Office of the Privacy Commissioner of Canada

Control Authorities

Personal Information in the French-speaking World

Paul-André Comeau
September 2007

TABLE OF CONTENTS

MESSAGE FROM THE PRIVACY COMMISSIONER

Over the past few years, the world has seen a technological explosion that challenges the historical relationship between the economy, society and individuals. With globalization and the ever-growing reach of the Internet, many bridges have been built between countries, cultures, markets. While these roads favour a welcomed rapprochement in many respects, they cannot, without clear, universally identified and accepted regulation, protect the personal data circulating on them.

Faced with this problem, Francophone data protection authorities recognize the priceless value of shared knowledge and practice to take advantage of each other's experience, for the challenges are essentially the same. Armed with the support of the Organisation internationale de la francophonie (OIF) for the development of an international instrument that would guarantee respect of the right to privacy, the representatives of 14 countries have agreed to form an Association of Francophone Personal Data Protection Authorities at the end of an initial meeting in Monaco in September 2006. At that meeting, Mr. Raymond D'Aoust, Assistant Privacy Commissioner with the Office of the Privacy Commissioner of Canada (OPC), seconded by Ms. Marie Georges of the Commission nationale de l'informatique et des libertés (CNIL), proposed to hire an expert to make a comprehensive study of current data protection systems. This motion was greeted favourably by the authorities in attendance.

It is with great pleasure that we now present this study. This invaluable document diagnoses the state of privacy protection in the Francophonie, first by mapping the data protection systems existing in various Francophone countries; then, by making a thorough analysis of the functions of those systems and the activities of authorities responsible for them. Thus can begin a process of sharing expertise and experience to deal with the problems faced by institutions of different legal cultures—but whose objectives are virtually the same.

I wish to salute the author of this document, Mr. Paul-André Comeau, who was president of Quebec's Commission d'accès à l'information from 1990 to 2000. With his broad experience and his keen eye, he has contributed significantly to the completion of our project. I also wish to warmly thank members of the Canadian Work Group on the Association Statutes: Mr. Jacques Saint-Laurent, president of Quebec's Commission d'accès à l'information, Mr. Raymond D'Aoust, Assistant Commissioner, PCC, Mr. Christian Whalen, counsel of the New Brunswick Ombudsman Office and the PCC, Ms. Nathalie Daigle, of the PCC's legal department, and finally, Ms. Florence M.C. Nguyen, main communication advisor. Together, they saw this project through.

We hope that the Association of Francophone Authorities will take advantage of this study to join a broader movement to safeguard the right to personal information protection, which is part of the human rights heritage. The constituent assembly of the Association will be held in Montréal in September 2007, as part of the 29th International Conference of Data Protection and Privacy Commissioners, a pre-conference of which will focus on data protection in the Francophone world.

We hope this work will provide food for your thoughts as much as it has enlightened ours.

Jennifer Stoddart
Privacy Commissioner of Canada

FOREWORD

This report has been prepared in view of the founding of the organization of personal data or information control authorities of French-speaking states, in Montréal, in September 2007. It results from an initiative of the Privacy Commissioner of Canada, Ms. Jennifer Stoddart, on behalf of her colleagues of French-speaking countries.

This brief outline of the eight control authorities operating in French-speaking countries in June 2007 was done in two steps. First, we examined available texts to get an idea of the origin and evolution of those administrative bodies. Then, we formally interviewed officials of the organizations to check our assumptions and deepen our knowledge of them.

The author of this study wishes to express his thanks to the heads of the control authorities and their staff who eagerly answered every one of our queries. Likewise, he acknowledges a debt of gratitude to Ms. Marie-Pierre Busson and Mr. Maxime Laverdière, who helped him through his research.

Finally, as the expression goes, the author assumes full responsibility for the content of this report.

Paul-André Comeau
Montréal, July 16, 2007

INTRODUCTION

Few observers noted a paragraph devoted to the issue of personal data or information[1] in the final communiqué of the XI[th] Conference of Heads of States and Governments of French-speaking Countries held in Bucharest in September 2006.[2] Considering the exponential increase in the cross-border movement of personal data, member states of the Organisation internationale de la francophonie (OIF) expressed their interest in the adoption of an international instrument guaranteeing the right of individuals to the protection of such information. Behind the diplomatic dressing, what must be seen is an agreement in principle on restrictive measures of world-wide scope.

At their previous summit in Ouagadougou in 2004, OIF members had emphasized the importance of personal information protection. In a very explicit way, that document called for the development of a form of international co-operation between 'independent authorities responsible in every country' to ensure the respect of measures for the protection of personal data.[3]

Those two recommendations are of concern to the citizens and leaders of nations making up the institutional French-speaking community. The goal of international co-operation formulated in both Romania and Burkina Faso cannot be more explicit. It suggests that every OIF member state will set up legal systems that effectively ensure the protection of personal data and the respect of privacy. The citizens of French-speaking countries should be the beneficiaries of 'the protection of individual freedoms and fundamental rights,' to repeat the terms used in the Ouagadougou communiqué.

How can these wishes be answered? How can the implementation of such systems be given concrete expression? Do models or precedents exist to guide and structure an intelligent adaptation of the principles and details of such legal construct? On what basis and with what goals can an international process be undertaken that would lead to the development and adoption of an international instrument? None of these questions is trivial at a time when independent authorities responsible for the protection of personal data are wondering about their powers and the effectiveness of their mission.[4]

Protection of personal data, respect of privacy: these objectives add to the challenges states committed to "good governance" must face. This challenge involves a dimension of individual

---

[1] *Données personnelles* [personal data] was the term chosen by the national authority representatives who launched the Conférence des commissaries à la protection des données de la Francophonie project, during their September 5, 2006, meeting in Monaco. The expression is used indifferently with *renseignements personnels* [personal information], which is more common in North America.

[2] XI[th] Conference of Heads of State and Government of Countries Using French as a Common Language. Bucharest, Romania, September 28 and 29, 2006 - *Bucharest Declaration*: paragraph 59.

[3] X[th] Conference of Heads of State and Government of Countries Using French as a Common Language, Ouagadougou, Burkina Faso, November 26 and 27, 2004. *Ouagadougou Declaration*: paragraph 51.

[4] It was one of the themes developed at the 29[th] Conference of Data Protection and Privacy Commissioners held in London, November 2 and 3, 2006. See on this topic: "The London Initiative: Communicating on Data Protection and Making It Effective."

rights that has been taken into account in many Western countries these past thirty years.[5] In the early 1970s, the United States and some European states tried to come to terms with the problem data processing posed for the respect of individual rights. Circumstances could vary from one country to another, but the issue remained the same: how to ensure the respect of the private sphere with the development of the new technologies. The West German state of Hesse, as early as 1971, and Sweden, in 1973, took action by passing a law on data protection. Seeing the scale of the debate on this issue, the United States followed suit in 1974.

French-speaking states in Western Europe and North America soon joined the movement. In Europe, France, Belgium, Switzerland, Luxembourg and Romania, and in North America, Canada, Quebec and New Brunswick implemented their own personal data protection system starting in 1977. They entrusted "independent bodies" with the mandate of ensuring the respect of rights and principles set out in their legislation on the protection of personal information.

This document describes in schematic form the situation of the eight "control authorities." The idea is to make a brief presentation of each of those institutions or administrative authorities. These tables will also bring to light the evolution of the mission and powers of those organizations.

Those various institutions, whose purpose is practically identical, certainly bear the imprint of different legal cultures. But they all rest on the same basic principles. Hence the interest of this work, which is not intended as a study in comparative law nor claims to be exhaustive. The goal is more modest. It is merely to suggest avenues of research in the light of these Francophone experiences and point out trends to those considering the possibility of implementing personal data protection systems.

[5] See the last available census: Electronic Privacy Information Center - *Privacy and Human Rights 2004,* Washington, EPIC, 2004, 775 p.

Belgium

Commission de protection de la vie privée

Belgium's Commission de protection de la vie privée (CPVP) is a very particular case within monitoring bodies. This institution can pride itself on existing even before the adoption of legislation to protect personal information in that country. An advisory body at its inception, the CPVP was elevated to the rank of control organization when the Belgian parliament passed its legislation.

It was introduced in a context of profound constitutional changes. The unitary state established in 1830 was converted in the 1990s into a true federal state within which coexist Walloons, Flemish and Bruxellois, as well as a German-speaking minority.

The steps taken on the European scene, first in the European Council in Strasbourg, then at the seat of the European Union in Brussels, also influenced Belgium's development in the protection of personal data.

The legislative process

The plan to create a national data super file of the population following the merger of a number of identity files in 1982 prompted the Belgian Parliament to appoint an "advisory commission on the protection of privacy," whose mission was to ensure the citizens' right to privacy was respected.

In 1992, Belgium adopted legislation on privacy and the protection of personal data. The creation in 1990 of the "Banque Carrefour de la sécurité sociale"—a bona fide national data bank—was one of the events that triggered it. So were the measures taken in 1991 to regulate consumer credit and track defaulting debtors. Parliament then took note of the concerns expressed by members of the advisory commission, who had assessed the limits of this system, and established the current Commission de protection de la vie privée in late 1991, one year before passage of the act.[6]

This act covers both the private and the public sectors. It applies over the entire territory of the federation. The protection of personal information and privacy comes within the sole remit of the federal authority, a different situation than what we see in other federal states, beginning with Canada.

[6] These paragraphs are inspired from notes written by the first chairman of the CPVP, Mr. Paul Thomas. Unpublished document entitled, "La Commission de la protection de la vie privée : Treize années de protection des données personnelles."

The Belgian Parliament brought major changes to the Act in 1998.[7] Like other member states of the European Union, Belgium then discharged its obligation to incorporate into its legal arsenal the principles stated in the 1995 European directive.[8]

A pluralist college

The Act of 1992 invests the commission with powers similar to those of monitoring bodies in neighbouring countries. In 2003, the federal Parliament responded to the indirect appeals made by the Commission, concerned by the shortcomings and inadequacies of its status. Parliament made major legislative changes affecting particularly the makeup, role and mandate of the Commission.[9]

Given the "collateral body" status of the Chamber of Representatives,[10] the CPVP now enjoys true independence, in line with the European directive stipulations. It reports directly to the President of the Chamber and is funded by Parliament's Budget Commission. The CPVP must also submit its annual report and management plan to the Chamber.

Within the Commission, the legislator has set up sectorial committees responsible for dealing with the files of specific areas: the national register of physical persons, the enterprises' data bank, the social security data bank, health data and federal public services. Another committee was formed in 2005 to monitor the PHENIX information system (now suspended), which handles the flow of data from the judiciary, including court records.[11] Finally, a 2006 act established a sectoral committee for statistics.

The CPVP has a pluralist structure that integrates a certain number of characteristics of Belgium's social and political reality. Commission members—eight permanent, and as many substitutes—are appointed by Parliament on the proposal of the government, which must suggest two candidates for each position to be filled. The linguistic balance between Walloons and Flemish must be respected and the composition of the Commission must also reflect the country's socio-economic diversity, including families and political parties.

