29E CONFÉRENCE INTERNATIONALE DES COMMISSAIRES
À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE

LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE

TERRA INCOGNITA

PRIVACY HORIZONS

29TH INTERNATIONAL CONFERENCE OF
DATA PROTECTION AND PRIVACY COMMISSIONERS

Atelier
Tueur de dragon
La vérification

Workshop
Dragon Slayer
Audit

26 septembre/Septembre 26
13h30 - 16h

Série Terra Incognita, cahier de travail # 6 / Terra Incognita, workbook series # 6

Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada

Table des matières / Table of contents

Biographies — Conférenciers

M. Artemi Rallo Lombarte, Ph. D. – Président 2
Mme. Yim Chan 2
M. Nicholas Cheung 3
M. Chris Turner 4
M. Joel Winston 4

En route vers les vérifications internationales en matière de protection des renseignements personnels (Privacy Laws & Business)

Introduction 6

Terminologie 7

Quelques définitions utiles 8

Pouvoirs de vérification et d'enquête relatifs à la protection de la vie privée : une comparaison entre juridictions choisies . . . 9

Y a-t-il un avenir pour la coopération transfrontalière en Europe et ailleurs dans le monde ? 16

Utilisation des vérifications en tant qu'outil de conformité 19

Conclusion 22

Suggestions aux fins de discussion : un modèle de vérification pour les organismes responsables de la protection des données 23

Annexe : Rapports des pays

1. France – Commission nationale de l'informatique et des libertés (CNIL) . . . 25

2. Royaume-Uni – Office of the Information Commissioner (ICO) (Bureau du commissaire à l'information) 29

3. Espagne – Agencia española de protección de datos (Agence espagnole de protection des données) 34

Bibliographie 45

Biographies — Speakers

Dr. Artemi Rallo Lombarte – Chair 2
Ms. Yim Chan 2
Mr. Nicholas Cheung 3
Mr. Chris Turner 4
Mr. Joel Winston 4

En Route to International Privacy Audits (Privacy Laws & Business)

Introduction 6

Terminology 7

Sample Definitions of "Compliance Audit" 7

Comparison of Privacy Auditing/ Investigation Powers in Selected Jurisdictions 8

Is Threre a Future in Europe and Beyond for Cross-Border Co-operation 13

Use of Auditing as a Compliance Tool . . . 15

Conclusion 18

Suggestions for discussion: A model for DPA audits 19

Appendix: Country Reports

1. France – CNIL 20

2. UK – Office of the Information Commissioner (ICO) 24

3. Spain – Data Protection Authority . . . 28

Bibliography 37

Biographies

Président : M. Artemi Rallo Lombarte, Ph.D.

Artemi Rallo Lombarte est directeur de l'Organisme de protection des données de l'Espagne. Il a mené des recherches dans divers centres internationaux comme l'Institut international des droits de l'Homme à Strasbourg, l'Université La Sapienza à Rome et le Centre de recherche en Droit constitutionnel de l'Université Paris 1 – Panthéon-Sorbonne. Il est auteur d'un grand nombre de monographies, de livres et d'articles scientifiques publiés dans plusieurs magazines spécialisés, et a participé à des recherches et projets à l'échelle nationale et internationale sur l'administration publique, la protection des droits fondamentaux dans le cadre de l'intégration européenne et la décentralisation politique dans les États membres de l'Union européenne. De plus, M. Lombarte a collaboré à des programmes d'appui institutionnel européens en Amérique latine qui visaient à promouvoir la décentralisation politique, et à renforcer les institutions parlementaires et le pouvoir exécutif et judiciaire. Il est titulaire d'un diplôme en droit avec très grande distinction (1988) et d'un doctorat en droit de l'Université de Valence (1990). M. Lombarte est professeur en droit constitutionnel à l'Université Jaume I de Castellón, où il a également été chef du département de droit constitutionnel (1993-1998).

Conférenciers

M^me^ Yim Chan

Yim Chan, CIPP/C, exerce les fonctions de directrice exécutive du service mondial de protection des renseignements personnels d'IBM Corporation ainsi que de chef du service de protection des renseignements personnels chez IBM Canada. Ses responsabilités au niveau mondial comprennent l'élaboration et la mise en œuvre de programmes pour le système mondial de gestion de la protection des renseignements personnels, et l'intégration de la protection des renseignements personnels dans les processus commerciaux concernés. En tant que chef du service de protection des renseignements personnels chez IBM Canada, M^me^ Chan est chargée de l'orientation des politiques et des pratiques de gestion de l'information à l'échelle de

Biographies

Chair : Dr. Artemi Rallo Lombarte

Artemi Rallo Lombarte is Director of the Spanish Data Protection Agency. He has conducted research at international centres such as the International Human Rights Institute in Strasbourg, La Sapienza University (Rome) and the Centre de Recherche de Droit Constitutionnel at the Paris I-Pantheòn-Sorbonne University. He is the author of numerous monographs, books and scientific articles in specialised magazines and has participated in national and international research and projects on public administration, protection of fundamental rights in European integration, and political decentralisation in EU Member States. Mr. Lombarte has worked with European institutional support programmes in Latin America, aimed at promoting political decentralisation and strengthening parliamentary institutions, executive and judicial power. He graduated in Law with Extraordinary Prize Honours (1988) and Doctor in Law at the University of Valencia (1990). He is Professor of Constitutional Law at the Jaume I University of Castellón, where he was also Head of the Constitutional Law Department (1993-1998).

Speakers

Ms. Yim Chan

Ms. Yim Chan, CIPP/C, is the Global Privacy Executive, IBM Corporation and the Chief Privacy Officer, IBM Canada. Chan's responsibilities include developing and implementing programs at the enterprise level for IBM's global privacy management system and embedding privacy into relevant business processes. In her capacity as the CPO for IBM Canada, Yim Chan guides information handling policies and practices across IBM Canada. During her 28 years with IBM, Yim Chan has held several positions in software compiler development, industry solutions, and was formerly the CIO for IBM Canada. Yim Chan holds two patents for a Business Application Dialogues Architecture and Toolset in the privacy assessment environment and has obtained CIPP/C certifica-

l'organisation. Au cours de ses 28 années de service à IBM, M^me^ Chan a occupé différents postes dans les domaines du développement de compilateurs de logiciels et des solutions sectorielles. Elle a également déjà été chef du service de l'information à IBM Canada. M^me^ Chan est titulaire de deux brevets pour une architecture de dialogue d'applications d'affaires et un ensemble d'outils dans l'environnement de l'évaluation de la protection des renseignements personnels. Elle détient une certification CIPP/C. Yim Chan est membre des conseils CPO canadien et américain et siège au conseil consultatif de l'International Association of Privacy Professionals (IAPP), qui a mis sur pied le programme canadien de certification destiné aux professionnels de la protection des renseignements personnels (CIPP/C). Elle est souvent invitée comme conférencière à des événements sur la protection des renseignements personnels et est sollicitée pour des entrevues sur cette question. M^me^ Chan est titulaire d'un baccalauréat en mathématiques et en informatique de l'Université de Waterloo, et d'un certificat de maîtrise en gestion de projet de l'Université George Washington. Elle a participé au programme de mentorat Women in Technology (WIT) dans la région du Grand Toronto.

M. Nicholas Cheung

Nicholas Cheung est directeur de projets à l'Institut canadien des comptables agréés (ICCA), où il est responsable de l'élaboration et de la mise en œuvre de projets liés aux services de certification. Actuellement, il dirige le secteur des services de protection des renseignements personnels et son travail consiste principalement à concevoir et à faire connaître de nouveaux services et ressources en la matière offerts par les comptables agréés. Parmi ces ressources, on trouve les Principes généralement reconnus en matière de protection des renseignements personnels, un cadre mondial de référence pour la protection des renseignements personnels qui a été élaboré par l'ICCA et l'American Institute of Certified Public Accountants, afin de créer une norme nord-américaine qui tient compte des exigences internationales. Nicholas Cheung est comptable agréé et Certified Information Privacy Professional/Canada, le programme canadien de certification destiné aux professionnels de la protection des renseignements personnels (CIPP/C).

tion. Ms. Chan is a member of the Canadian and U.S. CPO Councils and is on the Advisory Board of the International Association of Privacy Professionals' (IAPP) which developed the Canadian certification program for privacy professionals (CIPP/C). She is a regular speaker at privacy-related conferences and is sought after for privacy-related interviews. Yim Chan graduated from the University of Waterloo with a Bachelor of Mathematics/Computer Science degree and earned a Master's Certificate in Project Management from George Washington University. She has participated in the Women in Technology mentoring program in the Greater Toronto Area.

Mr. Nicholas Cheung

Nicholas Cheung is a Principal at the Canadian Institute of Chartered Accountants (CICA) where he is responsible for the development and implementation of projects related to assurance services. He currently leads the Privacy Services area where he is focused on developing and raising the awareness of new privacy resources and services offered by Chartered Accountants. These resources include Generally Accepted Privacy Principles (GAPP), a global privacy framework developed by the CICA and the American Institute of Certified Public Accountants to create a common North American privacy standard that takes into consideration international requirements. He is a Chartered Accountant and holds a Certified Information Privacy Professional/Canada designation.

M. Chris Turner

Chris Turner se joint au Information Commissioner's Office (Commissariat à l'information) vers la fin de 2002 et s'occupe d'abord de la gestion des activités d'observation, dans le domaine de la réglementation et des tribunaux. Après avoir accepté le rôle de développer la capacité de vérification du Commissariat, il est nommé chef de la vérification et des recours au sein de la division des mesures réglementaires en 2005. Avant d'arriver au Commissariat, Chris travaille pendant plus de 30 ans dans le domaine des technologies de l'information. Il se charge surtout de la gestion de projets et de l'analyse de systèmes dans un groupe varié d'organisations chevauchant plusieurs secteurs, dont les loisirs, les finances et la fabrication.

M. Joel Winston

Joel Winston est directeur adjoint de la Division des renseignements personnels et de la protection de l'identité au Bureau de la protection du consommateur de la Commission fédérale du commerce. Cette Division se charge notamment de diverses questions liées à la qualité des données, à la protection des renseignements personnels des consommateurs, au vol d'identité et aux rapports de solvabilité. M. Winston est membre du Groupe de travail sur le vol d'identité, qui relève du gouvernement fédéral, et qui a été créé par le président Bush en mars 2006. Avant d'occuper ce poste, il a été directeur adjoint de la Division des pratiques financières à la Commission fédérale du commerce, poste qu'il a occupé après avoir été directeur adjoint de la Division des pratiques publicitaires de la Commission. M. Winston donne souvent des conférences et des conseils, dans les milieux d'affaires et juridiques, qui portent sur diverses questions touchant la protection des consommateurs. C'est à l'Université du Michigan qu'il a obtenu ses diplômes de premier cycle et de droit.

Mr. Chris Turner

Chris Turner joined the Information Commissioners Office in late 2002 and worked initially in compliance management in the area of 'policing and judiciary'. After taking on a role for developing the Office's audit capability he was appointed Head of Audit and Remedies within the Regulatory Action Division in 2005. Prior to his move to the ICO Mr. Turner spent over 30 years working in IT, primarily in project management and systems analysis, within a diverse range of organisations across sectors including leisure, finance and manufacturing.

Mr. Joel Winston

Joel Winston is Associate Director of the Division of Privacy and Identity Protection of the Federal Trade Commission's Bureau of Consumer Protection. That Division has responsibility over consumer privacy and data security issues, identity theft, and credit reporting matters, among other things. Mr. Winston is currently serving on the federal government's Identity Theft Task Force, which was created by President Bush in March 2006. Prior to his current position, Mr. Winston was Associate Director of the FTC's Division of Financial Practices and, previous to that, Assistant Director in the FTC's Division of Advertising Practices. Mr. Winston is a frequent speaker and provides guidance and advice to the business and legal communities on consumer protection issues. He received his undergraduate and law degrees from the University of Michigan.

29E CONFÉRENCE INTERNATIONALE DES COMMISSAIRES
À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE

LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE

TERRA INCOGNITA

PRIVACY HORIZONS

29TH INTERNATIONAL CONFERENCE OF
DATA PROTECTION AND PRIVACY COMMISSIONERS

En route vers les vérifications internationales en matière de protection des renseignements personnels

En Route to International Privacy Audits

Par / by

Privacy Laws & Business
Stewart Dresner, administrateur général / Chief Executive
Valerie Taylor, conseillère / Consultant

Juin 2007 / June 2007

Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada

Introduction

La présente étude a été réalisée à la demande du Commissariat à la protection de la vie privée du Canada en vue de la 29e Conférence internationale des commissaires à la protection des données et de la vie privée, qui se tiendra à Montréal (Canada) du 25 au 28 septembre 2007.

Dans bon nombre de pays, les organismes responsables de la protection des données ne font pas de distinction entre une vérification de la conformité et une inspection sur place découlant d'une plainte susceptible d'entraîner une sanction pénale. Les pouvoirs légaux conférés à ces organismes pour la réalisation de vérifications varient d'un pays à l'autre – par exemple, en ce qui a trait à la possibilité de procéder à une vérification avec ou sans le consentement de l'organisation. Aussi ce rapport vise-t-il à dégager des traits communs aux pratiques de vérification en matière de protection de la vie privée dans différents pays.

La distinction entre une vérification et une inspection demeure subtile. Il n'existe pas de définitions et de critères communs pour différencier les deux concepts. Outre les nuances linguistiques, il faut tenir compte des facteurs suivants :

- les concepts juridiques;
- les pouvoirs conférés aux organismes responsables de la protection des données;
- les ressources allouées aux vérifications;
- les attitudes adoptées à l'égard des exercices de vérification.

Le récent document publié par le Groupe de travail de l'OCDE à ce sujet ainsi que l'*Étude sur la vérification* réalisée par la commissaire à la protection de la vie privée du Canada donnent de plus amples détails sur le traitement des vérifications en vertu de différentes lois nationales, en plus de commenter, dans une certaine mesure, les approches préconisées. Cependant, leur lecture ne procure pas d'information sur la façon dont procèdent les organismes nationaux de protection des données pour effectuer des vérifications régulières.

Les auteurs du présent rapport tentent de dépasser les dispositions légales pour étudier :

Introduction

This study was commissioned under a contract with the Office of the Privacy Commissioner of Canada in support of the 29th International Conference of Data Protection and Privacy Commissioners – September 25th to 28th, 2007 in Montreal, Canada.

Many countries' Data Protection Authorities (DPAs) do not distinguish a compliance audit from an inspection visit resulting from a complaint which could lead to a penal sanction. DPAs' legal powers to conduct audits differ in different countries–for example, whether they may audit without the consent of the organisation. Therefore, the objective of this report is to find common themes in privacy auditing in different countries.

Drawing a neat distinction between an audit and an inspection remains elusive. There are no common definitions and criteria to distinguish the two concepts. Language differences are only one factor; others include different:

- legal concepts;
- DPA powers;
- resources for conducting audits; and
- attitudes towards conducting audits.

The recent OECD Working Party paper and the Canadian Privacy Commissioner's Study on Auditing go into detail about the ways in which audits are treated in different national laws, and give some impression about approach. However, the reader does not learn how the national DPAs conduct regular audits.

