

38. As is natural, the Supreme Court of Brazil in *Paulstein Aureliano de Almeida, habeas corpus* (1996), found that "the violation of the secrecy of telephone conversations for purposes of criminal investigation or judicial proceedings is not self-applicable: it requires a law establishing the hypotheses and the form that will permit a court warrant. . . . The guarantee that is provided by the Constitution, until such time as legislation is defined, does not distinguish public from private telephones, even those installed within a residence, because the juridical good protected is the privacy of persons, a dogmatic prerogative of all citizens."
39. 10 JLR 438.
40. 1 TTLR 189.
41. Privy Council (1996) 48 WIR 1.
42. Court of Appeals, Jamaica, 1994, 31 JLR 87.
43. Compare *Bravo, Francisco v. Alfaro Standen SA, Assa SA*, Court of Appeals of Santiago, 2000: "A person who honours his debts must be removed from the records of overdue debtors"; and *Bettenhauser Keim, Francisco v. Congresin Ltda y DICOM SA*, Court of Appeals of Valdivia, 1996: "A credit bureau is guilty of an arbitrary act if it refuses to eliminate a person from a list of debtors after it has been demonstrated by reliable documentation that his debt has been fully discharged."
44. Alternatively see *Subtipos de Habeas data en el Derecho Argentino: sus posibilidades en el Peruano*, Argentine Association of Constitutional Law, 1996.
45. *Lazcano Quintana, Guillermo v. Veraz SA*, National Civil Court of Appeals (Argentina), February 23, 1999 (La Ley, ADLA XXVI-C, 1491). Note to the ruling by Santos Cifuentes (1999); Rabinovich-Berkman, *Cuestiones actuales en derechos personalísimos, Dunken, 1997, and Derecho Civil. Parte General*, Astrea, 1999.
46. LORTAD (Automated Data Processing Act).
47. *Lazcano Quintana, Guillermo v. Veraz SA*, National Civil Court, Hall D, February 23, 1999; *Urteaga, Facundo R. v. Estado Mayor Conjunto de las Fuerzas Armadas*, Supreme Court, October 15, 1998. See Cifuentes (1999).
48. The appeal was submitted by the Latin American Network of Women Transforming the Economy (REMTE-Chile) and the National Gender, Business and Human Rights Network against the body representing the judiciary (see Bidart Campos 1992: 415).
49. Law 23,990 on the National Blood System in Argentina and the 1977 Transfusions and Blood Banks Act in Venezuela are examples of legislation on such information.
50. "The right of non-discrimination will mean nothing for them if, for fear of their privacy, they retreat into isolation, cut themselves off from their activities, hide their suffering or feel guilt when in fact there is no reason to do so. Privacy is a right of everyone, and whenever a request for confidentiality is made in such cases the Court will take into account the reasons offered."
51. Administrative Disputes Court of Montevideo, first session, 1997, 1 *Lex* (1997) 17–27.

52. The Supreme Court of Costa Rica, in *M.J.J. v. Instituto Nacional de Seguros*, denied an appeal, ruling that, "in effect, it is not illegitimate discrimination but a reasonable differentiation if distinct conditions are established with respect to premiums or benefits for persons with certain functional limitations, as is done with respect to the age of an applicant. There are obvious grounds for unequal treatment in these cases, and so the court cannot accept the appellant's argument that he is in a condition of equality with other persons who do not have his physical problem, and that he must be treated as such." This point of view strips the insurance system of its eminently social function. Moreover, there must be a limit on the number of variables used in calculating premiums, otherwise the size of the sub-populations would be reduced to the point that the actuarial concept of "insurance" would be rendered meaningless.
53. Section 39 (2) also covers persons convicted within the last five years, or against whom charges are pending.
54. US Bureau of Justice Statistics (1997) *Privacy and Juvenile Justice Records: A mid-decade status report*.
55. In Latin America and the Caribbean, such systems were promoted by the SIPI programme of the Inter-American Children's Institute of the Organization of American States <http://www.iin.org.uy>.
56. Some security provisions have been built into the new Draft Code of the Child and Adolescent of Uruguay, Articles 11, 22 (f) and 211 to 215.
57. *S., V. v. M., D.A.* precautionary measures, filiation, Supreme Court of Argentina, April 3, 2001.
58. Adoption Records Database <http://www.skylace.net/adoption>.
59. 20 US 1232g.
60. Sample sites: <http://www.drugtestwithhair.com> and <http://www.drugfreeteenagers.com>.
61. The laws of Neuquén and the city of Buenos Aires allow for an alimony or support debtor to be prohibited from leaving the country until he meets his obligations. Other jurisdictions have adopted similar restrictions, for example, Srt. 90 of the Child Defence Act of Colombia and Article 220 of the Uruguayan Code of the Child.
62. See *Hodge v. Jones*, 31 F. 3d 157, cert. denied 115 S. Ct. 581 (1994) and Jones (1995).
63. In *P.M.D.J. v. CONSEP*, an appeal for habeas data was brought before the Constitutional Court of Ecuador. The court ordered that the appellant be deleted from the list because the particular article of the law criminalizing the possession of small narcotic doses had been repealed.
64. Appeal to the Supreme Court of Mexico, 2000. *Semanario Judicial de la Federación y su Gaceta*, Vol. 11 (April 2000), P.LX/2000, p. 74.
65. Government to issue identity cards to newborns babies, *The Star* (Malaysia), March 16, 2001.
66. <http://www.ss.gov.ph/other/othe5001.htm>.