---

[7] "Act of 11 December 1998 incorporating European Parliament and Council directive 95/46/CE of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data." *Moniteur belge*, February 3, 1999. This act came into effect on February 1, 2001.

[8] European Parliament and Council directive 95/46/CE of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[9] Act of 26 February 2003 "Act amending the act of 8 December 1992 on the protection of privacy with regard to the processing of personal data and the act of 15 January 1990 on the institution and the organization of a social security data bank to adjust the status and extend the jurisdiction of the Privacy Commission." *Moniteur belge*, June 26, 2003.

[10] The Commission de protection de la vie privée, along with some other bodies like the Revenue Court, is part of a group of institutions attached to the Chamber of Representatives as a "collateral body." See on this subject: Charles-Étienne Lagasse, *Les nouvelles institutions politiques de la Belgique et de l'Europe* (3rd edition), Namur, Erasme Didier-Hatier, 2003.

[11] This sectorial committee is established under Section 22 of the Act of 10 August 2005 instituting the Phenix information system, which exercises advisory and monitoring powers over the internal and external communication of personal data for the functioning of the judiciary. See the Commission's Web site at http://www.privacycommission.be.

The Chairman, assisted by a Vice-Chairman, must be a career magistrate, on temporary assignment during his stay at the Commission. The Commission must also include at least one computer scientist, one jurist and one person with professional experience in the management of personal data in the public sector.

The Commission selects its own staff—about 50 in all. Managers and other employees enjoy a particular status modelled after the federal civil service standards. The chairman is responsible for the Commission's administrative services—resource organization and management, studies and research, and external relations—but daily management is carried out by an administrator.

The Commission meets in plenary session every three weeks. The collective character of this structure in which the chairman holds no particular powers is reflected in the Commission's deliberations.

An original style

The Belgian Commission aims explicitly at maintaining a balance between the protection of freedoms and the processing of personal data.[12]

The Commission receives and registers processing statements filed by persons responsible for the protection of personal information in private and public organizations. And it resorts to mediation, explicitly provided for in the Act, to find a solution to complaints filed by citizens.

Any bill, regulation or departmental order that may impact on the protection of personal information may be referred to the CPVP by any political body in the federation. Its advice is required to be published along with the matter at issue in the *Moniteur belge*, the kingdom's official newspaper, and posted on the Commission's Web site. The government may accept or dismiss the opinions and recommendations of the Commission decided in plenary session. The Commission's power has been reinforced by several decisions of the State Council. The latter has indeed invalidated some measures because the government had failed to seek the Commission's opinion.

The Commission plays an active role in many respects. Most recommendations result from initiatives taken by the Commission, which, with the secretariat, does the preliminary research and the writing.

At the beginning of the last federal election in June 2007, the Commission repeated an interesting initiative as a preventive measure. It drew attention to a legal notice to remind the political personnel and candidates of their obligation to respect personal information, and it launched a citizen question forum.

The CPVP has tackled for a few years the issue of personal credit and the blacklists developed by creditors. Credit is covered by a federal law and the National Bank was given a mandate to trace the history of all consumer loans, including mortgage loans. This record, accessible to credit organizations, traces every loan—good and bad debts—making it possible to spot insolvent

[12] Commission's Management Plan, http://www.privacycommission.be/la_commission/plan_de_gestion.pdf.

debtors. The intervention and support of the Commission have humanized this practice of the consumer society.

New paths

With the deployment and globalization of new information and communication technologies (NICT), the SWIFT case represents the type of original, important area in which the CPVP is getting successfully involved.

Following reports in some US newspapers, the Commission launched an investigation into the role of SWIFT—an electronic transfer co-operative of banking transactions based near Brussels. This organization was alleged to have bowed to U.S. pressures on the heels of the *PATRIOT Act,* adopted by the U.S. Congress after the September 11, 2001, attacks. After a complex investigation, the Commission concluded the Belgian-incorporated co-operative had broken certain provisions of the law on the protection of personal information in the transfer of banking data to the United States.[13] Together with the monitoring bodies of some European Union countries, the Belgian Commission led the investigation that concluded there was a breach of the 1995 European directive.

By and large, the Belgian Commission wants to take advantage of its new status as a collateral body of the Chamber of Representatives to assume more pro-active responsibilities. Instead of being "captive" and dependent on external factors—opinion requests, citizen complaints**,** etc.—it plans on taking a series of initiatives to better fulfil its mission.

On the Brussels Grand Place

The European Union's evolution in the protection of personal information has profoundly influenced Belgium's development in the area. Today, as we have seen, the Belgian Commission plays a key role within the "Article 29 Working Party,"[14] which gathers persons responsible for data protection from every member state; two members of its staff follow through plenary meetings and the work of sub-committees.

Bilaterally, the CPVP offers advice and support to its counterparts in Western countries, beginning with neighbouring Luxembourg, and to European Union newcomers, like Romania. South Korea, Japan and Burkina Faso have also taken advantage of this discreet guidance these past few years.

[13] In a notice published on September 28, 2006, the Commission determined that SWIFT had failed to respect Belgian and European legislation in its processing of data. The press release is available on line at http://www.privacycommission.be/communiqu%C3%A9s/summary_opinion_Swift_%2028_09_2006.pdf

[14] Under Section 29, European directive 95/46/CE of 24 October 1995 set up an independent task force gathering representatives from the data protection bodies of every European Union member states, called the "Article 29 Data Protection Working Party.'

In its management plan tabled before Parliament, the Commission makes no secret of its international ambitions: it seeks to play "an essential role." In short, it intends to develop "the international dimension of its activities, because of the globalization of problems."[15]

[15] Commission's management plan, http://www.privacycommission.be/la_commission/plan_de_gestion.pdf [Translation].

Canada

Privacy Commissioner

In 1977, Canada's federal Parliament laid the foundations of its personal information protection system in the public sector, becoming one of the leaders among Western states deeply concerned by the advent of the first giant computers. At the same time, an ombudsman was appointed to supervise this system. This formula departed from the choices made in Sweden and in the German state of Hesse,[16] which devised an entirely different mechanism. This decision was also contrary to the choice made by Washington, which preferred to have the courts exercise this function.[17]

In 2000, another major surprise: the President of the Canadian Direct Marketing Association congratulated the Canadian federal government for having legislated on the protection of personal information in the private sector.[18] This legislation is itself an innovation: it is structured around a self-regulating code drawn up by the Canadian Standards Association.

The legislative process

The passing of personal information protection legislation by Canada's federal Parliament is the result of questioning, particularly among senior public officials, about the growing power of computer processing. A task force set up in Ottawa published a report specifically entitled *Computers and Privacy* in 1972.[19]

The notion of personal information as a dimension of privacy was first included in the *Canadian Human Rights Act*, adopted in 1977.[20] It was a prelude to the adoption of a formal law covering the entire federal public sector in Canada.[21] A quarter of a century later, the 1982 Act has yet to be reviewed and modified by Parliament.

Over the years, personal information protection was fleshed out with the adoption of the OECD guidelines[22] and the work carried out by the European Council in Strasbourg in the 1980s and revived in the mid-1990s.[23] The European Union's decision to adopt a major directive in 1995[24]

---

[16] David Flaherty explains how the precedents set in the state of Hesse and in Sweden had failed to convince experts of their relevance in the Canadian context. David H. Flaherty, *Protecting Privacy in Surveillance Societies*, Chapel Hill and London, The University of North Carolina Press, 1989, p. 265.
[17] *The Privacy Act (*1974)
[18] Stephanie Perrin, Heather H. Black, David H. Flaherty, T. Murray Rankin, *The Personal Information Protection and Electronic Documents Act*, Toronto, Irwin Law, 2001, p. 4.
[19] Report of the Joint Study Group of the Department of Communications and the Department of Justice, *Computers and Privacy*, Ottawa, Information Canada, 1972.
[20] *Canadian Human Rights Act,* R.S.C. c. H-6.
[21] *The Personal Information Protection Act*, R.S. 1985, ch. P.21.
[22] *Council recommendations concerning the guidelines on privacy and the cross-border flow of data of a personal character*, OECD, Paris, September 23, 1980.
[23] Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Convention 108), Strasbourg, January 28, 1981. Modified by a protocol (STE No. 179) on November 8, 2001.
[24] *European Parliament and Council directive 95/46/CE of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*.

added a new element to the questioning under way in Ottawa. Quebec had taken the lead in North America by passing legislation governing the private sector.[25] In all likelihood, the then Privacy Commissioner played a decisive role by recommending that the federal government do the same. In 2000, Parliament passed a law protecting personal information in the private sector.

The 2000 Act broke new ground in more than one respect. The legislation is based on the federal Parliament's exclusive power over inter-provincial trade. The *Personal Information Protection and Electronic Documents Act*[26] was modelled on the 10 principles of the code developed by the Canadian Standards Association. The legislation also bears the mark of the Information Highway Advisory Council formed in the early 1990s.[27] The federal act covers the private sector in Canada wherever provincial legislatures have not passed "substantially similar" legislation.[28]

The choice of a model

For two long hours in November 2003, the current Privacy Commissioner faced a barrage of questions from representatives of the four political parties on the House of Commons' Standing Committee on Government Operations and Estimates.[29] She was asked just about all and sundry during the session that brought to mind similar scenes in the United States' Senate. It was in fact a first: the Prime Minister's candidate for the commissioner's post was examined by a parliamentary committee.

Following this ordeal, she was appointed "officer of Parliament,"[30] a status that makes her truly independent from government and the administrative machinery. The Commissioner files her annual reports with Parliament. Upon the recommendation of an independent advisory group on the funding of "officers," Parliament approves her budget.

The legislator has vested the commissioner with powers akin to those of an ombudsman; therefore, she can only make recommendations. While she does not have at her disposal all the arsenal of a court, she can use broad powers to gather the evidence necessary to her audits and investigations. The Commissioner relies on the prestige of her post to encourage respect of the two acts she administers. In her annual reports, she can reprimand recalcitrant federal institutions. She can also release any information she deems in the public interest on practices of private sector firms in their management of personal information.

---

[25] *Act respecting the Protection of personal information in the private sector*, R.S.Q., c. P-39.1

[26] *The Personal Information Protection and Electronic Documents Act,* 2000, ch. 5.

[27] Final report of the Information Highway Advisory Council (IHAC) - *Connection, Community, Content: The Challenge of the Information Highway*, Ottawa, Department of Supply and Services, Canada, 1995: pages 163 and following.

[28] In late spring 2007, the House of Commons' Standing Committee on Access to Information, Personal Information Protection and Ethics completed its five-year review of this Act. Its final recommendations have yet to be tabled and approved by the House.

[29] This 'first' occurred in particular circumstances, to say the least, after the former commissioner charged with contempt of Parliament resigned in June 2003. See the work of the Standing Committee on Government Operations and Estimates, session of November 4, 2003.

[30] On this notion of "officer of Parliament," see: Paul Thomas, *ThePast, Present and Future of Officers of Parliament,* Canadian Public Administration/Administration publique du Canada, Vol. 46, No. 3 (Fall/Automne 2003), p. 287–314.