This report attempts to go beyond the legal provisions to study:

1. how the national DPAs in France, Spain and the United Kingdom conduct regular audits;
2. some examples from other countries;
3. experience of national DPAs co-operation when attempting an international audit;
4. the use of auditing as a compliance tool;
5. the anticipated benefits of audits both for DPAs, and data controllers and data processors.

In addition, the study authors offer a suggested model of good data protection audit practices (see pages 12-13) for discussion at the audit workshop at the Data Protection and Privacy Commission-

1. la façon dont les organismes chargés de la protection des données en France, en Espagne et au Royaume-Uni effectuent les vérifications régulières;
2. quelques exemples observés dans d'autres pays;
3. les efforts de coopération entre différents organismes nationaux participant à des vérifications d'envergure internationale;
4. le recours aux vérifications comme outils visant à assurer la conformité;
5. les avantages attendus des vérifications pour les organismes responsables de la protection des données ainsi que pour les préposés au contrôle et au traitement des données.

De plus, les auteurs proposent des pratiques exemplaires à suivre pour les vérifications relatives à la protection des données (voir pages 15-16). Ces propositions pourront faire l'objet de discussions lors de l'atelier sur les vérifications qui aura lieu en septembre dans le cadre de la 29e Conférence internationale des commissaires à la protection des données et de la vie privée.

Terminologie

L'évaluation des pouvoirs accordés dans diverses juridictions permet d'établir les distinctions terminologiques suivantes.

Vérification de la conformité
Il s'agit d'une évaluation proactive des méthodes et des procédures de traitement des données suivies à l'intérieur d'une organisation, qui vise à déterminer le niveau de conformité général de cette dernière aux lois sur la protection des données, et à cerner et à encourager les pratiques exemplaires. Les vérifications de la conformité peuvent se produire dans différentes circonstances :

1. *Vérifications imposées* : Les organismes responsables de la protection des données utilisent ces vérifications pour améliorer le niveau de conformité d'une organisation. Les vérifications peuvent être imposées en raison de mesures d'application ou de réglementation, à moins que les organisations concernées ne soient contraintes de les demander « volontairement »;
2. *Vérifications volontaires* : De telles vérifications sont effectuées à la demande d'organisations qui veulent déterminer ou améliorer leur niveau de conformité.

ers' 29th International Conference in Montreal in September 2007.

Terminology

An assessment of the powers in various jurisdictions suggests the following distinctions in terminology.

Compliance Audit
This is a proactive assessment by the DPA of the data processing activities, processes and procedures within an organisation to determine its general compliance with data protection legislation, and to establish and encourage good practice. Audits could be initiated in different circumstances:

1. "*Enforced" audit*: used by the DPA to improve an organisation's levels of compliance. It may be imposed on the organisation as part of enforcement or regulatory activity, or the organisation may be persuaded to "volunteer" for the audit.
2. *Voluntary audit*: carried out at the request of the organisation as a means of establishing or improving its own level of compliance.

Investigation/Inspection
This is an investigation into a specific area of data processing activity within an organisation where there is a suspected breach of the data protection legislation. It may lead to sanctions or other enforcement action being taken. An investigation could be initiated in one of two ways:

1. *Complaint-initiated*: caused by a complaint from an aggrieved individual who has been affected by the suspected breach.
2. *Self-initiated*: resulting from press enquiries or initiated by the DPA in areas of substantial public debate or concern.

Differences
Compliance audits are typically broad in scope, encompassing an entire organisation or function, whereas investigations or inspections are usually more focused.

Also, any enforcement action resulting from an investigation or inspection is usually open to challenge–not always the case in a compliance audit.

Sample Definitions of "Compliance Audit"

Office of the Canadian Privacy Commissioner
A formal and systematic examination of an organi-

Enquête ou inspection
Il s'agit d'une enquête sur des activités spécifiques de traitement des données au sein d'une organisation, lesquelles sont soupçonnées d'être non conformes aux lois sur la protection des données. Une telle enquête peut se solder par des sanctions ou d'autres mesures d'application. Elle peut être entreprise dans deux cas :

1. *Enquête amorcée suite à une plainte* : L'enquête résulte d'une plainte déposée par une personne lésée par la non-conformité présumée;
2. *Enquête émanant de l'organisme* : L'enquête résulte de l'initiative d'un organisme responsable de la protection des données ou d'une enquête journalistique sur des questions alimentant de grandes discussions ou suscitant des préoccupations publiques.

Différences
Généralement d'une vaste portée, les vérifications de la conformité peuvent toucher une organisation ou une fonction entière, alors que les enquêtes ou les inspections ciblent habituellement des questions précises.

Par ailleurs, toute mesure d'application résultant d'une enquête ou d'une inspection peut habituellement être contestée – ce qui n'est pas toujours possible dans le cas d'une vérification de la conformité.

Quelques définitions utiles

Vérification de la conformité [traduction] : Examen officiel et complet des pratiques de gestion des renseignements personnels, des politiques connexes, des systèmes et des ressources documentaires d'une organisation, afin de déterminer la mesure dans laquelle celle-ci se conforme aux lois et aux normes relatives à la protection de la vie privée, et en vue de la présentation de rapports officiels à ce sujet.

Commissariat à la protection de la vie privée du Canada

Audit : Mission d'examen et de vérification de la conformité [aux règles de droit, de gestion] d'une opération, d'une activité particulière ou de la situation générale d'une entreprise.

Petit Robert

Vérification de la conformité [traduction] : Examen complet et indépendant visant à déterminer si les activités liées au traitement des données à sation's personal information management practices and related policies, systems and holdings, to determine and report formally on the extent of compliance with applicable privacy legislation and standards.

Oxford English Dictionary
An audit is an official inspection [of an organisation's accounts], typically by an independent body.

UK Information Commissioner
A systematic and independent examination to determine whether activities involving the processing of personal data are carried out in accordance with an organisation's data protection policies and procedures, and whether this processing meets the requirements of the Data Protection Act 1998. The UK *Data Protection Act* describes it as an assessment of the following of good practice.

Comparison of Privacy Auditing/ Investigation Powers in Selected Jurisdictions

Status of Privacy Audits in Canada

Around two-thirds of the various privacy laws in Canada provide audit powers for the federal, provincial and territorial supervisory authorities. The remaining laws do not make any provision for privacy audits, without which the supervisory authorities have no legal authority to conduct audits.

Audits have only been carried out to any measurable extent by the federal Privacy Commissioner and Quebec's Access to Information Commission, and only the federal Commissioner appears to have an ongoing programme of formal compliance auditing. Audits have tended to focus on the public sector but are now starting to involve private sector organisations also.

There is legislative potential for Canadian supervisory authorities to carry out a much greater level of auditing, but this is not being taken up in practice. The likely reason for this seems to be a lack of resources.

However, there are significant variations between the audit powers available to the different supervisory authorities in Canada. This may make the sharing of knowledge and best practice more difficult and could discourage cross-boundary audits. It is perhaps not surprising, therefore, that most audits have been carried out by the federal super-

caractère personnel sont conformes aux politiques et aux procédures en matière de protection des renseignements personnels dont s'est dotée une organisation, et si ce traitement répond aux exigences de la *Data Protection Act* (loi sur la protection des données) de 1998. Cette loi britannique présente la vérification de la conformité comme une évaluation des efforts déployés pour appliquer des pratiques exemplaires.

UK Information Commissioner
(commissaire à l'information du R.-U.)

Pouvoirs de vérification et d'enquête relatifs à la protection de la vie privée : une comparaison entre juridictions choisies

Les vérifications relatives à la protection de la vie privée au Canada

Au Canada, près des deux tiers des diverses lois sur la protection de la vie privée confèrent des pouvoirs en matière de vérification aux organismes de supervision provinciaux, territoriaux et fédéral. Les autres lois ne contiennent aucune disposition sur les vérifications relatives à la protection de la vie privée. Or, sans de telles dispositions, les organismes de supervision n'ont pas l'autorisation légale de procéder à des vérifications.

Seuls le Commissariat à la protection de la vie privée du Canada et la Commission d'accès à l'information du Québec ont procédé à des vérifications de portée significative, et seul le premier semble avoir opté pour un programme continu de vérifications officielles de la conformité. Les vérifications sont surtout effectuées dans le secteur public, mais elles commencent depuis peu à toucher aussi des organisations du secteur privé.

Sur le plan juridique, les organismes de supervision canadiens pourraient élargir considérablement la portée de leurs activités de vérification, mais cette option n'est pas retenue dans les faits. Le manque de ressources semble l'explication la plus vraisemblable à cet égard.

Cependant, les pouvoirs de vérification accordés aux divers organismes de supervision canadiens varient beaucoup. Cette situation complique la mise en commun des connaissances et des pratiques exemplaires, en plus de décourager les

visory authority which has the clearest and most wide-ranging powers. These powers concern not only the legal authority to carry out audits, but also ancillary powers such as the power to summon witnesses, compel evidence, enter premises and demand the production of documents and records.

Status of Privacy Audits in France

French privacy laws provide the DPA (the CNIL) with inspection powers which are considered to include the power to carry out audits using either the powers of entry or on invitation by an organisation.

Inspection teams usually consist of three people, a legal expert, an IT expert and a former police officer. The inspection programme is not published in advance, nor are the inspection results made public. The DPA issues a report to the organisation on conclusion of the inspection unless the audit identified no issues.

The CNIL has conducted a number of major inspections in the last few years, covering both the public and private sectors. Organisations or sectors are selected for inspection based on complaints received (from individuals or the press) or problems identified by the CNIL during the notification or prior authorisation processes. Therefore these inspections fall in the category of "self-initiated inspections" in the enforcement arena. Compliance audits have not been carried out.

There is legislative potential for the CNIL to conduct compliance audits. Its enforcement powers have been strengthened in the last few years and it is currently exploring the use of those enforcement powers. The CNIL does not have the resources to conduct more wide-ranging audits and so it is focusing on enforcement-related investigations where potential risks to individuals have been identified, such as criminal records information, health data and financial information. This approach may change in future as its enforcement powers mature and if they gain additional resources.

Status of Privacy Audits in the United Kingdom

The UK privacy law gives the Information Commissioner's Office (ICO) specific power to carry out audits which are defined as an "assessment" of processing to determine the following of good

tentatives de vérifications transfrontalières. Dans ce contexte, il n'est peut-être pas étonnant que la plupart des vérifications soient effectuées par l'organisme de supervision fédéral doté des pouvoirs les mieux définis et les plus vastes. Ces pouvoirs ne consistent pas seulement en l'autorisation légale de procéder à des vérifications, mais aussi en des pouvoirs accessoires, comme ceux d'assigner des témoins, de contraindre au dépôt de preuves, de visiter les lieux et d'exiger la production de documents et de dossiers.

Les vérifications relatives à la protection de la vie privée en France

Les lois françaises sur la protection de la vie privée confèrent à la Commission nationale de l'informatique et des libertés (CNIL) des pouvoirs qui, considère-t-on, comprennent celui de procéder à des vérifications, sous perquisition ou à la demande d'une organisation.

Les équipes d'inspection sont habituellement composées de trois personnes : un conseiller juridique, un expert en TI et un ancien agent de police. Le programme d'inspection n'est pas publié à l'avance, et les résultats d'inspection ne sont pas communiqués publiquement. La CNIL remet un rapport à l'organisation concernée au terme de l'inspection, sauf si la vérification ne conclut à l'existence d'aucun problème.

Ces dernières années, la CNIL a effectué un certain nombre d'inspections majeures dans les secteurs public et privé. Les organisations et les secteurs qui doivent faire l'objet d'une inspection sont sélectionnés en fonction des plaintes reçues (de la part de particuliers ou de la presse) ou des problèmes cernés par la CNIL lors de la notification ou avant les processus d'autorisation. C'est la raison pour laquelle ces inspections appartiennent à la catégorie des « inspections menées sur l'initiative de l'organisme » dans le domaine de l'application des lois. Aucune vérification de la conformité n'a été réalisée.

Sur le plan juridique, la CNIL pourrait procéder à des vérifications de la conformité. Elle est d'ailleurs en train de sonder les possibilités offertes par les pouvoirs de contrainte qui ont été renforcés ces dernières années. Toutefois, elle ne dispose pas des ressources nécessaires pour effectuer des vérifications plus vastes, d'où son choix de concentrer ses efforts sur les enquêtes

practice. This power is in addition to enforcement powers to conduct self-initiated or complaint-initiated investigations.

The audit team usually consists of two or three trained data protection specialists, one of whom may have an IT background, although the ICO is considering bringing in specialists where more specific technical knowledge is required. Reports are provided to the organisation following the audit but are not made public. Typically audits reveal problems with data subjects' access to personal data, data retention, and internal governance issues.

The IOC has conducted a significant number of audits over the last few years and has a mature audit programme in place. Audits may be initiated by a complaint or other enforcement action, and used as a way of improving compliance, or they may be requested by the organisation. Some audits may be carried out in sectors that are generating substantial public debate or where there is a great deal of change underway, such as in the health sector.

All audits are carried out with the consent of the organisation and all information is provided voluntarily. Legal warrants to gain entry to premises are usually obtained only where there are serious breaches or the legislation or criminal investigations. The ICO has published a comprehensive audit methodology (see bibliography p.26).

The ICO has found that auditing provides an opportunity to observe organisations and the way in which they handle personal data in practice, and helps improve relationships. This helps to educate ICO staff on the practical difficulties of day to day compliance. It also provides useful insights which can feed into the ICO's guidance. The ICO's audit team is expanding and they will continue to promote auditing as a tool to raise awareness of data protection and to encourage compliance and good practice.

Status of Privacy Audits in Spain

Spain's rules on inspections and audit are specified in the law and a Royal Decree. This has the merit of legal certainty and Spain's Data Protection Agency has more staff to conduct audits than most other European Union countries. However, as the law requires the Agency to assess every

liées à l'application dans les cas où elle a découvert des risques potentiels pour les personnes, comme des renseignements sur le casier judiciaire, des données sur la santé et de l'information financière. Cette approche pourrait changer à mesure que les pouvoirs de contrainte de la CNIL se raffineront et si celle-ci obtenait des ressources supplémentaires.

Les vérifications relatives à la protection de la vie privée au Royaume-Uni

La loi sur la protection de la vie privée en vigueur au Royaume-Uni donne à l'Information Commissioner's Office (Bureau du commissaire à l'information) (ICO) le pouvoir particulier de procéder à des vérifications, plus précisément à une « évaluation » des processus de traitement afin de déterminer si une organisation recourt aux pratiques exemplaires. Ce pouvoir s'ajoute aux pouvoirs de contrainte lui permettant d'effectuer des enquêtes de sa propre initiative ou suite au dépôt d'une plainte.

L'équipe de vérification est habituellement composée de deux ou trois experts spécialisés dans la protection des données, dont l'un pourrait avoir de l'expérience dans le domaine de la TI – bien que l'ICO envisage de faire appel à des spécialistes lorsque des connaissances techniques plus pointues sont requises. L'organisation concernée reçoit un rapport après la vérification, mais le contenu de celui-ci n'est pas rendu public. En général, les vérifications font état de problèmes liés à l'accès des personnes à leurs renseignements personnels, à la conservation des données et à la gestion interne.