67. Supreme Court of Chile, 1996. "The appeal for protection must be brought against the banking institution that reported the complaints recorded in the Boletín Histórico, and not against the latter institution, which was acting in accordance with law."
68. Software is now available for recording any activity performed on a computer, including not only incoming and outgoing e-mail but also web sites visited, periodic screen scans and keystroke monitoring. This information is sent secretly to the "spy's" computer, and the user is unable to erase his tracks.
69. Ruling of September 9, 1974, Boletín Judicial No. 766, pp. 2437–44.
70. Article 53: "Entities issuing credit or bank cards are prohibited from informing 'personal financial background databases' on the holders and beneficiaries of credit card extensions or options when the holder has not paid his obligations, or is in arrears or undergoing refinancing, without prejudice to the obligation to inform the Central Bank of Argentina. Reporting entities are jointly and severally liable for damages and injury caused to beneficiaries of credit card extensions or options as a consequence of information provided."
71. *Semanario Judicial de la Federación* (1987), Vol. 217-228 (7), p. 75.
72. The Jamaican Constitution does not expressly prohibit wiretaps, but it provides a point of departure for analyzing the legal implications (cf. Section 22). In analyzing crimes under the Telephone Act of 1893 (Section 20), it is interesting to see how frequently axiological gaps appear in the face of new crimes resulting from the application of new technologies; it is difficult to cover them all in legislation and, generally speaking, they are treated as violations of constitutional rights.
73. (1979), Chancery Division 344 and (1979) 2 AII ER 620. See Demeriex (1992: 306–313).
74. National Court of Appeals in Criminal and Correctional Matters (Argentina), 1997. Another relevant decision is *In re Manuel Goggero* (National Court of Appeals in Criminal and Correctional Matters, 1999), reiterating the ruling established by the court in numerous precedents, to the effect that evidence obtained by a private party, even without the consent of the person involved, does not contravene any constitutional or procedural norm, regardless of its evidentiary value, but this is not applicable when it is the state itself that obtains it through one of its administrative organs, in the course of an unauthorized investigation or initiative. Such irregular investigation by the state, using subterfuge to obtain information and evidence on persons suspected of a crime, violates the constitutional principles that set minimum standards for due process and that are a condition of validity for any conviction. Similarly, ruling RHC 10534 of the Supreme Court of Brazil declares: "The recording of a conversation by one of the interlocutors does not constitute telephone tapping, and is admissible as proof in criminal proceedings" DJ 11/12/2000, p. 218.
75. Cámara Nacional Civil, sala E (1997), 1999-ii *Jurisprudencia Argentina* (1999) 339042.