The Commissioner can lastly refer to the Federal Court cases that have not been settled to her satisfaction and in which citizens' rights are threatened. Nearly all recommendations made by the commissioner, however, are implemented without the need to resort to a court order.

With the support of Assistant Commissioners, the Commissioner manages the control authority's staff of about 130. The Office of the Privacy Commissioner (OPC) includes seven branches: Research, Analysis and Stakeholder relations; Investigations and Inquiries; Audit and Review; Legal Services and Policy; Public Education and Communication; Human Resources; and Corporate Services.

The Canadian way

The Canadian system does not require any declaration nor prior authorization of data processing. The federal Act of 1982 does not make any distinction between types of personal information; thus, the notion of sensitive information is absent from the law.

The Canadian system aims at ensuring the respect of citizens' rights, an objective that presupposes from the commissioner the implementation of corrective measures and education programs. Examination of complaints filed by citizens, public information campaigns, and audits are the tools we find in the kit of the commissioner and her staff.

In most cases, complaints are dealt with informally by the OPC staff. The goal of the dialogue engaged with the parties is to come to a satisfactory agreement. Indeed, most of the 1,600 justified complaints filed with the OPC in an average year are settled out of court.

Since 1982, the Commissioner can initiate an audit or an investigation, which gives her true power. We saw it in 2006 when a large consumer credit rating agency sought a court order to prevent OPC investigators from auditing their systems and procedures.[31]

The enforcement of a personal information protection system in the federal public administration rests on "Canadian-style" job-sharing. Thus, the Treasury Board Secretariat, one of the government's central agencies, is responsible for setting standards and regulations on personal information protection. One of the branches of the agency acts as advisor to departments and organizations and holds training sessions for civil servants. The Justice Department retains its function as the government's legal counsel in the matter. Finally, the Department of Industry—which was behind the law governing the private sector—continues to play an important role in assessing provincial legislation on the private sector.

[31] Privacy Commissioner of Canada, *Report to Parliament 2006*, Ottawa, Public Works and Government Services Canada, 2007, p. 25.

The way of initiatives

This Canadian way may seem complex. But it encourages plural initiatives. Thus, Canada became the world's first country to require a "privacy impact assessment" (PIA) from all departments and agencies before launching or modifying programs that can have an impact on privacy. They are true feasibility studies that are meant ultimately to establish a culture of safeguarding privacy and personal information throughout the government apparatus.

The PIA techniques and procedures were developed by the Treasury Board Secretariat, which even worked out training on-line for those responsible for such projects.[32] It is a multi-disciplinary process that requires the co-operation of government experts, outside consultants, large computing, accounting and auditing firms. The results of those assessments must be submitted to the Privacy Commissioner before the new programs go into effect. The Commissioner can propose a strengthening of the programs' policies, practices and administrative framework. The goal, of course, is to prevent or minimize the risks of excessive intrusion on privacy and abuse of personal information.

Naturally, the Commissioner also initiates measures encouraging practices respectful of the citizens' right to protect their personal information. She has thus put out a list of precautions to take against various forms of surveillance—from video cameras to spy software that could be used in the workplace. She has also published identification and authentication guidelines that are much appreciated in a country that has no national identity card nor a population register.

The federation and the world

The federal commissioner maintains close contact with monitoring bodies throughout the Canadian federation and its "territories". With her counterpart, the Information Commissioner, she gathers the heads of the Canadian federation's control authorities twice a year. She regularly hosts foreign missions of jurists and senior officials from Mexico, China, Japan and elsewhere involved in the drafting or implementation of personal information protection legislation.

Over the past few months, the Commissioner directed the work that led to the final draft of the new OECD guidelines on cross-border co-operation in the enforcement of privacy laws.[33] She has also joined in the discussions of jurists and experts from the Asia-Pacific Economic Cooperation (APEC), who are drafting personal information protection guidelines for that world region.

Some months ago, the head of the investigation branch and a member of the legal branch of the OPC took part in a meeting of the "Article 29 Working Party" at the seat of European institutions, in Brussels. They explained to representatives of the European Union's 27 monitoring bodies the steps taken by Canada in what has come to be known as "the SWIFT

[32] See on this topic the following documents on the Treasury Board's Web site: The Policy on Privacy Impact Assessments (PIAs), The Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risk (www.tbs-sct.gc.ca).

[33] OECD, *Recommendations on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*, Paris, June 2007, 11 p.

affair."[34] This novel initiative provided a concrete example of the particular role played by the federal Commissioner in a sensitive case stemming from the war on terrorism declared by the United States following the events of September 11, 2001.

[34] The SWIFT affair, named after a company specializing in the electronic transfer of banking data and based near Brussels, refers to the disclosure of personal information as a result of pressure exerted by US authorities following the September 11 attacks. The "Article 29 Working Party" conducted an investigation and the European Commission found that SWIFT violated certain provisions of the European directive of 1995.

France

The Commission nationale de l'informatique et des libertés

The CNIL is undoubtedly the best-known acronym among people responsible for the protection of personal information. The Commission nationale de l'informatique et des libertés is a pioneer organization, in the strongest sense of the term. By creating the CNIL in 1978, the French Parliament set a precedent in the political landscape of the Vth Republic. It instituted the first independent administrative authority (IAA).[35]

The adoption by the National Assembly of the 1978 Act on "data processing and freedoms" and the establishment of the CNIL gave an institutional response to the perception of the problem posed by the appearance of the first generation of "giant computers," as they were then called. The alarm bell had been sounded a short time before by an article published in 1974 in the daily *Le Monde*.[36] The plan to create a super file of the entire French population, doubled with the attribution of a unique identifier for every citizen, had deeply troubled a certain number of senior officials and some intellectuals. The SAFARI Affair had first led to the creation of a working commission that was to propose to the government the drafting of the 1978 Act.

The legislative process

Observers and jurists cannot help but be impressed by the French Act of 1978. It covers both the public and the private sectors and all information that makes it possible to identify a person and to distinguish one person from another. It places under the authority of an original college—the CNIL—the supervision and control of the numerous provisions that make up a true system of data processing and use of personal information files.

Following the adoption of a directive on personal information by the European Union in 1995,[37] the French Parliament substantially modified its act in 2004, but without changing the nature of the CNIL.

The 2004 Act includes important provisions that open new directions for the CNIL, such as the authority to impose financial sanctions[38]. This measure is fraught with consequences: the CNIL can impose financial sanctions which, in the event of a second offence, may reach as much as 5% of a company's turnover.

---

[35] Independent administrative authorities have multiplied in France these past few years. They are institutions established outside the usual departmental structure. Their mandate is horizontal and they often exercise control activities. See on this topic: Grégory Maitre, "Autorités administratives indépendantes : l'état des lieux," *Les autorités administratives indépendantes,* Paris, La Documentation française (Collection Regards sur l'actualité), 2006, p. 16.

[36] Philippe Boucher, "Safari ou la chasse aux Français," *Le Monde,* March 21, 1974.

[37] European Parliament and Council directive 95/46/CE of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[38] Amended law of 6 August 2004, Chap. VII, s. 45–59.

A collegial institution

A true collegial institution, the CNIL is in a way a microcosm of the French political system. The institution reflects and expresses the pluralism of France's public powers. From the President of the Republic to the Economic and Social Council, the Council of State, the Court of Cassation and the Revenue Court, the various authorities appoint or vote on a certain number of the 17 CNIL members, who are named for a five-year term.

As an independent administrative authority, the CNIL has a fair degree of latitude. "The government, in principle, exercises no supervision nor any hierarchic power." [Translation][39] The government refers bills or regulations that could have an impact on data protection or the respect of privacy to the CNIL. Its opinions, relayed to Parliament and made public, are often carried in the media. They are not binding on the government. The latter maintains a link with the CNIL through the presence of a representative, who does not take part in the Commission's deliberations.

CNIL members elect their chairman, who is seconded by two vice-chairmen, also elected. Decisions, opinions or recommendations are decided at two or three monthly plenary meetings. It is at that level that the collegiate character of the organization is most apparent. Each member of the college is given the responsibility of a particular sector—economic affairs, social affairs, cultural affairs, justice, security, territorial communities, labour, health, etc. Each acts as CNIL's external representative and as reporter to the Commission. Finally, the chairman, the two vice-chairmen and three other members elected by their peers make up CNIL's "restricted group" that, under the 2004 Act, is in charge of applying sanctions.

Employees are hired by the CNIL and are either contract workers or seconded from the public service. They are distributed among three divisions within the CNIL—the legal, international affairs and expertise division, the user relations and controls division, and the human, financial and administrative resources division—and two departments—external and internal communication, and information and documentation. Staff members prepare the cases commissioners will have to decide on. They handle day-to-day contacts with the country's citizens, organizations and enterprises, as well as with their counterparts of the European Union and third countries.

The CNIL imprint

The CNIL upholds the enacted rules and principles to protect individual freedoms and citizens' privacy. In accordance with the 1978 Act, it has implemented a series of procedures requiring a prior statement of sensitive data processing or handling (religion, union membership, ethnic origin**,** etc.) and the constitution of a "file of files" recording all those statements.

To avoid confining the supervision of data processing to the bureaucracy, the legislator has invested the CNIL with a regulatory power. Thus, some 80% of current data processing is subject only to a simplified statement. Other data processing operations in the public sector were initially

[39] Martin Collet, "La création des autorités administratives indépendantes : symptôme ou remède d'un État en crise?" *Les autorités administratives indépendantes, op. cit.* (see note 1), p 7.

subject to a favourable opinion by the CNIL. Under the 2004 Act, this prior statement rule is maintained, but there are many possible exemptions. However, persons responsible for public or private files must seek the consent or prior opinion of the CNIL to proceed to so-called "high-risk" operations that could have serious consequences for individuals.

The Commission quickly set itself apart with of a novel doctrine that represented a major advance and from which France's tribunals, and even those of other countries, draw inspiration. This doctrine sets forth the basic principles that should govern the protection of personal data and ensure privacy.

The doctrine results in part from the examination of data processing projects and complaints filed with the CNIL. It also follows from the monitoring carried out through the years. The emergence of new technologies no doubt makes it possible to better grasp this aspect of the CNIL's work. The commission's expertise was deployed as early as 2003 in a close examination of the issue of radio-frequency identification (RFID)[40] and, in 2005, of nanotechnologies. Beyond the results of control operations carried out by CNIL computer engineers, this represents a forecast capability developed through a long collective, multidisciplinary experience.

In the wake of the deployment of various global positioning technology services, the CNIL had to clarify the latitude enterprises could have in the use of such devices to check, in the case of insurers, the speed of young drivers or the work effectively carried out by long-distance truck drivers.

Likewise, the rights of minors have been updated thanks to the summary of observations drawn from the collection of personal information from children on the Internet, and monitoring services have been set up for minors equipped with portable phones. These CNIL thoughts have led to various opinions adopted by all its European counterparts.[41]

Little by little, this doctrine has made its way into the legal community. Some of those principles have been cited before tribunals, particularly the State Council, France's highest administrative court, which has validated or confirmed a good number of CNIL theses.[42]

Perhaps more spectacularly, the CNIL has launched initiatives that have struck popular imagination. Thus, in 2002, the "Spam Box" operation collected in less than three months some 325,000 unsolicited e-mails.[43] It illustrated one of the scourges of electronic marketing and helped justify the European Parliament's initiatives in this regard.