Fort d'un programme de vérification bien rodé, l'ICO a procédé à un nombre important de vérifications au cours des dernières années. Les vérifications peuvent être amorcées par une plainte ou une autre mesure d'application, à moins d'être effectuées à la demande d'une organisation désireuse d'améliorer sa conformité. Certaines vérifications peuvent être menées dans des secteurs alimentant d'importants débats publics ou touchés par un nombre considérable de changements, comme le secteur de la santé.

Toutes les vérifications sont réalisées avec le consentement de l'organisation, et les renseignements sont fournis sur une base volontaire. L'autorisation légale d'entrer dans les

complaint on the grounds that the Agency must serve the citizen, it prevents the Director from allocating resources to audits on the basis of priorities and the merits of a case. New regulations expected to be adopted by the end of 2007 should enable the Director to become more flexible in his approach to complaints.

There are two types of audits: reactive audits resulting from a complaint, which may lead to a penal sanction; and preventive audits which involve the investigation of a specific sector, which are more likely to lead to recommendations on good practice.

Armed with the Director's authorisation document, the inspectors have the powers they need to enter premises and obtain documents. There is an incentive for organisations to co-operate in the process because obstructing inspectors is a separate infraction of the law which can lead to an additional fine.

Most audits are carried out as a result of individuals' complaints to the Agency. The telecommunications and financial services sectors are the two sectors which receive the most inspections.

International Cooperation

Spain led the European Union's project to audit the medical insurance sector in 2006 and 2007. The audit was conducted by a written questionnaire as the powers of the national authorities differ considerably. The report was approved by the Article 29 Data Protection Working Party on June 21st 2007. The announcement stated: "Although for the most part the companies are aware of data protection rules, nevertheless there are shortcomings in some areas. The Working Party, therefore, will continue its cooperation with the health insurance industry by issuing recommendations to promote privacy enhancing policies, and to raise awareness among customers."

Spain's Agency has concluded that:

1. international co-operation on audits, and much else, is much easier if only a few countries are involved (with similar enforcement tools), and
2. a shortage of people and financial resources means that an international audit is most usefully conducted on an issue which is a high priority for all the national partners involved in the project.

locaux d'une organisation n'est habituellement accordée que lors de cas sérieux de non-conformité ou dans le cadre d'enquêtes criminelles. L'ICO a publié des lignes directrices exhaustives en matière de vérification (voir la bibliographie, p. 26).

L'ICO a découvert que les exercices de vérification lui permettaient d'observer les organisations et leur façon de traiter les données à caractère personnel dans la pratique, en plus de contribuer à l'amélioration des relations avec elles. Sous cet angle, les vérifications aident le personnel de l'ICO à mieux comprendre les difficultés éprouvées au quotidien, inhérentes aux activités visant la conformité. De plus, elles fournissent des indications utiles qui peuvent enrichir les recommandations de l'ICO. Actuellement en période de croissance, l'équipe de vérification de l'ICO continuera de promouvoir la vérification comme outil de sensibilisation à la protection des données et afin d'encourager les organisations à se conformer aux règles et à adopter des pratiques exemplaires.

Les vérifications relatives à la protection de la vie privée en Espagne

En Espagne, les règles relatives aux inspections et aux vérifications sont précisées dans les lois et un décret royal. La Agencia Española de Protección de Datos (Agence espagnole de protection des données), dont les employés affectés aux vérifications sont plus nombreux que dans la plupart des autres pays de l'Union européenne, profite de cette approche en raison de la certitude juridique qu'elle apporte. Cependant, comme la loi exige de cet organisme qu'il évalue chaque plainte en tenant compte de sa mission, qui est de servir les citoyens, sa direction ne peut allouer des ressources aux vérifications en fonction des priorités et du bien-fondé de chaque cas. Les nouveaux règlements dont on prévoit l'adoption d'ici la fin de 2007 devraient permettre à la direction de l'Agence espagnole de protection des données de jouir d'une plus grande marge de manœuvre dans le traitement des plaintes.

Il existe deux types de vérifications : les vérifications qui découlent d'une plainte et qui risquent d'entraîner une sanction pénale et les vérifications préventives, qui reposent sur une enquête dans un secteur particulier et qui sont susceptibles de se solder par des

Audit methodology

Audits are conducted by a team of two IT experts with training in data protection law. There is no distinction between a legal and a data security audit. The inspectors give the evidence to the legal team at the Agency which recommends action to the Director.

Typical findings are poor data security, staff misuse of data, and no or few logs–so no audit trails.

Conclusion

The agency considers inspections and audits to be valuable because they are a "way of ensuring compliance without resulting in fines". The resulting recommendations help to raise awareness in all sectors of the benefits of good data protection practice.

The Agency's most important objective for the future is the ability to choose its own auditing priorities and methods rather than being required by law to investigate every complaint, however trivial. Ideally, the Director wants a dialogue rather than an adversarial relationship, reserving the latter approach for when the facts of the case dictate rather than rigid legal prescription.

Status of Privacy Audits in Other Jurisdictions

Of 14 countries surveyed in the Canadian Privacy Commissioner's Study on Auditing (December 2006), only two have neither express nor implied powers to conduct privacy compliance audits.

In most countries, the supervisory authority's audit powers are inferred from the power to conduct self-initiated investigations or reviews. As the study found, the scope of audit and ancillary powers available to the supervisory authorities differs widely from one country to another. The focus of most legislation (as can be seen from the OECD Report mentioned below) is on complaint handling and associated breaches of privacy legislation, and regulatory supervision. It is likely that resource issues also play a part in the apparently low priority for compliance auditing.

Australia

Very few countries seem to have published audit manuals or procedures, or to have established formal programmes of compliance auditing. The Office of the Privacy Commissioner (OPC) in Aus-

recommandations au sujet des pratiques exemplaires.

Munis du document d'autorisation de la direction, les inspecteurs détiennent les pouvoirs dont ils ont besoin pour visiter les lieux et obtenir des documents. Les organisations sont cependant incitées à coopérer dans la mesure où l'entrave au travail des inspecteurs constitue une infraction en soi qui peut justifier l'imposition d'une amende supplémentaire.

La plupart des vérifications ont lieu à la suite de plaintes déposées par des particuliers auprès de l'Agence espagnole de protection des données. Les secteurs des télécommunications et des services financiers sont ceux où les inspections sont les plus nombreuses.

Coopération internationale

L'Espagne a piloté le projet visant la tenue d'une vaste vérification dans le secteur de l'assurance-maladie, dans les pays de l'Union européenne, en 2006 et en 2007. Comme les pouvoirs conférés aux organismes nationaux diffèrent considérablement d'un pays à l'autre, cette vérification a pris la forme d'un questionnaire écrit. Le rapport a été approuvé par le Groupe de travail de l'article 29 sur la protection des données, le 21 juin 2007. Il a été rappelé, lors de la déclaration, que, [traduction] « bien que la plupart des entreprises connaissent les règles sur la protection des données, on continue d'observer des faiblesses dans certains secteurs. Aussi le Groupe de travail maintiendra-t-il sa coopération avec l'industrie de l'assurance-maladie en lui faisant part de recommandations pour encourager les politiques visant à améliorer la protection de la vie privée, et sensibiliser les clients à ces enjeux. »

L'Agence espagnole de protection des données est arrivée à deux conclusions :

1. Les efforts de coopération internationale dans le cadre de vérifications et de nombreux autres exercices sont beaucoup plus fructueux si seuls quelques pays y participent (et si leurs outils d'application sont similaires);
2. Le manque de ressources humaines et financières fait en sorte qu'une vérification internationale s'avérera plus utile si elle porte sur une question prioritaire pour tous les partenaires nationaux d'un projet.

tralia is one of the few, having published a self-audit manual for three industry sectors which raise particular concerns in Australia. The OPC also conducts regular audits of government agencies and has published the audit reports on its website since 2002. During 2005-6, it conducted audits only where it received separate funding to do so. While auditing may have measurable benefits both for the OPC and the audited organisation, the OPC has made a policy decision to focus its resources on complaint handling.

The Netherlands
The Dutch Data Protection Authority has published a privacy audit framework to assist those wishing to carry out privacy compliance audits, although the DPA itself focuses on investigations rather than audits (see bibliography page 26).

New Zealand
New Zealand uses self-auditing as part of the authorisation process for information matching and credit reporting activities, to ensure that such processing is carried out in compliance with the privacy legislation. Audits are submitted to the Privacy Commissioner and it is considered that the process will enhance regulatory oversight in these areas.

European Data Protection Supervisor
The European Data Protection Supervisor (EDPS) is the supervisory authority devoted to protecting personal data and privacy and promoting good practice in EU institutions and bodies. EDPS is conducting an audit of Eurodac, the database of fingerprints of illegal immigrants and applicants for asylum found in the EU. The in-depth security audit is due to report by the middle of 2007. The development of audit expertise within EDPS could lead to further audit projects in the future.

Is There a Future in Europe and Beyond for Cross-Border Co-operation?

Article 29 Working Party Declaration on Enforcement [25 November 2004]
The Article 29 Working Party looked (among other things) at the value of investigation and audit programmes as a means for encouraging compliance. Such programmes could be aimed at giving organisations a more accurate picture of how data protection rules should be implemented in a particular sector. They could also help DPAs create appropriate policies and guidance by emphasising how data controllers should comply.

Méthode de vérification

Les vérifications sont confiées à une équipe de deux experts en TI spécialisés dans les lois relatives à la protection des données. Aucune distinction n'est établie entre une vérification de nature juridique et une vérification relative à la sécurité des données. Les inspecteurs remettent la preuve à l'équipe juridique de l'Agence espagnole de protection des données, qui recommande des mesures à la direction.

Les conclusions les plus fréquentes ont trait à des lacunes en matière de sécurité des données, à une mauvaise utilisation des données par certains employés et à la rareté ou à l'absence de registres et, par le fait même, de traces de vérification.

Conclusion

L'Agence espagnole de protection des données considère les inspections et les vérifications comme des exercices très utiles du fait qu'elles permettent d'assurer la conformité sans entraîner d'amendes. Les recommandations qui en découlent aident à sensibiliser les intervenants de tous les secteurs aux avantages que procurent les pratiques exemplaires en matière de protection des données.

L'objectif le plus important auquel travaille maintenant l'Agence est de pouvoir fixer ses priorités et choisir ses méthodes de vérification au lieu d'être enjointe par les lois à enquêter sur toutes les plaintes, même celles d'une importance négligeable. La direction aspire à des relations centrées sur le dialogue plutôt que sur la confrontation, et ne réserve cette dernière approche qu'aux cas où des procédures judiciaires fermes sont requises en raison des faits et non des lois.

Les vérifications relatives à la protection de la vie privée dans d'autres juridictions

Des 14 pays étudiés dans l'*Étude sur la vérification* de la commissaire à la protection de la vie privée du Canada (décembre 2006), seulement deux ne prévoient pas de pouvoirs, explicites ou implicites, pour effectuer des vérifications de la conformité aux règles relatives à la protection de la vie privée.

Dans la plupart des pays, les pouvoirs de

Organisation for Economic Co-operation and Development Working Party on Information Security and Privacy report on cross-border enforcement of privacy laws [16 October 2006]
More recently, the OECD WPISP produced a report on cross-border enforcement of privacy laws. The report aimed to investigate the possibility of facilitating the co-ordination of cross-border privacy compliance and enforcement mechanisms.

Most supervisory authorities indicated in the report that they did not have–but would benefit from–appropriate powers to enable them to exchange information and carry out investigations jointly with, or at the request of, foreign authorities. Efforts to increase cross-border enforcement activity may therefore be hampered by the lack of powers available to supervisory authorities and inconsistent legal regimes, as well as a lack of resources and differing priorities within supervisory authorities.

While supervisory authorities generally did not report receiving a significant number of cross-border complaints, advances in technology and the globalisation of business suggest that the volume of cross-border data flows will continue to increase. The development of business and technological efficiencies brings with it increased privacy risks thus making it important to address the challenges of cross-border enforcement and co-operation.

European Commission report on the implementation of the European Data Protection Directive and follow-up work programme [7 March 2007]
One of the tasks identified by the European Commission is to reduce national divergences and improve harmonisation of data protection laws within Europe. The principle of Europe-wide synchronisation of national enforcement actions was agreed, and data protection authorities are encouraged to adapt their domestic practices to the common position.

However, as a practical matter, even where national laws set out to apply the same principles (e.g. the EU Data Protection Directive 95/46/EC or the OECD Guidelines), differences of interpretation and emphasis for cultural, historical and legal reasons may hinder co-operation between authorities or complicate the implementation of joint or concurrent audits.

European supervisory authorities have a duty un-

vérification des organismes de supervision découlent du pouvoir de procéder, de leur propre initiative, à des enquêtes ou des examens. Comme l'ont découvert les auteurs de l'étude, la portée des vérifications et l'éventail des pouvoirs accessoires accordés aux organismes de supervision varient grandement d'un pays à l'autre. La plupart des lois sont axées sur le traitement des plaintes et des infractions connexes aux lois sur la protection de la vie privée, ainsi que sur les activités de surveillance réglementaires (le rapport de l'OCDE dont nous faisons mention en témoigne). Il est probable que le manque de ressources contribue également à ce que les vérifications de la conformité soient, en toute apparence, de moindre priorité.

Australie
Rares sont les pays, semble-t-il, qui ont publié des manuels ou des méthodes de vérification, ou qui se sont officiellement dotés de programmes de vérification de la conformité. En Australie, l'Office of the Privacy Commissioner (Bureau du commissaire à la protection de la vie privée) (OPC) est l'un des seuls à avoir publié un manuel d'auto-vérification pour trois secteurs de l'industrie qui suscitent des inquiétudes. Il se distingue aussi par la réalisation de vérifications régulières dans les organismes gouvernementaux et, depuis 2002, par la publication des rapports de vérification sur son site Web. En 2005-2006, cet organisme a procédé à des vérifications uniquement dans les cas où il disposait de fonds distincts pour le faire. Bien que les vérifications apportent des avantages mesurables à la fois pour lui et pour l'organisation concernée, l'OPC a pris la décision stratégique de centrer ses ressources sur le traitement des plaintes.

Pays-Bas
Le College Bescherming Persoonsgegevens (organisme hollandais de protection des données) a publié un cadre de vérification en matière de protection de la vie privée pour guider ceux qui souhaitent procéder à des vérifications de la conformité aux règles relatives à la protection de la vie privée, bien que, pour sa part, cet organisme axe ses efforts sur les enquêtes plutôt que sur les vérifications (voir la bibliographie, p. 26).

Nouvelle-Zélande
En Nouvelle-Zélande, des autovérifications sont effectuées dans le cadre d'un processus d'autorisation visant le jumelage de

der the Data Protection Directive to co-operate with each other. However it is less common that a European supervisory authority would undertake proactive co-operation with an equivalent authority outside Europe because of fewer legal powers. However, there are examples of such cooperation. One is the formal Memorandum between Spain's Data Protection Agency and the United States Federal Trade Commission on cooperating in the fight against unsolicited e-mail communications, or "spam".