76. See *Viernes Entretenimiento CA amparo*, Supreme Court of Venezuela, 2000.
77. Action for *habeas corpus*, Supreme Court of Costa Rica, 1991.
78. Supreme Court of Chile, motion for protection, 1997, 468 *Fallos del Mes* 2055-2058.
79. Internet and data interception capabilities developed by FBI, <http://www.fbi.gov/congress/congress00/kerr072400.htm>
80. This type of equipment uses triangulation with signals from groups of satellites to fix a position on the ground. One such group of satellites is maintained by the US government (GPS), and another by the Russian government (GLONASS). Both are available for civilian use (research, aviation, automobiles, etc.). The US system introduces slippage in the signal so that accuracy for civilian equipment is degraded, although objects can still be located within 10 metres.
81. FBI, Implementation of the Communications Assistance for Law Enforcement Act (CALEA), <http://www.fbi.gov/congress/congress97/calea2.htm>.
82. Communications Assistance for Law Enforcement Act, <http://www.epic.org/privacy/wiretap/calea/calealaw.html> (HR 4922).
83. <http://www.europarl.eu.int/committees.echelon_home.htm>.
84. American Management Association (2000), Workplace testing, monitoring and surveillance, <http://www.amanet.org/research/pdfs/monitr_surv.pdf>.
85. Birsch and Fielder (1994).
86. J.O. of January 7, 1978, as corrected in the J.O. of January 25, 1978.
87. See, for example, the veto exercised by the President of Argentina against Article 29 of the Personal Data Protection Act (Law 25,326 of 2000), presumably in an effort to avoid the cost of creating an administrative structure.
88. Yasin (1997) <http://www.techweb.com/wire/news/1997/11/1120hack.html>.
89 US General Accounting Office Information security: Computer attacks at Department of Defense pose increasing risks, May 22, 1996. <http://www.gao.gov/AindexFY96/abstracts/ai96084.htm>.
90 Information and Privacy Commissioner, Ontario, Canada. *Privacy: The key to electronic commerce*, <http://www.ipc.on.ca/english/pubpres.sum_pap/papers-comm.htm>.
91. Resnick (1997) <http://www.sciam.com/0397issue/0397resnick.html>.
92. World Wide Web Consortium, P3P Vocabulary Working Group, Grammatical model and data design model, October 22, 1997, <http://www.w3.org/TR/WD-P3P-grammar.html> ; and P3P Architecture Working Group, General overview of the P3P architecture, October 22, 1997, <http://www.w3.org/TR/WD-P3P-arch.html>.
93. In this context, “authentication” means that the sender and the receiver can confirm the identity of the other party, as well as the origin and destination of the information.
94. “Non-repudiation” implies that the creator/sender of the information cannot deny authorship of the message or of the information.

95. Royal Decree 994/1999, regulating security measures for computerized files containing personal data, Spain, <http://www.agenciaprotecciondatos.org/datd8.html>.
96. Makrygiannis (n.d.) <http://www.adb.gu.se/-nickolas/papers/IRIS18.pdf> .
97. Leggiere (1998) <http://www.upenn.edu.gazette/1198/leggiere.html>.
98. See note 12 and accompanying text.
99. The end of privacy: The surveillance society", *The Economist*, May 1, 1999, pp. 21–3.
100. Some legal systems recognize limitations on freedom of the press. The German Constitution, for example, provides in Article 5 (2) that "These rights are subject to limitations in the provisions of general statutes, in statutory provisions for the protection of the youth, and in the right to personal honour".
101. This case was resolved after its publication in Spanish; the Supreme Court made freedom of expression to prevail.

Bibliography

Alterini, A. and A. Filippini (1986) Responsabilidad civil derivada de la difusión de noticias inexactas: acto ilícito o acto abusivo. *La Ley*, 1986-c: 406–18.

Annas, G. J. (1999) Genetic privacy: There ought to be a law. *Texas Review of Law and Politics*, 4: 9–15.

Antik, A. and L. Ramunno (2000) Habeas data: Comentarios sobre los bancos de datos privados destinados a proveer informes. *La Ley*, 2000-b: 1.164.

Bianchi, A. (1995) Habeas data y derecho a la privacidad. *El Derecho*, 161: 866–78.

Bidart Campos, G. J. (1992) Identidad, filiación y privacidad de una menor en su juicio de filiación paterna: nada de vedettismo informativo. *El Derecho*, 145: 415.

Birsch, D. and J. H. Fielder (eds) (1994) *The Ford Pinto case: A study in applied ethics, business and technology*. New York: State University of New York Press.

Budano Roig, A. (1998) La libertad de prensa, la censura previa y el derecho a la intimidad de una menor. *El Derecho*, 177: 181–217.

Cadoux, L. (1994) L'expérience française en protection des données personnelles dans le domaine des banques de données judiciares. In: G. Vasco (ed.), *Informática Judicial y Protección de Datos Personales*, pp. 157-171. Departamento de Justicia.

Cappelletti, M. and B. Garth, (1988) *Acesso à Justiça*. Fabris Editor.

Chaum, D., A.Fiat, and M. Naor (n.d.). Untraceable electronic cash. In: S. Goldwasser (ed) *Advances in cryptology crypto'88*. Springer-Verlag.

Cifuentes, S. (1995) La intimidad y el honor de los vivos y de los muertos. *El Derecho*, 162: 404.

Cifuentes, S. (1999) Reconocimiento Jurisprudencial del derecho a los datos personales informáticos y del habeas data en su verdadero fin tutelar. *La Ley*, 1999-e: 151.

Cifuentes, S. (1999) Nota al fallo: "Reconocimiento del derecho a los datos personales informáticos y del *habeas data* en su verdadero fin tutelar". *La Ley*, September 15.

del Villar, R., A. Díaz de León, and J. Gil Hubert (2000) La regulación de protección de datos personales y burós de crédito en América Latina. Paper presented at International Conference on Credit Reporting Systems. World Bank Institute.