---

[40] CNIL, Presentation by Mr. Philippe Lemoine on radio-frequency identification (RFID tags), October 30, 2003, session, 8 p.

[41] Article 29 Data Protection Working Party, Notice 5/2005 on the use of localization data for the purpose of providing value-added services. 2130/05/FR WP 115.

[42] As an example, see the State Council decision in litigation No. 262851 (July 28, 2004).

[43] CNIL, *Operation "Spam Box": CNIL teachings and actions about unsolicited electronic communications.* Report from Ms. Cécile Alvergnat, adopted on October 24, 2002.

New paths

In a pedagogic mode, the CNIL has taken advantage of the amended Act to promote the function of "freedoms and computer correspondent" (FCC). All entities covered by the Act are urged to appoint such a correspondent whose mandate is to encourage respect of the law in his community in return for a simplification of the procedures of prior data processing statements. This correspondent, who is not the file manager nor the person responsible for data processing, enjoys legal protection to discharge his consulting function independently. The CNIL has already set up a network of its correspondents and is gradually organizing a series of concrete activities to give upstream sense and weight to this function.

The CNIL is also conducting regional tours to establish direct contact with enterprises and other organizations that collect and use personal data. The CNIL's Web site is noted for its innovations and its features designed to inform as well as to raise public awareness.

Abroad

The CNIL has intervened early on the international scene. It first drew attention to the issue of personal data transfer from one state to another during the FIAT affair in the late 1980s.[44] The CNIL then outlined the basic principles that have largely inspired the provisions of the European directive governing the transfer of personal information beyond the European Union.

The CNIL also plays an important consulting role with some national commissions looking for models or support. This role was emphasized when new members joined the European Union. Jurists and politicians from Southern countries concerned with the protection of personal information also turned to the CNIL for help.

Within the International Conference of Data Protection and Privacy Commissioners created in the early 1980s, the CNIL wields obvious influence. Thus, the London Initiative launched in November 2006 at the instigation of Chairman Alex Turk[45] was supported by some ten different state commissioners. Faced with the double challenge posed by the speeding-up of new technologies and the wave of security standards, this proposal is intended to launch coordinated initiatives in information, communication and expertise, among others. It also encompasses the work that should lead to the effective recognition of a universal right to personal data protection.[46]

[44] Deliberation of July 11, 1989, in CNIL, *20 ans, les libertés et l'informatique, vingt délibérations commentées*, Paris, La Documentation française, 1998, p. 63.
[45] 28th International Conference of Data Protection and Privacy Commissioners, London, November 2006, "Communicating on data protection and making it effective," 7 p.
[46] This proposal had first been put forth at the 27th International Conference of Data Protection and Privacy Commissioners, Montreux Declaration, September 14–16, 2005).

Luxembourg

National Commission for Data Protection

The Grand Duchy of Luxembourg came both early and late to the introduction of a personal data protection system. This small country was indeed among the first states, in the 1970s, to take an active part in the work of the Council of Europe to develop specific rules and promote national legislation to safeguard the privacy of individuals in the computer age. It took nearly a quarter of a century, however, before an independent monitoring body was formed to uphold the principles of the innovative 1979 Act.

This paradox is part of the reality of a country whose population is less than a half-million, but which houses the headquarters of the largest iron and steel group and one of the largest money markets in Europe, if not the world. The history of Luxembourg in the area of personal data protection shows a real political will to guarantee citizens the respect of their privacy while taking into account the demands of a very particular economic development. This delicate but omnipresent reconciliation is achieved in tune with the European directives adopted in Brussels some time ago.

The legislative process

Following in France's footsteps, the Luxembourg Parliament decided at the end of 1979 to pass a law on the protection of personal data. This very strict legislation is structured around the principle of a personal information collection ban failing prior consent.

The Act was first amended in 1992.[47] This was when work began in Brussels on the European Union directive that was to radically change the face of personal information protection, certainly on the old continent, but also elsewhere in the world.[48] The Luxembourg government wanted, among other things, to subscribe to the rules adopted by the Council of Europe in 1980 on the cross-border transfer of personal information.[49]

In 2002, Luxembourg completely amended the 1992 Act[50] to fulfil the obligations imposed by the European directive in 1995. It should be recalled that the European Court of Justice had condemned the Grand Duchy for failing to translate into a national law within the allotted time the provisions of this mandatory directive for all member states of the European Union.

The movement gathered pace in February 2007 when the government announced it would table before the Chamber of Deputies a bill[51] that would significantly change the law enacted only

[47] Title of the 1992 Act.
[48] European Parliament and Council directive 95/46/CE of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[49] Convention for the protection of individuals with regard to automatic processing of a personal character (28 January 1981). Known as "Convention 108."
[50] Act of 2 August 2002 on the protection of individuals with regard to the processing of data of a personal character.
[51] Bill 5545 tabled before the Chamber of Deputies, March 6, 2006.

three years earlier. The bill implements the recommendations made by the monitoring body to streamline administrative forms and clarify certain difficulties of application.

The Luxembourg monitoring body

In the spring of 2002, Luxembourg dailies published in their career sections an ad soliciting applications for the three positions in the new National Commission for Data Protection (NCDP). The notice specified applicants had to be trained jurists or computer scientists. Among a preliminary list of candidates, the Minister of Media and Communications submitted his choices to the government. Finally, the Grand Duke, as head of state, ratified the appointment of the chairman of the Commission and the two other commissioners.

The new Commission took over from an advisory body formed in 1979 after the initial Act on the protection of data of a personal nature was passed, but that had never played a significant role. It should be pointed out that the legislator had not provided for any staff nor any administrative support for that organization.

The Luxembourg commissioners, appointed for a six-year term, have substitutes. Under the Chairman's administrative authority, they collectively decide how to carry out their mission and pursue the files and projects within their remit. The Commission is statutorily attached to the government through the Minister of Media and Communications. This ministerial control is essentially limited to the budget and the appointment and status of its employees.

The new Commission first had to recruit its staff within the public service, according to a scale stipulated in the Act itself. Today, roughly 10 people make up the staff of the monitoring body.

In a novel initiative, the legislator has entrusted the review of the NCDP's annual report to the Commission consultative des droits de l'Homme, which consists of representatives from civil society organizations particularly concerned with the defence of basic freedoms and the fight against discrimination, including, for example, Amnesty International. This commission, which advises the government every time human rights issues are at stake, plays the role of watchdog of the NCDP. In this capacity, in 2005, it issued a report approving the orientations of the NCDP stated in its first annual report.[52]

Grand Duchy style

In December 2005, a great many Luxembourg families were mailed a very special calendar. It was an NCDP initiative to promote, in a simple and intriguing mode, the discovery and appropriation of the purposes and principles of the privacy legislation. Moreover, the Commission had launched at its very beginning a well-targeted awareness campaign through information meetings with various economic and commercial sectors.

The calendar initiative brought to light one of the Commission's means of action. When their rights are threatened in this area, citizens are encouraged to go to the Commission, which can

[52] ACHR notice on the annual report of the National Data Protection Commission, March 7, 2005, published in appendix to the NCDP activity report for 2005 and 2006. See: www.cnpd.lu/publications/rapports/index/html.

then open an investigation. Such investigations can give rise to administrative sanctions, but the Commission favours an approach that is both conciliatory and educational.

It is in this frame of mind that the NCDP supports projects ranging from the establishment of e-government to the adoption of a VITALE-type medical smart card,[53] a step preceding doctors' centralized access to patient information.

The NCDP is also looking into the plan to reform the identity number assigned since 1979 to every citizen of the Grand Duchy, a reform made necessary by the dangers of such a system. In addition to restricting the use of this identifier to its own purpose, legislation will authorize, through technological tools tested in Austria, the development of sectoral identifiers derived from the national identity number, but that would not allow the interconnection of files unless formally approved by the NCDP.

The Commission can intervene in such areas of its own initiative or, in accordance with the European Union directive, when asked by the government to examine bills or regulations that can have an impact on the protection of personal data. The advice and recommendations of the Commission are automatically inserted into the documentation given to parliamentarians at the tabling of every bill.

The NCDP soon came up against a huge problem that prompted it to propose a major streamlining of administrative procedures dictated by law. In less than three years, more than 10,000 files piled up on its table. In most cases, the avalanche was due to the obligation made to companies and organizations to declare the existence of personal information files or to seek the approval of the Commission before processing these data. The Commission stressed above all public information, guidance and best practices for those responsible for files, and, if need be, assistance to citizens wanting to exercise their rights under the law.

The commissioners then drew important conclusions. They recommended that the government review the 2002 Act in depth, which led to the bill tabled in the Chamber of Deputies in February 2007.

A major reorientation

The bill seems to achieve the two main objectives set by the members of the Commission. First, it does away with much of the heavy procedures inherited from so-called first-generation laws on personal data protection. The whole aspect of prior declarations and authorizations will be considerably lightened. Only the obligation to declare to the NCDP the processing of data that truly involves certain risks will subsist.[54] This is a pragmatic answer to the Commission's simple statement of fact: all these measures bring no added value to the institution of a true culture of respect of privacy.

[53] The VITALE medical smart card has been distributed to more than 45 million persons in France since 2001. It specifies their right to the reimbursement of medical costs, but does not contain any medical information.
[54] Interview with Chairman Gérard Lommel, "Expliquer la loi, sensibiliser les citoyens," *Paperjam*, April 2007, p. 124.

In the same breath, members of the Commission want to enrich and broaden their educational effort and practice a form of guidance and awareness among those responsible for files both in the private and the public sectors. With regard to citizens, the objective is similar: "Instil or strengthen trust, be a force of proposals, a centre of competence that brings solutions in the data protection area," [Translation] according to the current chairman of the Commission.[55]

The NCDP's approach is also in line with the stated government practice of "maintaining the attractiveness of the Luxembourg site and preventing excessive regulation from having a deterrent effect on international groups anxious to settle in the Grand Duchy." [Translation][56]

At the heart of Europe

To summarize, the National Commission for Data Protection first turned to good account the experience of its neighbours—Germany, Belgium and France, among others. It is now attempting to make the most of its difference by embarking on an original path, centred on communication and constructive, even singular cooperation. It is maintaining course on the broad orientations set in Brussels and Strasbourg. This was evidenced by the glamour lent to "the European day of personal data protection," an initiative of the Council of Europe,[57] which has declared January 28 a day when Europeans should reflect on that aspect of their rights.

Within the international association of privacy commissioners, the Grand Duchy's monitoring body has adopted the slogan of the London Summit of November 2006: the communication strategy is "the central issue and today's prime concern" with regard to the protection of personal data.

[55] *Ibid*. p. 128.
[56] *Ibid*. p. 126.
[57] Interview with Chairman Gérard Lommel, "La confiance se mérite," *Le Jeudi*, January 25, 2007, p. 7.