One possibility within Europe would be to seek assistance from the Article 29 Working Party for pan-European audit or enforcement initiatives. The Working Party has recently investigated the health insurance sector across all European Member States. The national data protection authorities sent out written questionnaires to gather information from health insurance companies within their jurisdiction–this was the only way to collect consistent information across all countries because of the varying powers of European DPAs.

Co-operation among Data Protection Authorities on cross-border audits may be more successful in practice if only two or three–rather than many–countries are involved.

Binding Corporate Rules
The Article 29 Working Party has produced various guidelines and reports on the use of Binding Corporate Rules as a means of ensuring adequate protection for international transfers of personal information within a group of companies. An organisation's Binding Corporate Rules must provide for the use of either internal auditors, external auditors or a combination of both. The organisation's audit plan must also allow for audit by data protection authorities. There is a possibility, therefore, that as Binding Corporate Rules become more popular in Europe, there will be an increasing demand for DPA audits as part of verifying compliance.

Use of Auditing as a Compliance Tool

In jurisdictions where audits are carried out, there are many perceived benefits.

Promoting Audits

Where auditing is already carried out:

There is little need to promote auditing where the

renseignements et l'établissement de rapports sur la solvabilité afin de s'assurer que ces activités sont menées conformément aux lois relatives à la protection de la vie privée. Les vérifications sont remises au Privacy Commissioner (commissaire à la protection de la vie privée). Ce processus permettrait d'améliorer la surveillance réglementaire dans ces secteurs.

Contrôleur européen de la protection des données
Le contrôleur européen de la protection des données (CEPD) est responsable de la protection des renseignements personnels et de la vie privée ainsi que de la promotion des pratiques exemplaires dans les institutions et les organismes de l'Union européenne (UE). Le CEPD procède actuellement à une vérification d'Eurodac, la base de données des empreintes digitales des immigrants illégaux et des demandeurs d'asile présents dans l'UE. Un rapport de cette vérification approfondie est attendu pour le milieu de l'année 2007. Le perfectionnement des connaissances en matière de vérification au sein de cet organisme pourrait contribuer à la mise en œuvre d'un plus grand nombre de projets de vérification à l'avenir.

Y a-t-il un avenir pour la coopération transfrontalière en Europe et ailleurs dans le monde?

Groupe de travail de l'article 29 – Déclaration sur l'application [25 novembre 2004]
Le Groupe de travail de l'article 29 s'est notamment penché sur l'utilité des programmes d'enquête et de vérification comme moyens de promotion de la conformité. Ces programmes pourraient aider les organisations à comprendre plus précisément la façon d'appliquer les règles sur la protection des données dans un secteur particulier. Ils pourraient aussi faciliter le travail des autorités de protection des données dans la création de politiques et de lignes directrices pertinentes, en mettant l'accent sur la façon d'assurer la conformité des contrôleurs de données.

Groupe de travail de l'Organisation de coopération et de développement économiques sur la sécurité de l'information et la vie privée : Rapport sur l'application transfrontière de la législation relative à la vie privée [16 octobre 2006]
Le Groupe de travail sur la sécurité de l'information et la vie privée (GTSIVP) de l'OCDE a récemment déposé un rapport sur l'application

DPA has the authority to conduct audits at its discretion at any time. However, the ability to complete efficient and effective audits is highly dependent on an organization's cooperation, maintaining good working relationships, and securing an agreement to act on audit recommendations. This is particularly true if recommendations are not binding because the DPA has no order making power–the case in Canada at the federal level.

Carrying out audits on a consensual basis encourages participation. Organisations that volunteer to be audited are indicating a willingness to comply and adopt good practice.

Not publishing names and audit results may also help encourage organisations to participate voluntarily in audits. "Naming and shaming" could deter participation in an audit programme. However, this approach should be distinguished from publication of formal enforcement action.

Audits help to educate DPA staff on the practical difficulties of day-to-day compliance. They also provide useful insights which can feed into good practice guidance issued by the DPA.

Audits are often described as a tool for promoting compliance. Their effectiveness might be measured to some degree by comparing the number of complaints received about the organisation pre- and post-audit.

An audit's effectiveness might also be gauged initially by the extent to which an organization accepts the audit's recommendations and implements them either immediately or once the auditors have delivered their report and "gone away".

Where there is little or no auditing:

Resources are an issue for all DPAs. They concentrate their enforcement activity on those problems which have a significant impact on individuals. Auditing is proactive and the DPA may not have time or resources to devote to this activity. However, it does offer benefits:

- Creating and developing relationships and communication links with organisations;
- Encouraging good practice; and
- Encouraging openness and collaboration.

Auditing that targets high risk sectors could possibly lead to a reduction in time spent on enforcement activities.

transfrontalière des lois relatives à la protection de la vie privée. Ce rapport présente quelques options pour faciliter la coordination des mesures d'application et des mécanismes de conformité transfrontaliers.

La plupart des organismes de supervision interrogés dans le cadre de ce rapport ont répondu qu'ils ne disposaient pas des pouvoirs appropriés pour échanger de l'information et mener des enquêtes en collaboration avec des autorités étrangères ou à la demande de ces dernières, et qu'ils tireraient profit de tels pouvoirs. Les efforts déployés pour accroître la portée des mesures d'application transfrontalières se trouvent entravés non seulement par le manque de pouvoirs accordés, mais aussi par des problèmes de cohérence notés dans certains régimes juridiques, par le manque de ressources et par l'établissement de priorités différentes d'un organisme de supervision à l'autre.

Si, en général, les organismes de supervision n'ont pas fait état d'un nombre important de plaintes transfrontalières, les percées technologiques et la mondialisation des échanges commerciaux incitent à penser que la circulation transfrontalière de données continuera d'augmenter. Les gains en efficacité sur les plans commercial et technologique ont pour corollaire une augmentation des risques à l'endroit de la protection de la vie privée. Il importe donc de s'attaquer aux défis que posent l'application des lois et la coopération transfrontalière.

Rapport de la Commission européenne sur la mise en œuvre de la directive sur la protection des données et suivi du programme de travail [7 mars 2007]
L'une des tâches définies par la Commission européenne vise à atténuer les différences nationales et à mieux harmoniser les lois sur la protection des données en Europe. On s'est entendu sur le principe de l'harmonisation des mesures d'application nationales à l'échelle européenne et on encourage les autorités responsables de la protection des données à adapter leurs pratiques intérieures à la position commune.

Dans la pratique cependant, même si les lois nationales prescrivant l'application des mêmes principes (p. ex. la Directive sur la protection des données de l'Union européenne 95/46/EC ou les directives de l'OCDE), les différences

In addition, auditing could be developed into an official certification programme where organisations audited by the DPA receive a "seal of approval". This could be of commercial value to organisations and, as such, they may be prepared to pay for the service. This in turn could provide resources for the DPA to use in other areas of enforcement or promotion of good practice.

Promoting self-assessment:

Nothing prevents a DPA from also promoting and supporting organisational self-audit (self-assessments). This can be a potent tool. Given the myriad of organizations, it is likely to be more productive for organizations to assess their own privacy practices with a view to compliance and continuous improvement. This would characterize a strong privacy management framework. Ideally, organizations should "police" themselves. A potentially powerful "simple question" for a DPA to ask an organization is this–how do you govern and manage privacy?

Scope of an Audit

An audit can help raise awareness of data protection within an organisation. Those involved in an audit will think about the issues before the audit commences, during the audit itself, and after the audit has finished.

There are generally two recognised approaches to deciding the scope of an audit.

Narrow & Deep:
The narrower the scope of the audit, the more successful it will be in making clear and precise recommendations to the organisation. Recommendations are more useful and easy to understand and implement when they focus on a specific aspect of an organisation's processing activities, rather than those gleaned from a snapshot of the entire organisation.

Wide & Shallow:
An audit with a wide remit will involve more individuals in an organisation and so will help raise the profile of data protection across the organisation.

Wide & Deep:
If time and resources permit (or limited resources can be concentrated), an audit that is both wide

d'interprétation et l'importance des motivations culturelles et historiques, ainsi que des raisons juridiques, peuvent entraver la coopération entre les autorités et compliquer la mise en œuvre de vérifications conjointes ou simultanées.

Les organismes de supervision européens doivent coopérer les uns avec les autres, en vertu de la Directive sur la protection des données. Il est cependant peu courant pour ces organismes de coopérer de façon proactive avec d'autres autorités équivalentes à l'extérieur de l'Europe, en raison des pouvoirs juridiques moins importants. On trouve pourtant des exemples de coopération de ce genre, comme le mémorandum officiel qui lie l'Agence espagnole de protection des données et la commission fédérale du commerce des États-Unis (United States Federal Trade Commission) dans la coopération pour la lutte contre le courrier électronique non sollicité, ou « pourriels ».

En Europe, il est possible de demander l'aide au Groupe de travail de l'article 29 pour des initiatives paneuropéennes de vérifications et de mise en application de la loi. Le Groupe de travail a récemment enquêté sur le secteur de l'assurance-maladie dans tous les pays membres de l'Union européenne. Les autorités de protection des données nationales ont fait parvenir des questionnaires aux entreprises d'assurance-maladie de leur juridiction – il s'agissait du seul moyen de recueillir systématiquement des renseignements dans tous les pays, en raison des pouvoirs variés des autorités de protection des données en Europe.

La coopération entre les autorités de protection des données en matière de vérifications transfrontalières peut s'avérer plus efficace dans la pratique si elle engage deux ou trois pays plutôt qu'un grand nombre d'entre eux.

Règles d'entreprise contraignantes
Le Groupe de travail de l'article 29 a diffusé plusieurs lignes directrices et rapports sur l'utilisation des Règles d'entreprise contraignantes en vue de protéger adéquatement les renseignements personnels transférés d'un pays à l'autre par un groupe d'entreprises. Les règles d'entreprise contraignantes d'une organisation doivent prévoir l'apport de vérificateurs internes ou de vérificateurs externes, ou une combinaison des deux. Le plan de vérification de l'organisation doit aussi prévoir la vérification par les autorités

and deep is likely to have the greatest and most lasting impact. DPAs appear to conduct few of these although the Office of the Privacy Commissioner of Canada has used such comprehensive type audits (see website www.privcom.gc.ca).

There is always a tension between wanting to conduct a wide-ranging audit in few organisations and covering more organisations in a narrower and/or shallower audit. This is particularly true when an authority has jurisdiction across all sectors, as in Europe, but limited time and insufficient human and financial resources,

All approaches have advantages and disadvantages. Whichever approach is adopted, it is critical to interview the right personnel in the organisation to gain a thorough understanding of its personal data processing.

Conclusion

The majority of jurisdictions reviewed do not carry out "compliance audits" in the true sense. Many audits result from complaints or suspected breaches of privacy legislation which might be better categorised as investigation or enforcement activity.

There are a number of challenges raised by the use of audits as a tool for promoting data protection compliance and good practice.

1. Lack of legal powers for the DPA may limit auditing and ancillary matters such as access to premises and documents.
2. Restrictions on information sharing inhibit cross-border activity in particular.
3. Incompatible legal regimes, either within or outside a country, restrict co-operation on audit projects.
4. Inadequate resources require directing those resources first at complaint handling, necessarily giving auditing a lower priority.
5. Differing compliance priorities.

However, compliance auditing conveys clearly identifiable benefits. They:

- encourage compliance and good practice within the audited organisation;
- serve as an instrument of change, improving privacy systems and promoting accountability for privacy;
- reduce privacy risks;

de protection des données. Il est par conséquent possible que la popularité grandissante des règles d'entreprise contraignantes fasse augmenter la demande de vérifications effectuées par des autorités de protection des données dans le cadre d'examens de la conformité.

Utilisation des vérifications en tant qu'outil de conformité

Dans les juridictions où des vérifications sont effectuées, les avantages perçus sont nombreux.

Promotion des vérifications

Là où il y a déjà des vérifications

Il n'est pas nécessaire de promouvoir la vérification là où l'organisme responsable de la protection des données a le pouvoir de faire des vérifications à sa discrétion et à tout moment. Cependant, la capacité d'effectuer des vérifications efficientes et efficaces dépend grandement de la coopération de l'organisation, du maintien de bonnes relations de travail et de la passation d'une entente sur la mise en œuvre des recommandations de la vérification. Cela est particulièrement important si les recommandations ne sont pas contraignantes parce que l'organisme chargé de la protection des données n'a pas de pouvoir d'ordonnance – comme c'est le cas à l'échelon fédéral au Canada.

La réalisation des vérifications sur une base consensuelle encourage la participation. Les organisations qui se prêtent à une vérification montrent leur volonté de se conformer et d'adopter des pratiques exemplaires.

Le fait de ne pas publier les noms et les résultats des vérifications peut aussi encourager les organisations à participer de manière volontaire aux vérifications. « Nommer et humilier » peut décourager la participation à un programme de vérification. Cependant, cette approche ne doit pas être confondue avec la publication des sanctions officielles.

Les vérifications aident le personnel des organismes chargés de la protection des données à développer ses connaissances sur les difficultés pratiques de la conformité dans les activités quotidiennes. Elles lui permettent aussi d'enrichir ses recommandations en matière de pratiques exemplaires.

- educate the DPA's staff;
- help to inform guidance and practice recommendations issued by the DPA; and
- develop relationships and open communication with organisations.

Without increased resources for DPAs it seems unlikely that the widely varying levels of audit activity, will change.

Suggestions for discussion: A model for DPA audits

In every case, an audit is a systematic assessment of an organization's personal data processing. It is a regular process for the DPA and generally a one time experience for the organisation and its management. Therefore, it is fair to discuss a model for DPA audits which brings more order and predictability to the process.

Each national DPA could assess its own audit practice against the model and then consider whether it wishes to introduce the new features into its audit system should its legal powers permit, or seek amendment to the relevant law.

In addition, the workshop at the Data Protection and Privacy Commissioners' 29th International Conference in Montreal, 25th-28th September 2007 could usefully add to and refine the following outline DPA Audit Model.

DPA Audit Model

The DPA should have the authority to:

1. choose the data controllers and data processors to audit;
2. enter a data controller's or data processor's premises;
3. demand the production of documents and records;
4. obtain answers to questions;
5. publicise the results without revealing any trade secrets or confidential information;
6. conduct a follow-up audit, if necessary, and
7. other points?

An audited organisation should be obliged to:

1. cooperate with the auditors, for example, by providing auditors with information and access to systems;
2. explain to the auditors how personal data is processed, by whom and for which purposes, and

On décrit souvent les vérifications comme des outils de promotion de la conformité. Leur efficacité peut être évaluée, dans une certaine mesure, par la comparaison du nombre de plaintes reçues au sujet d'une organisation, avant et après la vérification.

De prime abord, l'efficacité d'une vérification peut aussi être évaluée d'après la réaction de l'organisation aux recommandations. Les met-elle en œuvre immédiatement ou seulement après le dépôt du rapport et le « départ » des vérificateurs?