Demeriex, M. (1992) *Fundamental rights in Commonwealth Caribbean countries.* University of West Indies.

Fuentes Torrijo, X. (2000) Criterios para solucionar el conflicto entre la libertad de expresión y la protección de la honra de las personas: dos métodos distintos de razonamiento jurídico. *Ius et Praxis*, 6(1): 427–41.

Gozaíni, O. (2001) *Habeas data. Derecho procesal constitucional*. Rubinzal Culzoni eds.

Gregorio, C. G. (1999) *Información, Privacidad y Derechos del Niño.* 17th Panamerican Children's Congress. oea/Ser.K/xxiv.18.1/cpn/doc.12/99.

Jones, J. (1995) Maintaining unsubstantiated records of "suspected" child abuse: Much ado about nothing or a violation of the right of privacy? *Utah Law Review*, pp. 887–912.

Leggiere, P. (1998) Constitutionalist in cyberspace. *Pennsylvania Gazette.* <http://www.upenn.edu.gazette/1198/leggiere.html>.

Makrygiannis, N. (n.d.) *Dispersed information system structures.* Department of Informatics, Göteborg University, Sweden. <http://www.adb.gu.se/-nickolas/papers/IRIS18.pdf>.

Martorell, F. (1993) *Impunidad diplomática.* Buenos Aires: Editorial Planeta.

Miller, M. (2000) Credit reporting systems around the globe: The state of the art in public and private credit registries. Paper presented at International Conference on Credit Reporting Systems. World Bank Institute.

Peña González, C. (1996) El derecho civil en su relación con el derecho internacional de los derechos humanos. In: C. Medina, and J. Mera Figueroa, (eds) *Sistema Jurídico y Derechos Humanos*. Chile: Universidad Diego Portales. pp. 545–660.

Pierini, A., V. Lorences, and M. I. Tornabene, (1999) *Habeas data: Derecho a la intimidad.* Editorial Universidad.

Prosser, W. (1960) *Handbook of the law of torts.*

Puccinelli, O. (1999) *El habeas data en Indoiberoamérica.* Santa Fe de Bogotá: Editorial Themis.

Resnick, P. (1997) Filtering information on the Internet. *Scientific American*, March. <http://www.sciam.com/0397issue/0397resnick.html>.

Roche, P. and L. Glantz, (1996) The Genetic Privacy Act: A proposal for national legislation. *Jurimetrics Journal*, 37: 1–11.

Rotunda, R. (1995) Computerized highways and the search for privacy in the case law. *Computer and High Technology Law Review*, 11: 119–27.

Roxborough, P. (1999) Invasion of privacy: Telephone customers upset with billing system. *Jamaica Gleaner*, March 8.

Rubenfeld, J. (1989) The right of privacy. *Harvard Law Review*, 102: 737–52.

Sagüés, N. P. (1995) Subtipos de habeas data. *Jurisprudencia Argentina*, 1995-iv: 352–5.

Schwartz, P. (1992) Data processing and government administration: The failure of the American legal response to the computer. *Hastings Law Review*, 43: 1321–89.

Shapiro, R. and G. Annas (1994) Who sees your medical records? *Human Rights: Journal of Individual Rights*, pp. 10–36.

Shepherd, L. (2001) Looking forward with the right of privacy. *Kansas Law Review*, 49: 251–320.

Slaibe, M. and C. Gabot, (2000) Habeas data: su alcance en la legislación comparada y en nuestra jurisprudencia. *La Ley*, 2000-b: p. 27.

Sosa, R. (2000) El habeas data y el amparo al derecho a la intimidad. *Gaceta Judicial* (República Dominicana), 74.

Traband, R. (1995) The Acton case: the Supreme Court's gradual sacrifice of privacy rights on the altar of the war on drugs. *Dickinson Law Review*, 100: 1–28.

Vibes, F. (2000) Internet y Privacidad: la difusión en Internet de imágenes lesivas de la intimidad, el honor y otros derechos personalísimos. *La Ley*, 2000-d: 1011–24.

Ward, B. (1997) Hackers find theft at fingertips. *Windsor Star*, October 21.

Warren, S. and L.D. Brandeis, (1890) The right to privacy. *Harvard Law Review*, 4: 193.

Williams, G. (1999) On the QT and very hush hush: A proposal to extend California's constitutional right to privacy to protect public figures from publication of confidential personal information. *Loyola of Los Angeles Entertainment Law Journal*, 19: 337–61.

Yasin, R. (1997) E-commerce sites top hacker hit list. *Internet Week*, reported in *Tech Web News*, November 20. <http://www.techweb.com/wire/news/1997/11/1120hack.html>.