New Brunswick

Office of the Ombudsman

When the *Protection of Personal Information Act* (POPIA) came into effect in 2001, the province's Ombudsman was given the responsibility of enforcing it throughout the government.[58] He adds to his functions the supervision of the *Right to Information Act*, in effect since 1980.[59]

In the spring of 2007, the Right to Information and Protection of Personal Information Task Force urged the province's citizens to offer their comments and suggestions on a Web site created for that purpose.[60] At the same time, the Personal Health Information Task Force began public consultations. A single sentence summed up the purpose of this measure: "The Government of New Brunswick believes the time has come for stronger legislation in our province to protect the privacy of personal health information."[61]

In short, the last Canadian province to pass personal information legislation went back to the drawing board to revamp an act that was not yet 10 years old.

The legislative process

New Brunswick had been the second province to adopt an access to information act in the late 1970s. On personal information protection, the same province lagged behind the rest of the Canadian federation.

Yet, as early as 1995, the Fredericton government had encouraged public and private organizations to commit firmly and voluntarily to the protection of personal information. This volunteer approach, as it was called at the time, was driven by the Department of Economic Development.

Obviously, the Fredericton government banked on the self-regulating approach taken in Ottawa at the behest of the federal Department of Industry that led to the adoption of the code of the Canadian Standards Association (CSA). It also followed with interest what was being worked out in the federal capital and at the seat of European institutions in Brussels.

In the late 1990s, the government changed attitude and opted for a formal legislation—the *Protection of Personal Information Act* (POPIA). "One of the main drivers in enacting POPIA," said the Ombudsman in a 2006 decision, "was so that the Government of New Brunswick and Canada in general could satisfy its trading partners, primarily in Europe, that transborder data

---

[58] *Protection of Personal Information Act*, Chapter P-19.1.
[59] *Right to Information Act*, Chapter R-10.3, sanctioned on June 28, 1978.
[60] Right to Information and Protection of Personal Information Review Task Force, *Working document on the review of the right to information and the protection of personal information*, Fredericton, Government of New Brunswick, 2007, p. 3.
[61] Personal Health Information Task Force, *Personal Health Information Access and Privacy*, Fredericton, Government of New Brunswick, May 2007, p. 4.

flow could be allowed in commercial exchanges without diminishing the level of privacy protection enjoyed by citizens there."[62]

The CSA code was the basis of the bill tabled by the government before the New Brunswick Legislative Assembly in 1998. It was undoubtedly one of the shortest such documents: 10 sections and, in appendix, the CSA code and a guide to interpret it. The new Act, which came into effect in 2001, covered only the public sector. It gave legal currency to a code developed by private sector representatives.

For want of provincial legislation, the private sector remained subject to the law passed by the federal Parliament in 2001. The federal Privacy Commissioner enforces it and acts as ombudsman for complaints and disputes arising in New Brunswick.

A multi-tasking ombudsman

By designating the Ombudsman to enforce the new act to protect personal information in the public sector, the New Brunswick Legislative Assembly was inspired by the example of Manitoba some years earlier. It also subscribed to the twinning of the right to information and personal information protection that had become the rule in all provinces of the Canadian federation after the precedent set by Quebec in 1982.

Since the creation of his post in 1967, the Ombudsman has inherited a number of mandates. He has jurisdiction to investigate citizens' complaints of an administrative nature against government departments, municipalities, school districts, district education councils, regional health authorities, Crown agencies and a number of agencies responsible to the province. He also defends children's rights. He relies on the moral authority of his function to discharge his numerous mandates. He is an officer of the Legislative Assembly and reports directly to it.

The Ombudsman's office has a relatively modest staff to fulfil the different mandates it has been entrusted with in the past 40 years: 14 employees and a legal counsel. Three staff members are assigned part-time to processing the files of both the right to information and personal information protection.

In the Executive Council Office—senior decision-making body of the public service that comes under the Premier—one person is responsible for implementing POPIA throughout the administrative machinery. That official informs and advises the representatives of the various departments and agencies responsible for enforcing the Act.

Dealing with cases

The ombudsman has received very few complaints since he has taken on this new function. However, within a few months, two major cases have drawn the attention of the media and the public in the area of personal information protection. One of the Ombudsman's interventions even led to the resignation of a minister!

[62] Shawn Graham and Edgar Vienneau v. Minister of Transportation and Premier's Office, Investigation report and recommendations by Ombudsman Bernard Richard, Fredericton, September 15, 2006, p. 10.

Shortly after taking office, the new ombudsman asked a retired judge to investigate a complaint made by a member of the Opposition against a government minister, who had disclosed personal information about an Opposition member inside and outside the Legislature. At the end of his investigation, the judge found the minister had infringed three basic principles of the CSA code integrated into the 1998 Act.[63] Within the next several hours, the minister tendered her resignation to everybody's surprise.

In a similar case, the Ombudsman took up a complaint by the leader of the Opposition against the minister of Transportation and the Premier's Office. In a carefully-written decision, the ombudsman concluded that two deputy ministers had departed from one of the principles of the statutory practice code of POPIA. He worried particularly about the misuse of the new Act for partisan purposes, hence the interest stirred by this investigation report, publicized contrary to the usual reserve of the Ombudsman's office.

Future prospects

The current New Brunswick Ombudsman is obviously awaiting the results of the task forces reviewing the 1998 Act. They are not expected to recommend legislation covering the private sector. What about the Ombudsman's mandate regarding the current law governing the public sector?

Pending their reports, the Ombudsman is proposing an ambitious program of legislative reform. He is recommending a new Information and Privacy Rights Code based on basic human rights. The Code would assemble all legislative provisions on privacy and access to information and apply to both the public and the private sectors. Rights would be enforced by an independent office vested with broad, effective ruling and investigative powers.

On the international scene, the Ombudsman feels this model could be useful in countries whose government structures are not firmly fixed in history and cannot multiply agencies or supervisory bodies. It is a minimalist solution that could inspire certain states in the French-speaking world interested in implementing a personal information protection system.

[63] Stuart G. Stratton Q.C. (proxy of the Ombudsman of New Brunswick), *Privacy Report,* Fredericton, July 21, 2005, p. 39.

Quebec

Commission d'accès à l'information

In 1982, the Quebec National Assembly caused a real stir by passing legislation encompassing both access to information and the protection of personal information in the public sector.[64] This decision ran counter to precedents set in Europe where a clear distinction was made between those two legislative topics. Likewise, by entrusting the supervision of the two parts of the new law to a single body, the 1982 Act established the "Quebec model."[65]

In early January 1994, another stir on the North American continent: legislation on the protection of personal information in the private sector. In Canada's federal capital, they had difficulty hiding their annoyance. The National Assembly's decision did not go unnoticed in Washington either at a time when the European Union was considering its 1995 directive, which would include an important provision concerning other countries.[66]

The legislative process

Thanks to the interest of some political leaders for… access to information, Quebec came to the protection of personal information in the mid-1970s. Premier René Lévesque's personal support gave final impetus to a project that had not been a topic of much public debate.[67]

The 1982 Act followed directly from the work of a study committee set up to examine the feasibility of legislation including both access to information and personal information protection. The National Assembly unanimously passed the law creating the Commission d'accès à l'information (CAI), which oversees the two systems.

The National Assembly completed its personal information protection system in June 1993 by adopting, again unanimously, *An Act respecting the protection of personal information in the private sector.*[68] Two factors explain this decision that many found somewhat exotic at the time. First, there was the inclusion of specific provisions on the respect of privacy and personal information in the new *Civil Code of Quebec*.[69] Then, the progress of the European Commission toward the adoption of the 1995 directive in Brussels was closely followed by the Quebec government.

---

[64] *An Act respecting access to documents held by public bodies and the protection of personal information*, R.S.Q., chapter A-2.1.

[65] Professor Herbert Burkert (University of St. Gallen, Switzerland) was the first to use this expression about the 1982 Quebec legislation in his PhD thesis. See *Informationszugang und datenschuntz. Ein Kanadiesches Beispiel* (Nomos : Frankfurt am Mein 1002).

[66] European Parliament and Council directive 95/46/CE of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[67] André Larocque, "La réforme électorale. L'héritage démocratique du Premier ministre René Lévesque," *Cahiers de recherche éthique* 21, Montréal, Fides, 1997, p. 339–342.

[68] *An Act respecting the protection of personal information in the private sector,* R.S.Q., c. P-39.1.

[69] S. 35–41 of the *Civil Code of Quebec* (S.Q. 1991, c.64).

The National Assembly finished reviewing both acts in 2006 following a long process. The 1982 Act provided for a review every five years—an obligation seen through in 1990. Since then, every attempt made to modify the act has been abandoned.[70] On the eve of the 25th anniversary of its public sector legislation, Quebec overhauled its personal information protection system and the mandates of the monitoring authority that is the Commission d'accès à l'information.[71]

A complex body

The Commission d'accès à l'information is a collegial, complex and plural organization: administrative tribunal, advisory body and monitoring body all at once.[72] The President and the four other CAI members are elected for a five-year term by a vote of two thirds of the National Assembly. Their candidacy is first submitted to the Opposition leader by the Premier. Tradition favours their unanimous election to bolster their credibility.

The Commission is made up of two distinct sections: one jurisdictional and the other supervisory. It is a collegial body. The President has administrative prerogatives only. Each member exercises specific powers on behalf of the Commission.

Commission members have a peculiar status, to say the least. They are appointed by the National Assembly and sworn in by its President.[73] However, the Commission tables its annual report to the National Assembly through a minister responsible for the independent organization and the enforcement of the Act.[74] The CAI budget is allocated by this minister, who acts as government advisor on personal information and access to information and can appeal to the Commission for this purpose. He also has a duty to assist departments and organizations in enforcing the Act.

From the outset, the minister responsible surrounded himself with a small number of officials, sometimes even with a directorate general of access to information and personal information protection whose size and importance have varied through the years. It is with the help of that team—the Secrétariat à la réforme des institutions démocratiques et à l'accès à l'information (SRIDAI)—that the minister responsible has just completed the statutory review of the Act and is to draft related regulations for Cabinet. This access directorate, as it is called in Québec City, also acts as government advisor and effectively answers requests and questions from departments and agencies.

---

[70] Bill 451, *An Act modifying the Act respecting access to documents held by public bodies and the protection of personal information, the Act respecting the protection of personal information in the private sector and other legislative provisions,* came to nothing after being tabled in 1998. The same happened to Bill 122 , tabled in June 2001. In both cases, the Cultural Commission of the National Assembly held public consultations as in May 1994.

[71] *An Act modifying the Act respecting access to documents held by public bodies and the protection of personal information and other legislative provisions,* S.Q. 2006, c. 22.

[72] Paul-André Comeau and Maurice Couture, "Accès à l'information et renseignements personnels : le précédent québécois," *Canadian Public Administration / Administration publique du Canada*, Vol. 46, No. 3 (Fall / Automne 2003), p. 368 *et seq*.

[73] For all that, they are not senior officials nor, in Québec City officialese, "persons appointed" by the National Assembly, like the Auditor General or the Lobbyists Commissioner.