Là où il y a peu ou pas de vérification

Les ressources sont problématiques pour tous les organismes chargés de la protection des données. C'est pourquoi ils orientent leurs mesures d'application de la loi sur les problèmes qui ont une incidence importante sur les particuliers. La vérification est proactive et les organismes responsables de la protection des données ne disposent pas toujours du temps ou des ressources nécessaires pour se consacrer à ces mesures. Cependant, ce type de vérification offre d'autres avantages :

- Elle permet de créer et de développer des relations et des canaux de communication avec les organisations;
- Elle encourage l'adoption de pratiques exemplaires;
- Elle encourage la transparence et la collaboration.

Les vérifications qui visent les secteurs à haut risque pourraient entraîner une diminution du temps accordé aux mesures d'application de la loi.

En outre, les vérifications pourraient ouvrir la voie à l'élaboration d'un programme d'attestation officielle qui permettrait aux organisations qui font l'objet d'une vérification par un organisme chargé de la protection des données de recevoir un « sceau d'approbation ». Les organisations pourraient y voir une valeur commerciale ajoutée et, du coup, accepter de payer pour le service. De leur côté, les autorités de protection des données pourraient utiliser ces ressources supplémentaires pour entreprendre des activités dans d'autres domaines d'application de la loi ou pour promouvoir des pratiques exemplaires.

3. other points?

A data controller and data processor being audited by a DPA should have the right to:

1. be informed in advance, for example, a minimum of a week to arrange a mutually convenient day (this process is to be distinguished from a complaint about practices contrary to the law which may lead to a penal sanction and which would be handled by an investigation process with a different legal status);
2. be informed of the DPA's audit methodology;
3. have discussed with the DPA in advance the audit's scope (for example, processes, locations, numbers and positions of people to be interviewed);
4. accompany the auditors on the premises to facilitate discussions with staff at different levels (but not be present when individual and groups of staff are interviewed so that they may speak freely);
5. appoint IT staff to work with the audit team to ensure that any audit process involving an IT system does not damage that system;
6. receive a copy of an initial written report at the conclusion of the audit to ensure that management sees the observations, and any points that may cause conflicting views be discussed and possibly resolved (this report should be signed to show that the report has been read and discussed);
7. be given a period [four weeks?] to comment on a draft report before it is published [and that view to be published together with the DPA's report?];
8. be given a reasonable period to correct any identified faults before any follow-up audit, and
9. other points?

Appendix: Country Reports

1. France – CNIL

Meeting on 5th June 2007
Clarisse Girot – Head of European & International Affairs, CNIL
Florence Fourets – Head of Inspection and Audit, CNIL
Valerie Taylor – Consultant, Privacy Laws & Business

Legislative background
The French data protection legislation was

La promotion de l'auto-évaluation

Rien n'empêche les organismes responsables de la protection des données de promouvoir et de soutenir également l'autovérification (l'auto-évaluation) par les organisations. Il s'agit d'un outil prometteur. Étant donné le grand nombre d'organisations, il serait sans doute plus productif pour celles-ci d'évaluer elles-mêmes leurs pratiques relatives à la protection de la vie privée pour en vérifier la conformité et en favoriser l'amélioration continue. Une autovérification s'inscrirait dans un cadre bien établi de gestion de la protection de la vie privée. Idéalement, les organisations devraient « se surveiller » elles-mêmes. L'organisme chargé de la protection des données pourrait demander aux organisations de répondre à la question suivante : « comment gérez-vous la protection de la vie privée? », ce qui pourrait déclencher chez elles un processus de réflexion efficace.

Portée d'une vérification

Une vérification peut sensibiliser davantage une organisation à la protection des données. Les personnes qui participent à une vérification réfléchissent aux questions et aux problèmes que pose la protection des données avant, pendant et après la vérification.

En règle générale, il existe trois approches reconnues pour déterminer la portée d'une vérification.

Ciblée et en profondeur
Plus l'approche est ciblée, plus les vérificateurs sont en mesure de formuler des recommandations claires et précises à l'intention de l'organisation. Les recommandations sont plus utiles et faciles à comprendre et à mettre en œuvre si elles mettent l'accent sur un aspect précis des procédures de traitement des données plutôt que sur l'ensemble des activités de l'organisation.

Vaste et en surface
Une vérification dont la portée est plus grande exige la participation d'un plus grand nombre de personnes au sein de l'organisation et peut contribuer à accroître l'importance accordée à la protection des données.

Vaste et en profondeur
Si le temps et les ressources le permettent (ou si des ressources limitées peuvent y être

amended in 2004, in part to grant the regulatory authority (CNIL) new enforcement powers and sanctions. In the past, the CNIL relied largely on the notification process to establish whether there were any areas of concern about particular organisations.

The law does not specifically mention audits. There are powers to carry out "verifications" and the CNIL may enter premises (subject to giving appropriate notification to the public prosecutor) for the purposes of exercising these powers and copying any documents required. The power to carry out verifications is interpreted by the CNIL as an enforcement power. The CNIL considers that it has a power to carry out audits either using the powers of entry or on invitation by the organisation.

Terminology
The CNIL has initiated a number of inspections (verifications) where there have been suspected breaches or other potential areas of weakness. These inspections focus on specific issues or problem areas within an organisation and do not usually involve a review of the entire organisation.

Audits are viewed as assessments aimed at general compliance and good practice and would generally involve a thorough review of an entire organisation. The CNIL does not yet conduct general compliance audits, although some verifications have consisted of a full-fledged audit of the inspected party. The inspection/audit team is small (a total of six dedicated people but often including agents from other departments, such as the legal department). At present, the CNIL does not have the resources to conduct general compliance audits which are costly, time consuming and would tie up a significant number of team members.

Inspections carried out
In the last few years, the CNIL has carried out several major inspections in both the public and private sectors.

In the public sector, it conducted a detailed inspection of a major French city and local council suspected of non-compliance. The decision to inspect was prompted by a finding that the city council had an abnormally low rate of notification in CNIL's notification register. Formal compliance notices were issued following the inspection and sanctions may be imposed if the city fails to com-

consacrées en même temps), l'approche vaste et en profondeur aura les plus importantes retombées à long terme. Les autorités de protection des données semblent ne réaliser que très peu de vérifications de ce genre, mais le Commissariat à la protection de la vie privée du Canada a procédé à ce genre de vérifications exhaustives (voir le site Web www.privcom.gc.ca).

Il faut toujours trancher entre la possibilité de faire une vérification vaste dans quelques organisations et celle de vérifier plus d'organisations de manière plus ciblée ou en surface. C'est particulièrement le cas pour les organismes qui couvrent tous les secteurs, comme en Europe, mais qui n'ont pas le temps et ne disposent pas de ressources humaines et financières suffisantes.

Chaque approche a ses avantages et ses inconvénients. Peu importe l'approche privilégiée, il est essentiel de faire des entrevues avec le personnel concerné de l'organisation pour bien comprendre le mode de traitement des renseignements personnels de cette dernière.

Conclusion

Dans la plupart des juridictions examinées, il n'y a pas de « vérifications de conformité » proprement dites. De nombreuses vérifications font suite à des plaintes ou à des cas présumés de non-conformité aux lois sur la protection de la vie privée, et devraient éventuellement être considérées comme des enquêtes ou des mécanismes d'application.

L'utilisation des vérifications en tant qu'outil de promotion de la conformité et des pratiques exemplaires de protection des données pose certains défis.

1. Les organismes chargés de la protection des données n'ont pas toujours de pouvoirs juridiques, ce qui limite la vérification et les activités connexes, comme l'accès aux lieux et aux documents.
2. Les restrictions sur les échanges de renseignements entravent les activités transfrontalières en particulier.
3. L'incompatibilité des régimes juridiques, tant à l'intérieur qu'à l'extérieur d'un pays, peut nuire à la coopération dans les projets de vérification.
4. Étant donné l'insuffisance des ressources, il

ply.

Another inspection involved the electronic health records programme in France. This was selected for inspection because of its significance both nationally and within Europe, and because of the sensitive nature of the data involved. All parties involved were inspected, including sub-contractors.

Criminal investigation records held by the police (containing details of victims, suspects and, witnesses) are also inspected regularly. Such verifications essentially take place through the data subject's exercise of an indirect right of access to police files. This access right may be exercised only by CNIL's members with the authority of magistrates.

In the private sector, one thorough audit has involved online banking services. Again, this was identified as an area which presented particular risks to the security of confidential personal data.

The CNIL also conducted an inspection into the e-ticketing scheme used in the Paris public transport network. Here again, all parties involved were inspected, including sub-contractors. This series of inspections amounted in practice to a data protection audit of the whole scheme.

Rationale & Process

Organisations or sectors are selected for inspection based on complaints received (from individuals or the press) or problems identified by the CNIL during notification or prior authorisation processes.

The CNIL does not publish its programme of inspections in advance, nor does it make public the results of an inspection. In future, it will publish a list of organisations which have been inspected in its annual report.

In the vast majority of cases, the CNIL does not give advance notice to the organisations being inspected, nor are they given any specific guidance other than that which is generally available. Inspections tend to be carried out in areas where the CNIL has provided general guidance in the past, such as health records.

Inspection teams usually consist of three people, a legal expert, an IT expert and a former police officer. The organisation is fully involved in the

faut d'abord traiter les plaintes. Les vérifications n'arrivent qu'au deuxième rang des priorités.
5. Les priorités en termes de conformité sont divergentes.

Cependant, les vérifications de la conformité présentent des avantages notables.

- Elles font la promotion de la conformité et des pratiques exemplaires au sein de l'organisation qui fait l'objet d'une vérification;
- Elles sont un outil de changement, améliorant les systèmes de protection de la vie privée et encourageant la responsabilisation en matière de vie privée;
- Elles atténuent les risques d'atteinte à la vie privée;
- Elles informent le personnel des organismes responsables de la protection des données;
- Elles aident les organismes responsables de la protection des données à formuler des directives et des recommandations éclairées;
- Elles contribuent au développement des relations et favorisent une communication ouverte avec les organisations.

Sans une augmentation des ressources accordées aux autorités de protection des données, il semble peu probable que les niveaux très variables de l'activité de vérification changeront.

Suggestions aux fins de discussion : un modèle de vérification pour les organismes responsables de la protection des données

Dans tous les cas, une vérification est une évaluation systématique du traitement qu'effectue une organisation des données à caractère personnel. Il s'agit d'une procédure régulière pour l'autorité de protection des données, mais d'une expérience ponctuelle pour l'organisation qui en fait l'objet et sa direction. Il semble donc logique de discuter d'un modèle de vérification pour les organismes chargés de la protection des données dans le but de rendre la procédure plus ordonnée et prévisible.

Chaque organisme national responsable de la protection des données pourrait comparer ses pratiques de vérification au modèle et envisager d'intégrer les nouveaux éléments suggérés dans son système de vérification si ses pouvoirs

inspection process and signs off on the inspection record. The team would also issue a report following the conclusion of the inspection, unless no issues were identified. Inspections may take one to four days, depending on the size of the organisation, location of the inspection and issues involved. The CNIL has an internal, unpublished methodology which teams use when carrying out inspections.

Sanctions may be issued following an inspection and there would be a constant exchange of communications with the organisation about this process. Typically, inspections reveal issues about security or a lack of internal procedures.

Data Protection Officers
There is a formal system of Data Protection Officers in France–organisations may appoint an internal DPO and this removes certain obligations from the organisation (for example, concerning notification). Part of a DPO's job would be to conduct an internal audit of the organisation and so this role helps to promote auditing and good practice within organisations.

International Aspects
The electronic health records programme was investigated in France as part of the Article 29 Working Party investigation into the health insurance sector. Some complaints raise international issues but the CNIL has conducted no other audits across international borders.

Benefits of Auditing/Inspections & Problems
An inspection gives the CNIL the opportunity to understand how an organisation operates in practice, rather than by simply reading a notification. It also helps to forge good communication links with the organisation and helps compliance as the organisation becomes more aware of the CNIL and its powers of enforcement, and is encouraged to improve internal procedures.

The resource issue is the major problem–the CNIL is under-resourced and unable to conduct more wide-ranging audits. Therefore, they are focusing on the issues of significance to individuals, such as criminal records information, health data and financial information.

Future Developments
In France, the major change in recent years has been the increased use of sanctions. This has helped to raise the profile of data protection from a

juridiques le lui permettent, ou encore de proposer une modification à la loi applicable.

En outre, l'atelier prévu dans le cadre de la 29e Conférence internationale des commissaires à la protection des données et de la vie privée, qui se tiendra à Montréal du 25 au 28 septembre 2007, est l'occasion d'étoffer et d'améliorer le plan du modèle de vérification présenté ci-dessous.

Modèle de vérification pour les autorités de protection des données

L'organisme chargé de la protection des données devrait avoir le pouvoir :

1. de choisir les préposés au contrôle et au traitement des données à vérifier;
2. d'entrer dans les locaux de ces préposés;
3. d'exiger la production de documents et de dossiers;
4. d'obtenir des réponses à ses questions;
5. de publier les résultats de la vérification sans révéler les secrets commerciaux ou les renseignements confidentiels;
6. de procéder à une vérification de suivi, au besoin;
7. autre chose?

Une organisation vérifiée devrait être dans l'obligation :

1. de coopérer avec les vérificateurs en leur fournissant des renseignements et l'accès aux systèmes, par exemple;
2. d'expliquer aux vérificateurs le mode de traitement des données à caractère personnel et les fins de ce traitement, et d'identifier les personnes qui procèdent à ce traitement;
3. autre chose?

Un préposé au contrôle ou au traitement de données qui fait l'objet d'une vérification par un organisme chargé de la protection des données devrait avoir le droit :

1. d'être informé à l'avance – par exemple, au moins une semaine à l'avance – afin de prévoir une journée qui convient à tous (ce processus doit être distingué de celui du traitement d'une plainte au sujet d'une pratique contraire à la loi susceptible d'entraîner une sanction pénale et traitée dans le cadre d'une enquête au statut juridique différent);
2. d'être informé de la méthode de vérification employée par l'organisme chargé de la protection des données;

straightforward legal issue to a matter of broader general compliance.

It is possible that auditing could develop into an official certification programme of some kind, where organisations audited by the CNIL receive a "seal of approval". This could be of commercial value to organisations. However, unless and until there are additional resources available, the CNIL will be unable to pursue the development of a formal audit programme.

Conclusion
The CNIL does not audit in the sense of a broad review of an organisation's data processing activities for the purpose of promoting good practice. It focuses its limited resources on enforcement-related investigations where potential risks to individuals have been identified.

2. UK – Office of the Information Commissioner (ICO)

Meeting on 6th June 2007
Chris Turner – Head of Audit & Remedies, ICO
Sian Jones – Audit & Remedies Manager, ICO
Stewart Dresner – Chief Executive, Privacy Laws & Business
Valerie Taylor – Consultant, Privacy Laws & Business

Legislative background
The *Data Protection Act 1998* gives the Information Commissioner the specific power to carry out audits, either with the consent of the organisation in question–or by obtaining a warrant from the courts which allows access to premises without consent. The ICO has not actively considered seeking a warrant.

The Office may charge a fee for carrying out audits, with the permission of the Secretary of State, but has never done so.

Terminology
Audit is defined as an "assessment" of processing to determine the following of good practice. An audit is a broad assessment that would generally involve a thorough review of an organisation's processing activity, or a specific area of that activity. The audit team is small (three people) but they are dedicated almost entirely to audit activity. ICO expects to recruit two further people, most likely from within. Separate departments handle com-

3. de discuter à l'avance de la portée de la vérification avec l'organisme chargé de la protection des données (par exemple, des processus, des lieux, du nombre de personnes à interviewer et des postes de ceux-ci);
4. d'accompagner les vérificateurs sur les lieux pour faciliter les discussions avec le personnel de différents niveaux (mais pas au moment des entrevues avec un employé ou un groupe d'employés, afin que ceux-ci puissent parler librement);
5. de nommer des employés de la TI qui travailleront avec l'équipe de vérification pour veiller à ce que les systèmes de TI ne soient pas endommagés pendant les étapes de la vérification;
6. de recevoir, à la fin de la vérification, une copie de l'ébauche du rapport pour s'assurer que la direction puisse lire les observations et qu'elle discute des éléments conflictuels pour essayer de les résoudre (ce rapport devrait être signé pour montrer qu'il a bel et bien été lu et qu'il a fait l'objet d'une discussion);
7. d'obtenir un délai [quatre semaines?] pour formuler ses commentaires sur l'ébauche du rapport avant qu'il ne soit publié [et de faire publier ceux-ci avec le rapport de l'organisme chargé de la protection des données?];
8. d'obtenir un délai raisonnable pour corriger les faiblesses relevées par la vérification avant le suivi;
9. autre chose?

Annexe : Rapports des pays

1. France – Commission nationale de l'informatique et des libertés (CNIL)

Réunion du 5 juin 2007
Clarisse Girot – Directrice des relations européennes et internationales, CNIL
Florence Fourets – Directrice de l'expertise informatique et des contrôles, CNIL
Valerie Taylor – Conseillère, Privacy Laws and Business

Contexte législatif
En 2004, la loi sur la protection des données a été modifiée en France, en partie pour que de nouveaux pouvoirs d'application et de sanctions soient accordés à l'autorité de réglementation (CNIL). Avant, la CNIL s'appuyait grandement sur la procédure de notification pour cerner les

plaints and enforcement.

Audits carried out
In the past year the team conducted eight audits and plans a similar number of full audits in the coming year, along with 12-15 smaller audits into specific functions (for example, confidential waste disposal).

The ICO has recently publicised results of two of its audits, one involving a large public authority—Liverpool City Council—and another involving a major financial institution—Halifax Bank of Scotland (HBOS). The Liverpool City Council audit resulted from enforcement action against the authority following a complaint to the ICO. The HBOS audit followed press reports of security incidents at the bank which, if true, would breach an undertaking it previously gave the ICO.

Rationale
Organisations may be selected for audit in a number of ways:
1. A complaint received by the Compliance Division may be referred to the Remedies team, leading to a recommendation for audit. Consideration will be given to the size of the organisation, the detriment to individuals, the severity of the issue, and whether the problems are systemic.
2. An organisation which is subject to enforcement action or formal undertaking may agree to an audit as part of the sanctions imposed.
3. The Practice & Development Teams may suggest potential areas for audit, particularly concerning sectors or specific forms of processing that are generating substantial public debate, or where there is a great deal of change, and associated risk, underway. Examples include the health sector and public sector information sharing initiatives.
4. Organisations may approach the ICO directly to ask for an audit. This may be as a result of ICO publicity of their audit function. The ICO will then consider whether there are resources available to carry out the audit, the potential benefit to the organisations and how the audit could assist in developing its knowledge base.

The public sector is much more receptive to being audited than the private sector and, although the ICO has carried out many more audits in the public sector than the private sector, this is now beginning to change.

problèmes d'organisations en particulier.
La loi ne mentionne pas précisément le recours à des vérifications. La CNIL détient le pouvoir de procéder à des « vérifications » et elle peut entrer dans les locaux d'une organisation (à la condition de donner un avis approprié au procureur public) dans le but d'exercer son pouvoir et de photocopier tous les documents nécessaires. La CNIL interprète ce pouvoir comme un pouvoir d'application de la loi. Elle considère qu'elle peut imposer des vérifications ou en effectuer à la demande d'une organisation.

Terminologie
La CNIL a procédé à un certain nombre d'inspections (vérifications) qui ont permis de relever des cas de non-conformité ou des faiblesses. Ces inspections mettent l'accent sur des questions ou des problèmes précis au sein de l'organisation et ne nécessitent habituellement pas un examen complet de l'organisation.

Les vérifications, perçues comme des évaluations visant à vérifier la conformité et les pratiques exemplaires, devraient comporter un examen exhaustif de l'ensemble de l'organisation. La CNIL ne réalise pas encore de vérifications de la conformité générale, quoique certaines vérifications aient été des examens complets de fond en comble des organisations ciblées. L'équipe d'inspection/vérification est petite (six employés nommés au total et, souvent, quelques agents d'autres départements, comme les Services juridiques). À l'heure actuelle, la CNIL n'a pas les ressources nécessaires pour faire des vérifications de la conformité générale, car elles sont coûteuses, elles exigent beaucoup de temps et elles emploieraient trop de membres de l'équipe.

Inspections réalisées
Au cours des dernières années, la CNIL a procédé à plusieurs inspections importantes dans les secteurs publics et privés.

Dans le secteur public, elle a fait l'inspection d'une grande ville française et de son conseil municipal qu'on soupçonnait de non-conformité. La décision d'inspecter était motivée par le fait que le conseil municipal avait un nombre anormalement bas de notifications dans le registre des notifications de la CNIL. On a fait parvenir des avis de conformité officiels au conseil municipal après l'inspection. S'il ne se conforme pas, des sanctions lui seront imposées.

Sometimes an organisation's own agenda may shape the scope of an audit. For example, if the organisation's data protection contact believes it needs a high level commitment to data protection issues, the audit can be seen as a catalyst for change.

Process
While it is feasible for the ICO to obtain a warrant in order to carry out an audit, it has never done so. All audits have been carried out with the consent of the organisation. Warrant powers are usually reserved for serious breaches and criminal investigations. Information collected during an audit is provided voluntarily by the organisation. Again, it is possible for the ICO to use its enforcement powers to demand the production of documents, but this has never been done in connection with an audit and the ICO would prefer to operate on a consensual basis.

The ICO has published an audit methodology which is available on its website. This has been adapted and revised internally, particularly for use in smaller function-specific audits. The ICO has also developed its own internal checklists and questionnaires covering specific areas, such as information technology, and will consider updating the methodology when time permits.

The ICO would normally *request* information from the organisation being audited. There are powers to *demand* the production of documents and materials but it is unlikely that these would be used in a consent-based audit.

Audit teams consist of two or three people who are trained data protection specialists. One may have an IT background but the ICO is considering bringing in specialists where, for example, more specific technical knowledge is required. The 'on site' compliance aspect of the audits usually takes three days. Typically audits reveal problems with data subjects' access to personal data, data retention, and internal governance issues.

Reports are provided to the organisation but are not made public. The current policy is not to publicise audit details in the majority of cases. Audits are conducted with the consent of the organisation and so they are treated as confidential. The ICO also considers that, with consensual audits, publicising the findings might act as a deterrent.
There is no guarantee that the ICO will not take enforcement action as a result of an audit be-

Une autre inspection portait sur le programme des dossiers médicaux électroniques en France. On a décidé de se pencher sur ce programme en raison de son importance, tant à l'échelle nationale qu'européenne, et de la nature sensible des renseignements qu'on y trouve. Tous les intervenants ont été inspectés, y compris les sous-traitants.

Les rapports d'enquête criminelle conservés par la police (contenant des détails sur les victimes, les suspects et les témoins) sont aussi inspectés régulièrement. Ce genre de vérifications se produit surtout lorsque la personne visée par les données exerce son droit indirect de consulter les dossiers de la police. Ce droit d'accès peut être exercé seulement par les membres de la CNIL avec l'autorité du magistrat.
Dans le secteur privé, une vérification exhaustive a porté sur les services bancaires en ligne. Là encore, il s'agissait d'un domaine qui représentait des risques particuliers relatifs à la sécurité des données confidentielles à caractère personnel.

La CNIL a aussi réalisé une inspection du mécanisme de billetterie électronique utilisé par le réseau des transports en commun de Paris. Là encore, tous les intervenants ont fait l'objet d'une inspection, y compris les sous-traitants. Cet ensemble d'inspections a permis de faire une vérification du mécanisme entier en ce qui concerne la protection des données.

Justification et processus
Les organisations ou les secteurs à inspecter sont sélectionnés en fonction des plaintes (de particuliers ou des médias) ou des problèmes cernés par la CNIL au cours d'une notification ou avant les processus d'autorisation.

La CNIL ne publie ni son programme d'inspections à l'avance ni les résultats d'une inspection. À l'avenir, elle prévoit publier dans son rapport annuel une liste des organisations qui ont fait l'objet d'une inspection.

Dans la plupart des cas, la CNIL n'avertit pas à l'avance les organisations qui seront inspectées. Elle ne leur donne d'ailleurs aucune directive particulière à ce sujet. En règle générale, on procède aux inspections dans les domaines où la CNIL a déjà offert des directives générales, comme pour les dossiers médicaux.

Les équipes d'inspection regroupent

cause serious issues may be uncovered. However, because audits are carried out on a consensual basis, it would be very unusual for the organisation in question not to agree to resolve any issues that might be found. Agreeing to an audit indicates a willingness to address issues and establish good practice. The ICO would also look favourably upon an organisation that was open about its processing activities–and any problems–and had requested an audit.

International Aspects
The Article 29 Working Party has investigated the health insurance sector. A questionnaire was sent to the organisations in this sector–the only way of collecting information in a consistent manner across borders. The health insurance sector was selected because of the sensitive nature of information held and the perceived associated risks. Some of the health insurance companies also operate across Europe and this issue affects all European countries.

There could be a possibility of co-operating with other Data Protection Authorities on cross-border issues. This might work most successfully if only two or three countries were involved, rather than all EU countries, for example.

Benefits of Auditing & Problems
Auditing gives the ICO the opportunity to observe organisations and the way in which they handle personal data in practice. This helps educate ICO staff on the practical difficulties of day to day compliance. It also provides useful insights which can feed into guidance issued by the office on good practice.

An audit also helps improve relationships and encourages the organisation to stay in touch with the ICO if there are future problems or questions. If the audit can be carried out as a two-way dialogue, it helps encourage compliance and good practice and promotes data protection within the organisation.

The ICO does not currently have the resources to follow up on audit recommendations but ideally would wish to do so in some cases. Complaints monitoring can help by providing a mechanism for assessing whether recommendations have been implemented.

Future Developments
The ICO is hoping to expand the audit team and

habituellement trois personnes : un conseiller juridique, un spécialiste de la TI et un ancien agent de police. L'organisation participe à part entière au processus d'inspection et doit approuver le dossier d'inspection. L'équipe doit aussi préparer un rapport après l'inspection, sauf si aucun problème n'a été relevé. Une inspection prend d'un à quatre jours, selon la taille de l'organisation, le lieu de l'inspection et les problèmes en cause. La CNIL a une méthode interne non publiée qu'utilisent les équipes lorsqu'elles procèdent aux inspections.

À la suite d'une inspection, des sanctions peuvent être imposées. Dans ce cas, il y a des échanges continus avec l'organisation au sujet du processus. D'ordinaire, les inspections révèlent des problèmes de sécurité ou des procédures internes insuffisantes.

Correspondants à la protection des données
La France a un système officiel de correspondants à la protection des données (CPD). Les organisations peuvent nommer un CPD interne, ce qui les dispense de certaines obligations (en ce qui concerne la notification, par exemple). Le CPD a pour tâche, entre autres, de faire des vérifications internes et contribue du coup à promouvoir la vérification et les pratiques exemplaires au sein de l'organisation.

Aspects internationaux
Le programme des dossiers médicaux électroniques a fait l'objet d'une inspection en France dans le cadre de l'enquête sur le secteur de l'assurance-maladie menée par le Groupe de travail de l'article 29. Certaines plaintes révèlent des problèmes internationaux, mais la CNIL n'a pas réalisé d'autres vérifications transfrontalières.

Avantages et problèmes de la vérification/ inspection
L'inspection permet à la CNIL de comprendre le fonctionnement de l'organisation dans les faits, plutôt que sur papier. Elle aide à établir une bonne communication avec l'organisation et à la sensibiliser davantage au rôle de la CNIL et à ses pouvoirs d'application de la loi, ce qui contribue à accroître la conformité. De plus, elle favorise l'amélioration des procédures internes.

Le principal problème vient du manque de ressources. C'est pourquoi la CNIL ne peut procéder à des vérifications de plus grande envergure et met l'accent sur les questions qui

will continue to promote auditing as a tool for raising awareness of data protection and encouraging compliance and good practice.

It assessed demand for an audit accreditation scheme two years ago. Although audit companies expressed some support, data controllers showed little interest.

Conclusion
The ICO has conducted audits for several years and has a publicly available methodology. It publicises the audit function which is helping to raise awareness of the benefits of auditing and encouraging organisations to approach the ICO with audit requests. Audits are also used to resolve issues as part of enforcement activity.

3. Spain – Data Protection Authority

Meeting on 7th June 2007
Professor Artemi Rallo Lombarte – The Agency's Director
Ms. Mercedes Ortuño Sierra – Head of the International Department
Stewart Dresner – Chief Executive, Privacy Laws & Business

Spain's Data Protection Authority (the Agency) has jurisdiction over the private sector throughout Spain. Although there are three other Data Protection Authorities responsible for Madrid, Catalonia and the Basque country, they have jurisdiction solely for the public sector in these communities which are outside the scope of this study.

Legislative background
Data protection audits in Spain are conducted within the framework of Art. 40 of Spain's Data Protection Act (Organic Law 15/1999 of 13th December 1999 on the Protection of Personal Data known by the abbreviation LOPD). This law provides the general framework for data protection and implements European Union Directive 95/46/ CE into Spain's law.

Art. 40 is entitled "Powers of inspection" and covers the powers of the Agency to:

1. inspect personal data files and obtain any information they require;
2. require the disclosure or transmission of documents and data and to examine them;
3. inspect hardware and software used to proc-

touchent les particuliers, comme la protection des renseignements des casiers judiciaires, des données médicales et des informations financières.

Développements à venir
En France, l'utilisation accrue de sanctions est le plus important changement des dernières années. Cette pratique a permis de rehausser le profil de la protection des données. Elle n'est plus perçue uniquement comme un problème juridique, mais comme une question de conformité générale.

Il est possible que la vérification devienne un programme d'attestation officielle qui permettrait aux organisations vérifiées par la CNIL d'obtenir un « sceau d'approbation ». Ce sceau pourrait avoir une valeur commerciale pour les organisations. Néanmoins, sans ressources supplémentaires, la CNIL ne pourra pas élaborer de programme de vérification officiel.