[74] For some time now, the minister responsible for Canadian Intergovernmental Affairs, Aboriginal Affairs, Francophones within Canada, the Reform of Democratic Institutions and Access to Information has held this responsibility.

The CAI has a staff of about 45 managers, professionals and officials, including the President and commissioners. All are from the public service and are distributed among four departments: legal affairs, analysis and evaluation, secretariat, and administration.

Finally, the Association de l'accès et de la protection de l'information (AAPI) groups the individuals responsible for access to information and personal information protection throughout the public sector, including decentralized agencies. The AAPI is intended as a centre for work and dialogue.[75] It offers its members online training courses and holds seminars and meetings.

At work

The Quebec personal information protection system encompasses the public and private sectors, in accordance with the policy followed in Europe since the 1970s. The two acts of 1982 and 1993 enjoy a special status in Quebec's legal arsenal. They have been elevated to the rank of "preemptive legislation" and, as such, have precedence over all other laws and regulations. To depart or shield from them a single provision of a new act or amendment of an act, the National Assembly must expressly state it, that is, resort to en exemption clause.

The Quebec legislator did not prescribe a declaration of files or an authorization request prior to data processing, nor did the two acts of 1982 and 1994 do not make a distinction either between types of personal information. However, some sectoral legislation, particularly in the health sector, recognizes the existence of sensitive data, without so much as using that term, and provides for special measures in handling them.

The Quebec system is structured around the life cycle of personal information. Each stage of this cycle—collection, use, disclosure, retention and disposal—must be surrounded by steps and precautions guaranteeing the respect of citizens' rights, in accordance with the basic principles of the *Civil Code* and the two protection of personal information acts. The Commission d'accès à l'information sees to the application of those principles. It discharges that broad mandate by developing preventive and corrective measures.

The Commission may, of its own initiative, make recommendations on any bill or regulation. Its prior intervention is mandatory in some personal information exchange projects between departments or agencies. Its advice is not binding on the government, but if disregarded, it must be published in the *Gazette officielle du Québec*. This transparency requirement also applies to all personal information files held in the public sector. Finally, the CAI must be informed prior to the creation of any biometric data bank, and can give its advice or even issue an order on this matter.

Original avenues

What is the definition of personal information? In what circumstances could access to an individual's medical file be denied to him or her? How far can we go in crossing off personal information included in a file? These are some of the issues dealt with in the case law developed

[75] See the Association de l'accès et de la protection de l'information website, at www.aapi.qc.ca.

through decisions of the Commission.[76] Those decisions of the legal affairs department conclude the adversary hearings held by the Commission to settle a dispute. CAI decisions are binding and, in some cases, may be appealed to the Court of Quebec, hence the development of this jurisprudence.

With the multiplication of surveillance cameras in public places, the Commission regulated video surveillance in 2004 to safeguard the individuals' right to privacy. Beforehand, it held public hearings in Montréal and Québec City, where a score of companies, police services, departments and hospital organizations submitted briefs.

On an average year, some 100 researchers, especially in the fields of human sciences and health, seek the advice of Commission d'accès à l'information before undertaking their work. This procedure, required by law, is intended to protect the privacy of citizens whose information is deemed essential to the research. Little by little, CAI requirements have spread through the codes of ethics adopted by both researchers and organizations whose personal information files are coveted for research purposes.

Abroad

The model developed by Quebec—a single piece of legislation, a single monitoring body for access to information and personal information protection—has spread first within the Canadian federation where most other provinces have adopted it.[77] Later, Hungary (1992), the United Kingdom (2000), Germany (2001) and Switzerland (2004) followed the same path.

In the mid-1990s, the Commission d'accès à l'information joined in the work undertaken at the seat of the European Union in Brussels to examine the potential impact of the use of the smart card in health services. It even co-chaired two research groups sponsored by the European Commission.

Finally, shortly after its inception in 1987, the CAI hosted one of the first international conferences of personal data protection and privacy commissioners at a time when states having such legislation were not legion. In 1997, it was behind an international conference whose theme—Privacy Without Borders—echoed one of the concerns arising from globalization. In September 2007, the table is set for the creation in Montreal of an international conference of all monitoring bodies within the Francophonie.

[76] See the site of the Commission under 'CAI Decisions' the section *Jurisprudence:* www.cai.gouv.qc.ca
[77] See table on this topic in Paul-André Comeau and Maurice Couture (cited in note 8): pages 372 and 373.

Romania

National Authority for the Control of Personal Data Processing

At the seat of the National Authority for the Control of Personal Data Processing in downtown Bucharest, a foreign visitor may be puzzled by the constant stream of this country's citizens.[78] They are greeted by staff members of this barely two-year old organization. They can get any information they need to understand a law intended to ensure that an aspect of their fundamental rights is upheld.

When it joined the European Union on January 1, 2007, Romania had legislation and a personal data control authority that met the requirements of the directive adopted in 1995 by the European Council and Parliament. It was due to the initiative of the first ombudsman—or people's advocate—that this Balkan state firmly embarked on this road even before negotiations began to join the European Union.

The legislative process

The step taken by Romania corresponded to the will asserted after the regime change of 1989 to install the components of a true constitutional state. This resolute choice explained the inclusion in the constitution of a concrete provision on personal data or information.[79] Hence the legal foundation of the campaign led by the Republic's Advocate of the People for the adoption by Parliament of a personal data protection system in line with of the current practice in most Western European and some Central European states.[80]

In subscribing to this objective in 2001, the Romanian parliamentarians killed two birds with one stone. They first broadened and fleshed out the sphere of individual rights. Their decision also fell within the scope of an objective pursued by Bucharest from the early 1990s: membership in the European Union whose member states had just significantly widened the door by signing the Treaty of Maastricht.

The text of the 2001 Act,[81] which indiscriminately covers the public and private sectors, is obviously inspired by the 1995 European directive.[82] Besides, the legal offshoot came about through co-operation between Romanian jurists and European Commission experts.

---

[78] This text has not been reviewed by the President of the National Authority for the Control of Personal Data Processing of Romania.

[79] Romanian Constitution published in the *Official Monitor of Romania*, Part 1, No. 233, November 21, 1991, approved by the national referendum of December 8, 1991.

[80] After the regime change in late 1989, many Central and Eastern European countries—the CEECs, in European Union lingo—quickly adopted legislation on personal information protection. So did Slovenia in 1990, Hungary in 1992, Poland in 1997, the Czech Republic in 2000, to mention a few, all now members of the European Union.

[81] Act No. 677/2001 for the protection of individuals with regard to personal data processing and the free movement of such data. [Translation of the title of the Act adopted by the Bucharest Parliament].

[82] European Parliament and Council directive 95/46/CE of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

The control authority

When the law on personal data protection was passed by Parliament, the Advocate of the People was given the mission to set up a unit or a department within his office to fulfill these new mandates.

In 2005, Parliament called this arrangement into question. From a strictly legal point of view, there was an obvious contradiction. The power of sanction the Advocate of the People was vested with in matters of personal data protection was hardly compatible with his status as mediator merely empowered to make recommendations. Furthermore, under the 1995 European directive, the control authority had to be independent of the government.[83] Hence, the creation of a free national authority in 2005.

Parliament appoints the President and Vice-President of this control authority for a five-year term. Candidates for both positions, necessarily jurists, are previously submitted to Parliament by all political parties. The final choice is incumbent on a Senate commission that fulfils this task by interviewing the candidates in a public session.

The Romanian supervisory body is directly attached to parliament, more particularly to a Senate commission. Its annual report is filed with this commission before being published in the *Official Gazette of Romania.* The body's normative decisions and guidelines get the same treatment and are, therefore, widely circulated.

The control authority's independence is also reinforced by the allotment of its annual budget which appears in the state's budget estimates under a distinct heading. In case of disagreement with the government over the budget, the president of the control authority can, under a provision of the law,[84] ask Parliament to clear up the matter.

The 2005 Act was completed one year later by a regulation that determines the staff and makeup of the control authority.[85] The body had less than 40 employees in the spring of 2007—most of whom had started out under the Advocate of the People—but can have as many as 50. Newcomers will be hired by the President, who manages the organization.

In accordance with this very detailed regulation, the control authority includes seven branches or departments with specific mandates, ranging from the conduct of investigations to the transfer of personal information to another state, and legal affairs.

[83] *Act No. 102/2005 on the creation, the organization and the functioning of the National Authority for the Control of Personal Data Processing.* [Translation].
[84] S. 17 of the 2005 Act.
[85] *Regulation on the organization and functioning of the National Authority for the Control of Personal Data Processing* [Translation].

The authority's beginnings

The Romanian control body must of course uphold the mandate and obligations set by legislation modelled on the European directive. Thus, it has already given advice sought by government on a number of bills or regulations and made recommendations. In addition to the investigation of complaints filed, among others, against banks or credit agencies, a joint investigation was conducted with the Italian monitoring authority.[86] Finally, the Romanian authority has exercised a few times the power of sanction vested in it by the legislator.

The control authority has been particularly prolific in devising initiatives to inform and educate the public. Thus, Romanian citizens have been able to better understand the meaning and importance of the protection of their personal data thanks to the tips that scroll regularly at the bottom of the screen on community television channels.

Staff members have held information seminars in various sectors of economic and social activity. They have also organized meetings in various regions of the country to inform the public of the objectives of the law and the services offered to citizens.

On the European front

Even before Romania joined the European Union, the control authority had subjected itself to an audit of its operations, structure and procedures by experts from the European Commission. Brussels gave full marks to the efforts deployed by Bucharest.

Throughout the negotiations with the European Union, officials of the control authority took part in the meetings and work of the European Commission's Article 29 Working Party.[87] The habit was formed and today the Romanian body takes an active part in projects led by this group in fields at the leading edge of progress, like biometrics and the many forms of e-government.

At the last conference of heads of states or governments of Francophonie countries held in Bucharest in October 2006, Romania was plunged into the heart of the work carried out for nearly a quarter of a century by persons responsible for personal data protection. This is when the call was launched for the development of a worldwide restrictive legal instrument to protect personal information.

From the wise provision inserted into the brand new constitution to the Francophonie summit, Romania's journey toward personal data protection has been steady.

[86] The "Garante per la protezione dei data personali."
[87] Under section 29 of the 1995 directive (see note 4), the European Commission formed a permanent group—the Article 29 Data Protection Working Party—bringing together representatives from control authorities of all member states.

Switzerland

The Federal Data Protection and Information Commissioner

Faced with the dazzling development of data processing and the fears it gave rise to, Switzerland introduced a personal data protection system in 1992. Two crises also shook public opinion. In both cases, it was the discovery of police control files that alerted the media and moved the federal Parliament to act.

In 2004, the federal Parliament passed a law on access to information based on the search for greater administrative transparency. As regards access to official documents, the mediation mandate was entrusted to the Federal Commissioner, who was already responsible for the monitoring of personal data protection.[88]

The legislative process

Nearly 20 years elapsed between the time the issue was first raised in the federal Parliament and passage of the 1992 Act. The discovery in 1974 of a file put together by a retired colonel listing sympathizers to extreme left wing causes and revelations in the early 1990s about a secret super file compiled by the federal police were the major incidents that marked the road toward the creation of a personal data protection system.

This parliamentary process first led to the creation of two commissions of experts, who drafted a bill. Then, in 1983, the government launched a wide public consultation. The federal administration, with the help of experts, continued to work throughout those years. In 1988, government tabled a bill in due form before Parliament.

The 1992 Act[89] set up a general personal information protection system in the federal public sector and the private sector, inspired by the OECD guidelines proposed in Paris in 1980.[90] It implements the basic principles set forth in the Convention adopted by the European Council in 1981.[91]

The development of the law followed a systematic examination of the legislation already in place, particularly in Germany, Austria, France and Scandinavia. The Swiss legislator had to wrestle with the barely concealed resistance of the economic and financial community and the no less fierce suspicion of part of the administration to achieve this result. We can no doubt surmise in

[88] *Federal Act on the principle of transparency in the administration of 17 December 2004.* With this law, the Bern Parliament in some way subscribed to the precedent established by Quebec in 1982. See on this topic: Paul-André Comeau and Maurice Couture, "Accès à l'information et protection des renseignements personnels," *Canadian Public Administration / Administration publique du Canada*, Vol. 46, No. 3 (Fall / Automne 2003), p. 364–389.
[89] *Federal Act on data protection* (DPA) of June 19, 1992.
[90] Council recommendations on guidelines governing privacy protection and the cross-border flow of data of a personal character (September 23, 1980), Paris, ISBN – 92 – 64 – 19710 - 2.
[91] Convention for the protection of individuals with regard to automatic processing of data of a personal character (January 28, 1981); hereafter referred to as "Convention 108."

this legislative process the search for a broad consensus, an important feature of that country's political and social life.

In 2004, the federal Parliament brought significant changes to the personal information protection system,[92] through the determined intervention of two parliamentary commissions that wanted to increase the transparency of personal data processing. They wanted at the same time to surround with tight precautions pilot projects involving the use of sensitive data and personality profiles. The review also introduced an incentive standard for software providers and individuals responsible for data processing: the legislator recommends that they submit their systems and procedures to an evaluation by independent, registered certification organizations.

This legislative amendment has enabled Switzerland to ratify the protocol of Convention 108 of the European Council on control authorities and the cross-border flow of personal data. It also reinforces the powers of the controlling body with regard to legal procedures. Likewise, sectoral law integrates some of the provisions implemented within the European Union to which the Swiss government has decided to subscribe.[93]

Federal Commissioner

The Federal Data Protection and Information Commissioner manages the day-to-day supervision of legal provisions on the protection of personal data. He also oversees the mechanism enabling citizens to have access to "official documents" produced and held by the federal public sector, and provides mediation when the application is turned down.

The Federal Commissioner is appointed by the Federal Council—the government—and is administratively attached to the Federal Chancellery. He operates without outside control, relying on a permanent secretariat of some 20 people, most of them jurists or computer scientists, headed by the Deputy Commissioner. They are career public servants from the federal administrative apparatus.

The Federal Commissioner files every year with the government a report that is published. In addition, he regularly appears before parliamentary commissions on matters within his remit.

The cantons of the Swiss Confederation also have control and monitoring bodies, as do some cities, beginning with Zurich, the country's largest city. The Federal Official has no authority over those bodies, which in practice complete the overall system set up in Switzerland to enforce the law on personal information.

The Swiss way

The Federal Commissioner acts as adviser to the Swiss Parliament and government. The law states that he must be consulted about bills and regulations that may affect privacy or the protection of personal information. He does not have direct access to the government; the

[92] *Federal Act on data protection* (DPA), June 20, 2006, statement.
[93] Particularly the Schengen Agreement on the free movement of individuals within certain countries of the European Union and the adoption of a protocol to Convention 108 of the European Council.

Chancellor of the federation relays and, if need be, defends the Official's proposals before the Federal Council.

The Federal Commissioner has control, advisory and information duties. He also has a mandate to examine complaints filed with his office. His inquiries may lead to recommendations to both public and private sector organizations. Unlike the CNIL, for example, he cannot impose sanctions, which does not seem to lessen the effectiveness of his actions.

The Federal Commissioner can only issue recommendations. If his decisions are ignored or dismissed, he can appeal to the new Administrative Tribunal, which will make a decision if the recommendation is directed at a person responsible for processing in the private sector. If the recommendation is directed at a federal organization, the Federal Commissioner will soon be able to refer the matter to the Administrative Tribunal.

In Switzerland, the power of recommendation is somewhat akin to heavy artillery. In the business and banking sectors, the dread of any form of negative publicity a public recommendation could entail is a strong incentive to find a solution together with the Commissioner. Another indication of this power's weight is the fact that recommendations from the Federal Commissioner can now be referred to the Administrative Tribunal.

The road to innovation

In the search for concrete solutions to citizens' problems, the Federal Commissioner does not hesitate to borrow from the latest technologies. Thus, he convinced the management of a supermarket chain to use an encryption technique that hides the faces of persons captured by the video surveillance cameras installed nearly everywhere in stores.[94] If needed, these pictures can be "unscrambled" by a person or an authority designated for this purpose, as is done with phone-tapping.

In a similar vein, a sports centre has given up storing its customers' biometric data in a central file in an avowed attempt to develop customer loyalty. The centre's management has agreed to offer its customers a card equipped with a microprocessor—commonly called a smart card—which contains some biometric data. At the centre's entrance, a machine checks whether the data on the card match the bearer's physical characteristics.

Moreover, Swiss firms have formed an association to ensure the defence and promotion of their viewpoints. The group does not hesitate to differ from the solutions proposed by the Federal Commissioner. It also organizes seminars and training workshops for people responsible for personal data protection in companies and organizations.

The Federal Commissioner has caused a small revolution in the world of control organizations by announcing in May 2007 his decision not to answer every individual application addressed to him and not to investigate every complaint filed with his secretariat. The meagre financial resources allotted to him have encouraged him to set up a "personalized telephone counsel service" at set

[94] This technology was developed at the École polytechnique fédérale of Lausanne and has just been marketed.

hours of the day[95] and to develop his Web site. Complaints are collected, however, and integrated into monitoring activities, if need be.

The enactment of the law on access to information and the resulting increased workload without additional resources are not irrelevant to this measure, which has forced a reorganization of the Federal Official's services. Two units of his administration now dedicate their time to the various tasks related to the protection of personal information, and a third implements the section on administrative transparency.

World outlook

In the matter of personal information protection, the Swiss monitoring body participates closely in the legal process developed in Strasbourg and Brussels.

Even though he is not subject to the European directive of 1995,[96] the Federal Commissioner follows attentively the work of the Article 29 Working Party and reflects their advice in his practice. Moreover, through bilateral agreements, Switzerland has brought its law on personal data protection closer to European law. Following an evaluation by the European Commission, the Swiss personal information protection system was recognized as adequate.

Within the Council of Europe Article 108 advisory committee, the Federal Commissioner is a full-fledged participant in the development of new measures for personal data protection. He is also called by the European Council to take part in training programs for states that wish to join the Strasbourg organization.

Finally, since its inception, the Swiss monitoring body has fully participated in international and European conferences of data protection and privacy commissioners.

[95] Press release of May 4, 2007, on the Federal Commissioner's Web site: www.edoeb.admin.ch
[96] European Parliament and Council directive 95/46/CE of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

TRENDS AND PROSPECTS

This document is intended to describe the current state of personal information or data protection in member states of the Organisation internationale de la Francophonie. The idea is to show the originality demonstrated by the independent authorities invested with the mandate of implementing and enforcing the legal systems devised for that purpose.

Written in descriptive form, this report draws for each of the eight governments a brief portrait of the legislative process leading to the creation of these "control authorities." It sums up the mandate and operational framework of these institutions and outlines a number of innovations or novelties designed to implement the principles and mandates enacted by the legislator.

This approach partly answers the wishes expressed by heads of state or government of the Organisation de la Francophonie at their last summit meetings in Bucharest and Ouagadougou. Twice, they clearly advocated the introduction of legal systems that ensure the protection of personal data in every state of the Francophonie. This outline of the makeup of control organizations is presented as a catalogue of the institutions devised in some states of the Francophonie: legislators and civil society representatives engaged in the search of a concrete solution to the problem of implementing this right to privacy can take instruction and inspiration from it.

The eight control authorities described in this document form the history of the development of the legal concept of personal data protection and its translation into real legal systems. They appeared at various moments from the mid-1970s until the beginning of the new millennium. To begin with, the emergence of data processing and the advent of the first super computers inspired the first laws in some states of the Francophonie in Europe and North America, namely in France, Quebec and Canada.

In some cases, events, indeed domestic crises, have led to this process. One can think of the discovery of secret files in Switzerland or the development of giant data banks in Belgium. In both cases, the data processing factor was key.

The tackling of these issues by at least two international institutions—the Council of Europe and the OECD—has strongly contributed to the evolution of this file in the same countries. The demolition of the Berlin Wall also had a considerable indirect impact on several states that sought and obtained membership in the European Union. Derived from the Copenhagen criteria, the adoption of a legal system of personal data protection was imposed as a prerequisite on applicant states. Already engaged on this path under the influence of the first mediator appointed after the adoption of the new constitution, Romania was able to meet European demands before joining the Union on January 1, 2007.

On either side of the Atlantic, this legislative evolution took different routes regarding the universality of rights and obligations ensuing from it. In Europe, these provisions indiscriminately targeted all the actors, public and private, handling personal data. In North America, the legislator first subjected the entire public sector to the law before imposing the same obligations on private sector organizations.

In nearly every case, the enactment of legislation was accompanied by the creation of a control body vested with the power to enforce the rights thus guaranteed to citizens and the obligations ensuing from them. Various considerations can no doubt account for the difference of powers and mandates conferred on these "control authorities," to use the term that became current in the 1990s. It was the influence of the European Union directive of 1995[97] that made it imperative to give these new authorities or institutions a status of real independence, or at the very least true autonomy.

The control authorities set up by states of the Francophonie meet common objectives. The legislators designed bodies that surely bear the imprint of a particular institutional culture, but whose variety embraces for the most part the range of choices made in every state endowed with a personal data protection system. A good number of these bodies are attached, under various forms, to the country's parliament; this marks their distance with government and administrative organs and broadens their room for manoeuvre.

Control authorities within the Francophonie can give rise to the development of a basic typology.

The ombudsman or mediator model rests on the moral authority this institution is vested with ever since its inception a long time ago in Scandinavian countries. Rather than binding decisions, the incumbent issues "recommendations." Canada's Parliament and New Brunswick's Legislative Assembly have opted for this model, with some variants. In Ottawa, the Privacy Commissioner fully exercises her functions with respect to the two acts structuring the personal information protection system; a sectoral ombudsman, shall we say. In Fredericton, this mandate was added to that of the Ombudsman, who ensures citizens are respected throughout the administrative apparatus.

Other states have a collegial institution taking on similar responsibilities. The CNIL is obviously looked on as a leader, not only because of its length of service, but also because of its influence. These "colleges," whose number of members may vary from three—as is the case in Luxembourg—to fifteen—like the CNIL—are naturally structured according to a sharing of mandates that makes it possible, among others, to deal with the priorities set by the college itself or, in some cases, by the legislator.