Conclusion
La CNIL ne fait pas de vérifications complètes des procédures de traitement des données des organisations dans le but de promouvoir les pratiques exemplaires. Avec ses ressources limitées, elle met l'accent sur les enquêtes liées à l'application de la loi dans des cas où des risques possibles pour les particuliers ont été identifiés.

2. Royaume-Uni – Office of the Information Commissioner (ICO) *(Bureau du commissaire à l'information)*

Réunion du 6 juin 2007
Chris Turner – Chef de la vérification et des recours, ICO
Sian Jones – Gestionnaire de la vérification et des recours, ICO
Stewart Dresner – Administrateur général, Privacy Laws & Business
Valerie Taylor – Conseillère, Privacy Laws & Business

Contexte législatif
La *Data Protection Act* (loi sur la protection des données) de 1998 donne au commissaire à l'information le pouvoir d'effectuer des vérifications, soit avec le consentement d'une organisation, soit après avoir obtenu un mandat d'un tribunal qui l'autorise à entrer dans les locaux sans ce consentement. L'ICO n'a pas envisagé activement de demander un mandat.

ess the personal data;
4. obtain access to the premises where personal data is processed;
5. order the cessation of improper or illegal data processing and the deletion of improper or illegal files (Article 37f, as a preventive measure), and
6. block files in cases where a very serious violation is taking place (Article 49).

Inspectors are obliged to keep secret any information they acquire during and after conducting these tasks.

Secondary legislation is to be updated by the end of 2007 to provide more detailed rules on inspection procedures. Updating is needed because the current relevant secondary legislation, Art. 18 Royal Decree 1332/1994, was adopted to operate with the former 1992 law.

Terminology
There are two types of inspections or audits:

1. **Reactive inspections** result from a complaint of a privacy violation, or where the Agency learns of a privacy violation by other means, such as the media. In these cases, in addition to the powers cited in Art. 40 of the Data Protection Act, the Director of the Agency has a judicial power to issue a subpoena. He can also order that processing of personal data be stopped if it does not comply with the law.

   The most serious problem is the law's requirement that the Director of the Agency investigate *all* requests and complaints about privacy, regardless of whether they are worth expending the required resources. The rationale is that the Agency must by law be "at the service of the citizen". But, in practice, it means that the law prevents the Director from being an effective manager. He cannot choose his priorities nor allocate his resources according to his judgement of the importance of a complaint.

2. **Preventative audits** are those involving investigations of a specific sector to assess the extent to which organisations in the sector meet their legal obligations. These audits are designed to be educational not punitive, given that the result is usually recommendations on good practice. The 2005 annual report describes this type of audit as being "for fulfil-

Le Bureau peut facturer des frais de vérification, avec la permission du secrétaire d'État, mais il ne l'a jamais fait.

Terminologie
Le terme vérification désigne une « évaluation » des procédures en vue de déterminer si les pratiques sont adéquates ou non. Une vérification est une évaluation générale qui comprend habituellement un examen complet des procédures de traitement des données d'une organisation ou d'un secteur d'activités particulier. L'équipe de vérification est petite (trois personnes), mais elle se consacre presque entièrement à des activités de vérification. L'ICO prévoit recruter deux autres personnes, probablement à l'interne. Des services distincts s'occupent des plaintes et de l'application de la loi.

Vérifications réalisées
L'an dernier, l'équipe a réalisé huit vérifications et prévoit en réaliser le même nombre cette année, en plus de 12 à 15 vérifications de plus petite envergure concernant des fonctions particulières (par exemple, l'élimination des rebuts confidentiels).

L'ICO a récemment publié les résultats de deux de ses vérifications, l'une concernant un grand organisme public – le Liverpool City Council – et l'autre concernant une importante institution financière – la Halifax Bank of Scotland (HBOS). La vérification du Liverpool City Council a été effectuée en raison de mesures prises contre cet organisme à la suite d'une plainte déposée auprès de l'ICO. La vérification de la HBOS a été amorcée à la suite de comptes rendus journalistiques sur des incidents liés à la sécurité à la Banque. S'ils étaient confirmés, ces incidents briseraient une promesse faite antérieurement à l'ICO.

Justification
Les organisations qui font l'objet d'une vérification peuvent avoir été sélectionnées de différentes manières :

1. Une plainte reçue par la Division de la conformité peut être renvoyée à l'équipe des recours, entraînant ainsi la recommandation d'une vérification. La taille de l'organisation, les préjudices subis par des particuliers, la gravité du problème et le fait que ce problème soit systémique ou non sont les facteurs pris en considération.

ment of all the principles and rights of LOPD in a sector of activity previously selected. They are not aimed at declaring breaches, but rather at establishing a diagnosis of the situation of fulfilment, to detect deficiencies and provide recommendations that must be fulfilled to resolve them."

Sectoral audits
The sectors which have been audited in recent years are:

2006: Public and private schools
2005: Personnel recruitment by Internet
2004: Hospital laboratories and firms that provide them services
National Public Administration Institute
Hotel chains
2003: National Statistics Institute
Censuses of population and housing
2002: Competitions, games and television raffles
Remote banking (banking on-line)
Common file on asset insolvency
2001: National Statistics Institute
Historic car insurance files
Large department stores
2000: Electronic commerce
Hospitals
National AIDS Register
Directorate General of Traffic
1998: Bingo halls
1997: Public hospitals

The Agency's recommendations are at the following link:
https://www.agpd.es/index.php?idSeccion=75

Preparing for an audit and the inspectors' powers
The powers of the inspectors derive from the power vested in the Director of the Agency as the agent of the state. With his signature on the appropriate document (as his assessment of the inspection comes within his powers specified in the law and the Royal Decree above), the Agency's inspectors have "state authority" to enter premises and carry out their investigations and audits.

The Agency's Deputy Director is the Head of Inspections and he assembles a team appropriate to the sector being audited. They prepare by agreeing on:

- the scope of the audit

2. Une organisation qui fait l'objet d'une mesure d'application ou d'une procédure officielle peut accepter une vérification dans le cadre des sanctions imposées.
3. Les équipes responsables des pratiques et du perfectionnement peuvent suggérer des secteurs d'activités à vérifier, en particulier en ce qui concerne des secteurs ou des types de traitement précis qui alimentent d'importants débats publics ou qui sont touchés par des changements considérables auxquels sont associés des risques, comme le secteur de la santé et les projets d'échange d'information du secteur public.
4. Les organisations peuvent s'adresser directement à l'ICO pour demander une vérification. Cette demande peut résulter d'une annonce publique de la fonction de vérification de l'ICO. L'ICO vérifie ensuite s'il a les ressources nécessaires pour effectuer la vérification demandée, et détermine l'avantage potentiel que l'organisation en question peut en tirer et la façon dont cette vérification pourrait l'aider à enrichir sa base de connaissances.

Les organismes du secteur public sont beaucoup plus ouverts aux vérifications que ceux du secteur privé, mais, même si l'ICO a effectué beaucoup plus de vérifications dans le secteur public que dans le secteur privé, la situation est en train de changer.

Il arrive que le programme même d'une organisation détermine la portée d'une vérification. Par exemple, si la personne-ressource chargée de la protection des données croit que l'organisation a besoin d'un haut degré d'engagement à l'égard de la protection des données, la vérification peut être considérée comme une façon de catalyser des changements.

Processus
Bien que l'ICO puisse demander un mandat pour procéder à une vérification, il ne l'a jamais fait. Toutes ses vérifications ont été effectuées avec le consentement des organisations. Les pouvoirs conférés par un mandat sont habituellement réservés à des cas graves de non-conformité et à des enquêtes criminelles. L'information recueillie pendant une vérification est fournie volontairement par l'organisation. Ici aussi, l'ICO peut utiliser ses pouvoirs de contrainte pour exiger la communication de documents, mais il ne l'a jamais fait dans le cadre d'une vérification et

- how to divide the work among members of the audit team, and
- the types of sample systems and material they will review.

The inspection team, empowered by the Director's warrant, has the power to obtain documents from the data controller and even from third parties. For example, if an Internet company were to disappear, the inspectors would be able to access e-mail and web logs of third parties. Obstructing the inspectors is a separate infraction of the law which can lead to a higher fine. The national court treats such obstacles seriously–the maximum fine is 601,000 € per infraction of a provision of the data protection law.

The Agency never charges organisations a fee for conducting an audit.

A few times a year, an organisation may request an audit, usually as a result of informal discussions when both the Agency and the organisation agree that an audit would help clarify the situation. Such audits would not normally lead to a fine.

Rationale
The reasons for choosing a sector to audit can be due to:

- individual complaints (93 per cent of cases quoted in the 2005 annual report), and
- others (7 per cent of cases quoted in the 2005 annual report), problems identified by the media or, in the case of schools, as a result of a Congressional initiative expressed to the Agency's Director during presentation of his annual report to the Congress.

The most common sectors to receive inspection visits in 2005, according to that year's annual report, were:

- telecommunications (24 per cent of inspections and 29 per cent of legal proceedings which could lead to sanctions);
- financial services (19 per cent of inspections);
- public authorities (11 per cent of inspections).

Occasionally public and private sector organisations request an audit even if they are not subject to an Agency investigation. They may be faced by a new technology or a new use of personal data and seek the Agency's guidance. For example, Telefonica, (the major telecommunications company) asked for an audit of its new digital identity card which presented some novel privacy issues.

préfère procéder avec le consentement de l'organisation.

L'ICO a publié une méthode de vérification et l'a affichée sur son site Web. Cette méthode a été adaptée et révisée à l'interne, en particulier pour des vérifications plus restreintes de fonctions précises. L'ICO a également dressé ses propres listes de contrôle et questionnaires concernant des champs d'activité particuliers, comme la technologie de l'information (TI), et actualisera sa méthode lorsque le temps le lui permettra.

L'ICO *demande* normalement de l'information à l'organisation qui fait l'objet d'une vérification. Il existe des pouvoirs qui permettent d'*exiger* la communication de documents et de matériel, mais il est peu probable qu'ils soient utilisés dans le cadre d'une vérification avec consentement.

Les équipes de vérification sont composées de deux ou trois personnes spécialisées dans la protection des données. Il peut arriver qu'une de ces personnes ait de l'expérience en TI, mais l'ICO envisage de faire appel à des spécialistes lorsque, par exemple, des connaissances techniques plus pointues sont requises. La vérification « sur place » des aspects liés à la conformité prend habituellement trois jours. Généralement, les vérifications révèlent des problèmes concernant l'accès des personnes à leurs renseignements personnels, la conservation des données ou la gestion interne.

Les rapports sont remis à l'organisation, mais ne sont pas publiés. La politique actuelle est de ne pas publier les détails d'une vérification dans la majorité des cas. Comme les vérifications sont effectuées avec le consentement de l'organisation, elles sont traitées comme de l'information confidentielle. L'ICO considère aussi que, dans le cas des vérifications consensuelles, la publication des résultats pourrait constituer un facteur de dissuasion.

Il n'y a aucune garantie que l'ICO n'imposera pas de sanction à la suite d'une vérification qui a révélé de graves problèmes. Cependant, comme les vérifications sont effectuées avec le consentement des organisations, il serait très étonnant que l'organisation en question refuse de résoudre un problème révélé par une vérification. Le fait qu'une organisation accepte de faire l'objet d'une vérification indique sa volonté de résoudre les problèmes et d'établir une bonne pratique. De

And ENA, the public sector institute for training civil servants, also sought an audit.

Publication of audit results
The results and recommendations of sectoral audits are published to help improve standards across the sector.

If an audit results in a fine, then the name of the organisation is published. One example was a case involving serious security breaches in an online banking service.

The Agency publishes on its website (www.agpd.es) the names of the organisations which it audits, along with the full text of all of the Agency's Resolutions. The information is anonymized when a sanction is imposed on a physical person but it names legal persons (such as corporations). The Annual Report refers to the most important cases in general terms and refers readers to the website. The Agency gives the identification number of the sanction procedure so it can be checked on the website but does not provide organisations' names, although sectors are indicated where relevant. This policy is the result of an Agency Instruction in 2004 which stated that once a decision has been communicated to the affected parties, it must be made public in the following month.

Results of investigations/audits carried out
In 2006, 1,282 enforcement investigations were started, of which:

- 281 led to penal sanctions legal proceedings;
- 103 led to a public warning against public administration bodies (as it is the policy not to fine public authorities because ultimately the public pays in higher taxation)
- 632 cases concerned refusing a person access to records about themselves.

International Data Protection Audits
Spain has some experience cooperating with other national Data Protection Authorities, particularly on investigating and prosecuting unsolicited e-mail marketing, or spam. For example, the Agency has cooperated with the Netherlands Data Protection Authority in investigating a website, hosted by a Dutch company, which included illegally-collected personal data. This collaboration resulted in the removal of the illegal content from the website.

A wider data protection audit exercise has been

plus, l'ICO verrait d'un œil favorable une organisation disposée à faire preuve de transparence à l'égard de ses activités de traitement des données – et tout problème connexe – qui a demandé une vérification.

Aspects internationaux
Le Groupe de protection des données de l'article 29 a enquêté sur le secteur de l'assurance-maladie. Un questionnaire a été envoyé aux organisations de ce secteur — la seule manière systématique de recueillir de l'information dans divers pays. Le secteur de l'assurance-maladie a été sélectionné en raison de la nature sensible de l'information qui y est traitée et des risques perçus relativement à cette information. Certaines sociétés d'assurance-maladie œuvrent un peu partout en Europe et cette question touche tous les pays européens.

Il est possible de coopérer avec d'autres organismes chargés de la protection des données pour régler des questions transfrontalières. Ces efforts de coopération peuvent donner de bons résultats si seulement deux ou trois pays y participent, plutôt que tous les pays de l'Union européenne (UE) par exemple.

Avantages et problèmes de la vérification
Les vérifications donnent à l'ICO la possibilité d'observer, dans la pratique, les organisations et leur mode de traitement des données à caractère personnel. Elles éclairent le personnel de l'ICO sur les difficultés pratiques que soulève la conformité au quotidien. Elles lui donnent aussi des indications utiles susceptibles d'enrichir ses directives en matière de pratiques exemplaires.

Les vérifications aident également à améliorer les relations et encouragent les organisations à rester en contact avec l'ICO pour régler des questions ou des problèmes éventuels. Lorsque les vérifications donnent lieu à un dialogue, elles encouragent la conformité et les pratiques exemplaires, et favorisent la protection des données à l'intérieur des organisations.

Actuellement, l'ICO n'a pas les ressources requises pour effectuer un suivi après avoir formulé des recommandations au terme d'une vérification, bien que, dans certains cas, ce serait l'idéal. Le contrôle des plaintes peut servir de mécanisme d'évaluation pour déterminer si les recommandations ont été mises en œuvre ou non.

conducted over the last year initiated by the European Union's Art. 29 Data Protection Working Party. The Agency's International Department has led most of the 27-EU-member state initiative to audit the medical insurance industry.

This sector was chosen because it was considered to be reasonably comparable in the different member states and it processes sensitive data on millions of people. The audit was conducted in cooperation with the national medical insurance associations in each country and with the European confederation of medical insurance companies. The research examined many issues, including those related to employment–such as the extent to which medical data is shared with employers when medical insurance is a fringe benefit. For example, to whom does a medical insurance company release personal data in different circumstances?