These same powers may be imparted to a single incumbent who has, like colleges, an administrative organization. It was the choice made in both Switzerland and Romania.

Finally, the last element of this basic typology is the administrative tribunal, in the strict sense of the term. This status confers to the authority restrictive decision-making powers and can lead to the development of a form of jurisprudence. The Quebec National Assembly chose this model upon adopting its legislation.

This typology is merely intended to illustrate the variety of decisions made by the legislators of Francophonie states as to the basic features of the control authorities set up when they adopted

[97] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJL 281/31.

their personal information protection legislation. It sums up, with two exceptions, the complete range of choices made in this regard the world over. In some cases, what serves as a control body is incorporated into a department or an organization; one cannot imagine such a structure claiming any independence or autonomy. Finally, a few states have rejected the option of setting up a control body while adopting personal information protection legislation. The US Congress, for one, has decided to hand over to the tribunals the enforcement of these rights and principles.

These control authorities perform the functions and mandates entrusted to them by their empowering legislation. Here again, we can group these activities under many criteria. For the purpose of this paper, it is the nature of the subject or subjects of these interventions that was considered.

The control authorities were established to ensure the respect of the rights to privacy and personal data protection conferred on citizens by law. Some intervene preventively; such notably is the case of European organizations, which require prior data processing statements. In North America, the emphasis was laid on the resolution of problems or disputes arising from the failure to respect the principles and obligations prescribed by law and which directly affect citizens.

Beyond this schematic classification, every independent agency has devised and implemented mechanisms, or initiated activities both in a preventive and therapeutic spirit. This explains the proliferation of information campaigns and the publication of guides to inform citizens of their rights. Likewise, we see a lot of initiatives designed to help citizens who feel they have been wronged or unfairly treated.

The state, the administrative machinery and the entire public sector are also the subject of the control authorities' measures and initiatives. Within the European Union, governments refer to them any bill or regulation likely to have an impact on personal data protection: it is one of the requirements of the 1995 directive. This advisory role is shared, at various degrees, by all agencies of the Francophonie. These responsibilities are exercised in ways and styles inspired by the culture of each political system; hence the diversity in the forms of intervention. As an example, one can point out the feasibility studies—a variant on the well-known impact studies carried out in environment—ordered before the adoption or modification of legislation to minimize the invasion of the citizens' privacy.

We also note certain differences regarding the implementation of obligations and requirements of this new legal system within the political apparatus. Thus, in Quebec and Canada, the legislator has entrusted the design and implementation of measures, procedures and other obligations to one department while the control authority sees to the respect of these provisions and their conformity with the principles of the law. Such a distinction is not seen in Europe.

The private sector is also the subject of control authorities' initiatives. The authorities provide advice and support to persons responsible for personal data in enterprises and organizations subjected to legislation. A few years ago in France, the CNIL set up a real network to maintain contact with these persons and encourage the dissemination of information. In the event of incidents or problems, control authorities start investigations and can conduct audits on site.

The similarity of missions and methods has led privacy commissioners to form an association to share their experiences and problems and devise forms of co-operation across borders. This dialogue probably developed very early and intensely in Europe. From the very start of the work that led to the adoption of the Council of Europe cross-border transfer of personal information convention, in Strasbourg, privacy commissioners began working together. They have been meeting regularly ever since and carry out major projects on a pan-European basis. With the adoption of the 1995 directive by the European Union, this co-operation has intensified within the so-called Article 29 Working Party where common positions are worked out and concrete projects are undertaken.

On a broader front, the preparation of the OECD "guidelines" also brought the national authorities together and, shortly after, the persons responsible for data protection. This movement was reactivated recently for an update of these important guidelines, which have influenced the legislators of many countries as they drafted their national legislation. On an international basis still, the data protection and privacy commissioners promptly formed into a conference, and Montréal this year is welcoming their 30th summit meeting.

Finally, the control authorities have become involved in bilateral co-operation and have lent a hand to countries that wished to equip themselves with a personal data protection system. This co-operation intensified during the preliminaries to the European Union expansion in 2004. It is practised on every continent and has become keener with the promotion of good governance rules, among others.

A brief look at the progression of control authorities within the Francophonie reveals trends that suggest avenues for the future.

A major innovation has been the recent bestowal to some authorities of a power of sanction whose primary objective is dissuasion, but whose effects are not negligible.[98]

Some agencies advocate a change of tasks and priorities. They are inclined to favour a more systemic role that would give precedence to measures designed to meet the challenge that NICT proliferation poses to privacy. Indeed, they call into question the way of fulfilling their mandates; hence the avowed intention of streamlining some of the procedures. Such is the case of Luxembourg and Switzerland in particular.

Protection of personal information and access to information, the two dimensions of citizens' rights have sometimes been combined, particularly in North America. Given concrete expression by the "Quebec model," the concept was revived in 2004 by the Swiss Parliament's decision to entrust the Federal Commissioner with the mandate to enforce the *Federal law on the principle of freedom of information in government.* The New Brunswick Ombudsman has just declared himself in favour of the cohabitation of these two systems—access to information and personal information protection.[99] In 2005, Canada's federal government gave up the idea of following

[98] See CNIL, *27e Rapport d'activités 2006,* Paris, La Documentation française, 2007, p.23.
[99] Bernard Richard, *Inside and Outside the Box: Proposals for an Information and Privacy Rights Code for New Brunswick* (submission to the New Brunswick Right to Information and Protection of Personal Information Review Task Force), Fredericton, July 5, 2007, 39 p.

this path on the basis of recommendations made by a former justice of the Supreme Court of Canada.

These trends are directly reflected on the international scene. They explain, among other things, the movement in favour of regional groupings of already existant national authorities as well as governments engaged in the process of adopting privacy legislation. It is the goal pursued for some time by member states of APEC, which brings together the most industrialized countries of Asia and the Pacific. This is the path on which countries of the Francophonie are embarking by grouping together.

It was probably with the London Declaration, in the fall of 2006, that the heads of control agencies best drew attention to the most obvious problems regarding privacy in every country. At the initiative of the CNIL President, participants at the London conference drew the lessons from two sets of factors. First, they brought to light the scale of the challenges posed by globalization and the dazzling development of NITCs. Then, in the same breath, they pointed out the indirect consequences for privacy of the events of September 11, 2001, with the multiplication of laws and measures designed to combat terrorism. This is the context in which emerges the proposed international convention that would ensure every human the respect owed to their privacy and their personal information.

CONTACT LIST

Belgium
Commission de protection de la vie privée

Willem Debeuckelaere, President
Rue Haute, 139
1000 Bruxelles
Phone: 32(0)2/213.85.40
Fax: 32(0)2/213.85.65

E-mail: commission@privacycommission.be
Web site: http://www.privacycommission.be

Canada
Office of the Privacy Commissioner

Jennifer Stoddart, Commissioner
112 Kent Street, Tower B (3rd floor)
Ottawa, Ontario K1A 1H3
Phone: (613) 995-8210
Fax: (613) 947 6850
Web site: http://www.priv.gc.ca

France
Commission nationale de l'informatique et des libertés

Alex Türk, President
8 rue Vivienne
CS 30223
75083 Paris
Cedex 02

Phone: 01 53 73 22 22
Fax: 01 53 73 22 00
E-mail: rh@cnil.fr

Web site: http://www.cnil.fr

Luxembourg
National Commission for Data Protection

Gérard Lommel, President
41, avenue de la gare (4ième étage)
L-1611 Luxembourg
Phone: 352 26 10 60 –1
Fax: 352 26 10 60 – 29
E-mail: info@cnpd.lu
Web site: www.cnpd.lu

New Brunswick
Office of the Ombudsman

Bernard Richard, Ombudsman
Sterling House
767 Brunswick Street
C.P. 6000
Fredericton
E3B 5H1
Phone: (506) 453-2789
Fax: (506) 453-5599
E-mail: nbombud@gnb.ca
Web site: http://www.gnb.ca/0073/index-f.asp

Quebec
Commission d'accès à l'information

Jacques Saint-Laurent, President
575, rue Saint-Amable
Bureau 1.10
Québec (Québec)
G1R 2G4
Phone: (418) 528-7741
Fax: (418) 529-3102
E-mail: Cai.Communications@cai.gouv.qc.ca
Web site: http://www.cai.gouv.qc.ca/

Romania
National Authority for the Control of Personal Data Processing

Georgeta Basarabescu, President
Str.Olari nr. 32
Sector 2
024057 Bucharest
Phone: 40-21 252 55 99
Fax: 40-21 252 57 57
E-mail: anspdcp@dataprotection.ro
Web site: http://www.dataprotection.ro

Switzerland
Federal Data Protection and Information Commissioner

Jean-Philippe Walter, Substitute Official
Feldeggweg 1
CH-3003 Bern
Phone: 41 (0)31 322 43 95
Fax: 41 (0)31 325 99 96
Web site: http://www.edoeb.admin.ch

SHORT BIBLIOGRAPHY

INTERNATIONAL DOCUMENTATION

- EC, *Directive 2002/58/EC of European Parliament and Council of 12 July 2002 regarding the processing of data of a personal character and the protection of privacy in the electronic communication sector***, [2002] J.O.L. 201/37.**
- EC, *Directive 95/46/EC of European Parliament and Council of 24 October 1995 concerning the protection of individuals with regard to the processing of data of a personal character and the free movement of such data*, [1995] J.O.L. 281/31.
- Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, Strasbourg, 28.I.1981.
- OECD, *OECD Guidelines on the protection of privacy and the cross-border flow of data of a personal character*, 23 September 1980.

GENERAL REFERENCES

- Comeau, Paul-André and Maurice Couture. "Accès à l'information et protection des renseignements personnels ," *Canadian Public Administration / Administration publique du Canada,* vol.46, no.3 (fall / automne), p. 364-389, 2003.
- De Terwangne, Cécile, Yves Poullet and Paul Turner. *Vie privée : nouveaux risques et enjeux / Privacy: New Risks and Opportunities*, Brussels, Éditions Stroy-Scientia, 1997.
- Benyekhlef, Karim. *La protection de la vie privée dans les échanges internationaux d'informations*, Montreal : Éditions Thémis, 1992.
- Oble-Laffaire, Marie-Laure. *Protection des données à caractère personnel*, Paris : Éditions d'Organisation, 2005.
- Flaherty, David H. *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*, Chapel Hill, University of North Carolina Press, 1989.
- Perrin, Stephanie; Black, Heather, H; Flaherty, David H. and Rankin, T. Murray. *The Personal Information Protection and Electronic Documents Act: An Annotated Guide*, Toronto, Irwin Law, 2001.

USEFUL WEB SITES

- Art.29 Data Protection Working Party
  http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm

- Electronic Privacy Information Center (EPIC)
  http://www.epic.org/

- OECD Privacy Policy Statement Generator
  http://www.oecd.org/document/42/0,3343,en_2649_34255_28863271_1_1_1_1,00.html

- Privacy International
  http://www.privacyinternational.org