The audit was conducted by a written questionnaire. Much time was spent on drafting and revising the questionnaire. The process was made more difficult because of national differences, such as:

1. level of understanding of even one common language;
2. data protection legal concepts;
3. existence or lack of audit powers;
4. appropriate methodology for the audit;
5. national rules on medical confidentiality;
6. national rules on interface between data protection law and freedom of information law;
7. national rules on use of genetic information as a factor in assessing an insurance risk leading to discrimination against people with a predisposition towards a certain health condition;
8. relationships between public authorities and private companies, and
9. enthusiasm for the task.

Adding to these difficulties was a lack of experience in some national DPAs in drafting and conducting audits and managing such an ambitious international project.

The national authorities co-operate more easily when they are conducting an enforcement action because normally few countries are involved.

Spain is now also co-operating in a separate OECD audit initiative which includes such non-European countries as Canada and Japan.

Développements futurs
L'ICO espère élargir son équipe de vérification. Il continuera de promouvoir la vérification comme outil pour accroître la sensibilisation à la protection des données et pour encourager la conformité et les pratiques exemplaires.

Il y a deux ans, il a évalué la demande d'un cadre d'attestation des vérifications. Même si les sociétés de vérification ont exprimé un certain appui, les contrôleurs de données se sont montrés peu intéressés.

Conclusion
L'ICO, qui dirige des vérifications depuis plusieurs années, a élaboré et publié une méthode. En faisant la promotion de la fonction de vérification, il contribue à la sensibilisation à ses avantages et encourage les organisations à lui demander d'effectuer des vérifications. Les vérifications sont aussi utilisées pour régler des questions dans le cadre de mécanismes d'application.

3. Espagne – Agencia española de protección de datos (Agence espagnole de protection des données)

Réunion du 7 juin 2007
M. Artemi Rallo Lombarte – Directeur de l'Agence
M^me^ Mercedes Ortuño Sierra – Chef du Département des affaires internationales
Stewart Dresner – Administrateur général, Privacy Laws & Business

En Espagne, le secteur privé relève de l'Agence espagnole de protection des données. Même s'il existe trois autres organismes responsables de la protection des données (à Madrid, en Catalogne et dans le Pays basque) ceux-ci n'exercent leur compétence que dans le secteur public de ces collectivités, dont ne traite pas la présente étude.

Contexte législatif
En Espagne, les vérifications sur la protection des données sont encadrées par l'article 40 de la loi sur la protection des données (Loi organique 15/1999 du 13 décembre 1999 sur la protection des données à caractère personnel, connue sous l'acronyme de LOPD). Cette loi assure un cadre général de protection des données et l'application de la Directive de l'Union européenne 95/46/CE par la loi espagnole.

L'article 40 s'intitule « Pouvoirs d'inspection » et

The Agency has also started conducting audits in some Latin American countries to check on the data protection procedures in place in countries to which data processing has been transferred from Spain but which do not meet the "adequacy" terms of the EU Data Protection Directive.

The Agency has concluded that:
- international co-operation on audits, and much else, is much easier if all the authorities involved have the same enforcement tools and capabilities, and
- a shortage of people and financial resources means that an audit is most usefully conducted on an issue which all the national partners consider a high priority.

Audit methodology
The Agency inspection team must work according to the specifications of the Royal Decree (see above), the text of which is available to all. The inspection team must follow these procedures because the investigation could result in a heavy fine, prompting the company to appeal to a court if the procedure had not been followed properly.

An inspection/audit team consists of two inspectors, meaning that the observations of one are always checked against those of the other inspector. There is no distinction in audit methodology between privacy and data security audits as the inspectors conduct both in the same visit. They enter the premises with a laptop computer and write a summary of the audit and present it to the company manager at the end of the visit. The inspectors give the organisation's manager a list of practical points which need attention, regardless of whether a penal sanction will come later in the process. He or she must sign the document to confirm that they have received it.

There is more flexibility of approach if there has not been a complaint against the company because there is less likelihood of a penal sanction.

There are no plans to amend the audit methodology but the Agency hopes the new Regulations will give the Director and his inspectors more flexibility to decide whether to audit an organisation. An inspection team consists of IT specialists with knowledge of data protection law. During the audit, inspectors instruct an organization's own staff member to interrogate and interact with computers and all types of IT systems. This ensures that a company cannot accuse an inspector of damaging

traite des pouvoirs de l'Agence suivants :

1. vérifier les fichiers de données à caractère personnel et obtenir toute information que cette vérification requiert;
2. exiger la communication ou la transmission de documents et de données et les examiner;
3. vérifier le matériel informatique et les logiciels utilisés pour traiter les données à caractère personnel;
4. obtenir l'accès aux locaux d'une organisation où des données à caractère personnel sont traitées;
5. ordonner la cessation de tout traitement de données inadéquat ou illicite et l'élimination des fichiers invalides ou interdits (article 37f, à titre de mesure préventive);
6. bloquer les fichiers dans les cas de très graves atteintes à la vie privée (article 49).

Les inspecteurs sont obligés de garder secrète toute information recueillie pendant et après l'accomplissement de leurs tâches.

La loi secondaire sera mise à jour d'ici la fin de 2007, de façon à contenir une description plus détaillée des règlements sur les procédures d'inspection. Cette mise à jour est requise parce que la disposition secondaire actuelle, l'article 18 du Décret royal 1332/1994, doit s'harmoniser avec l'ancienne loi de 1992.

Terminologie
Il y a deux types d'inspection ou de vérification :

1. **Les inspections** sont amorcées à la suite d'une plainte qui concerne une atteinte à la vie privée ou d'une information dont l'Agence a pris connaissance, par exemple dans les médias, selon laquelle il y a atteinte à la vie privée. Dans ces cas, en plus des pouvoirs mentionnés à l'article 40, le directeur de l'Agence a le pouvoir judiciaire d'émettre une assignation à témoigner. Il peut aussi ordonner l'interruption du traitement de données à caractère personnel si celui-ci n'est pas conforme à la loi.

   La contrainte la plus sérieuse est que le directeur de l'Agence enquête sur *toutes* les demandes et les plaintes relatives au respect de la vie privée, sans égard à leur importance relativement aux ressources requises pour effectuer une enquête. Cela s'explique par le fait qu'en vertu de la loi, l'Agence doit évaluer

company property.

On return to the Agency, team members present their factual report to a legal officer who conducts a legal analysis and recommends a sanction to the Director. If there is no evidence of a violation, the legal officer notes this conclusion in the Agency archive. Legal officers do not go on inspection/audit visits. The Agency always uses its own inspection/audit staff; it does not use outside auditors. Its inspection/audit team consist of 19 inspectors with IT skills, 14 legal experts and 17 auxiliary staff.

A company under audit appoints a manager to accompany the inspectors/auditors to check on the conduct of the inspection/audit. This ensures that the company understands the way in which the evidence is collected and the rationale for the observations and/or subsequent actions which are decided upon. An audit normally takes one to two days but the time from first receiving a complaint until the finalisation of a report, and subsequent decision on a sanction by the Director, often takes around six months (the maximum term permitted by the LOPD).

Reports and Resolutions
The factual report is shared with the audited organization which can then suggest amendments or propose an alternative version stating its viewpoint. The organization's response is considered by the legal analysts as they draft the Agency's resolution. Once the Director signs the Agency's final resolution, it is published on the Agency's website. The final resolution can be challenged in court. Typical findings are:

- poor data security which could enable a hacker to enter the system easily;
- staff misuse of data;
- no or few logs, so no audit trails.

The Agency has published specific areas of concern from its 2006 national audit of data protection in schools. These include:

1. weaknesses in information and consent to the processing of data;
2. poor quality data during the different steps of the processing;
3. lack of adequate safeguards regarding individuals' data protection rights, for example, access, correction, deletion and objection to processing, and
4. poor level of security, particularly regarding

chaque plainte en tenant compte de sa mission, qui est « de servir chaque citoyen ». Cependant, en pratique, cela signifie que la loi empêche le directeur d'agir en gestionnaire efficace. Il ne peut pas établir les priorités, ni allouer ses ressources en fonction de son appréciation de l'importance d'une plainte.

2. **Les vérifications préventives** sont celles qui comportent des examens d'un secteur en particulier pour évaluer la mesure dans laquelle des organisations du secteur concerné respectent leurs obligations juridiques. Ces vérifications ont des visées éducatives, non punitives, étant donné qu'elles aboutissent habituellement à la formulation de recommandations de pratiques exemplaires. Le rapport annuel de 2005 décrit ce type de vérifications comme des procédures [TRADUCTION] « aux fins du respect de tous les principes et droits énoncés dans la LOPD, relatifs à la protection des données à caractère personnel dans un secteur d'activité présélectionné. Elles ne visent pas à dénoncer des cas de non-conformité à la loi, mais plutôt à établir un diagnostic de la situation en ce qui a trait au respect des obligations juridiques, pour déceler les lacunes et formuler des recommandations pour y remédier ».

Vérifications sectorielles
Les secteurs qui ont fait l'objet de vérifications ces dernières années sont :

2006 : Écoles publiques et privées
2005 : Recrutement de personnel par Internet
2004 : Laboratoires d'hôpitaux et entreprises qui leur offrent des services
Institut national d'administration publique
Chaînes d'hôtels
2003 : Institut national de la statistique
Recensements de la population et des ménages
2002 : Concours, jeux et loteries télévisées
Banque à domicile (traitement en ligne des opérations bancaires)
Fichier commun sur l'insolvabilité d'un actif
2001 : Institut national de la statistique
Fichiers passés sur l'assurance-automobile
Grands magasins
2000 : Commerce électronique
Hôpitaux

sensitive data.

However, this national school audit exercise led to the preparation and distribution of advice on the use of personal data to more than 14,000 schools.

The Agency's website contains advice on data security for data controllers, as well as specific advice for each sector resulting from sectoral audits.

Benefits of audits
The Agency considers inspections and audits to be valuable because they are "a way of ensuring compliance without resulting in fines". The resulting recommendations help raise awareness in all sectors of the benefits of good data protection practice in managing personal data for the benefit of the organisation, the individuals and compliance with society's expectations expressed in the law.

The Agency's audits can lead to a discussion of practical management steps companies need to take to comply with the law, rather than being hit with large fines, and so it would be logical to expect companies to accept Agency audits. A data protection regulator's audit will never be welcome but can be regarded as acceptable in the same way as inspections in other fields–such as fire inspections in a factory or food hygiene in a restaurant. One result of this approach is that relations with companies improve the more an audit establishes practical steps a company can take to integrate data protection law into good management practices.

Future steps
The Agency's most important objective for the future is the ability to choose its own auditing priorities and methods rather than being required by law to investigate every complaint– however trivial. Some complaints could be dealt with by letter and others may, indeed, require an audit team's visit.

In future, smaller companies may outsource their data protection management to experts who could run a specialist service which a small company could not provide by itself. As a result, these experts would be in a better position to engage with inspectors from the Agency than small business owners.

The Agency's new Director wants to concentrate

Registre national sur le SIDA
Direction générale de trafic
1998 : Salles de bingo
1997 : Hôpitaux publics

Le lien suivant mène aux recommandations de l'Agence :
https://www.agpd.es/index.php?idSeccion=75

Préparation d'une vérification et pouvoirs des inspecteurs

Les pouvoirs des inspecteurs découlent du pouvoir conféré au directeur de l'Agence, en tant que représentant du gouvernement. Avec sa signature sur le document approprié (car son évaluation de l'inspection fait partie des pouvoirs précisés dans la loi et le Décret royal mentionnés ci-dessus), les inspecteurs de l'Agence peuvent, « en vertu de l'autorité de l'État », entrer dans les locaux d'une organisation et effectuer leur enquête et leur vérification.

Le directeur adjoint de l'Agence est le chef des inspections et il forme une équipe appropriée pour le secteur qui fait l'objet d'une vérification. Les membres de l'équipe se préparent en convenant des éléments suivants :

- la portée de la vérification;
- la manière de répartir les tâches entre eux;
- les types d'échantillons (systèmes et documents) qu'ils examineront.

En vertu du mandat de l'Agence, l'équipe d'inspection est autorisée à demander des documents au contrôleur de données et même à des tiers. Par exemple, si une entreprise Internet venait à disparaître, les inspecteurs pourraient avoir accès aux courriels et aux carnets Web des tiers. L'entrave à l'exercice de leurs fonctions constitue une infraction distincte et peut mener à une amende plus élevée. La Cour du pays considère que ce type d'infraction est grave — l'infraction à une disposition de la loi sur la protection des données peut entraîner une amende allant jusqu'à 601 000 euros.

L'Agence n'impose jamais de frais aux organisations pour la conduite d'une vérification.

Plusieurs fois par année, une organisation peut demander une vérification, habituellement à la suite de discussions informelles pendant lesquelles l'Agence et l'organisation conviennent qu'une vérification pourrait aider à clarifier la

on organisations whose processing of personal data has a great impact on large parts of the population; for example, an organisation managing a bio-bank or a DNA bank. The Agency was able to persuade a company managing a data bank of eight million blood donors that research could be conducted with anonymous data.

The new Director ideally wants a dialogue rather than an adversarial relationship, reserving the latter approach for when it is required by the facts of a case rather than a rigid legal prescription. Audits have their place in the larger objective stated by the Agency that "the future of privacy or data protection will depend on the credibility of the Supervisory Authorities in providing an effective protection against violations".

Bibliography

This analysis is based on the following key materials:

1. The Canadian Privacy Commissioner's Study on Auditing, December 2006
2. The OECD Working Party on Information Security and Privacy report on Cross-Border Enforcement of Privacy Laws, October 2006
3. European Commission Communication on the follow-up of the Work Programme for better implementation of the Data Protection Directive, March 2007
4. Article 29 Working Party Declaration on Enforcement [25 November 2004]
5. Organisation for Economic Co-operation and Development Working Party on Information Security and Privacy report on cross-border enforcement of privacy laws [16 October 2006]
6. European Commission report on the implementation of the European Data Protection Directive and follow-up work programme [7 March 2007]
7. The Article 29 Working Party paper WP108 on Binding Corporate Rules
8. Interview with representatives from the CNIL in France, June 2007
9. Interview with representatives from the UK Information Commissioner's Office, June 2007
10. Interview with representatives from the Data Protection Agency in Spain, June 2007

situation. Normalement, de telles vérifications n'entraînent pas d'amende.

Justification
Un secteur peut faire l'objet d'une vérification pour les raisons suivantes :

- des plaintes de particuliers (93 p. 100 des cas mentionnés dans le rapport annuel de 2005);
- autres (7 p. 100 des cas mentionnés dans le rapport annuel de 2005) : des problèmes relevés par les médias ou, dans le cas des écoles, en raison d'une initiative du Congrès prise lors de la présentation du rapport annuel par le directeur de l'Agence.

Les secteurs qui ont reçu le plus régulièrement des visites d'inspection en 2005, conformément au rapport annuel de l'année, sont les suivants :

- les télécommunications (24 p. 100 des inspections et 29 p. 100 des procédures juridiques qui pouvaient entraîner des sanctions);
- les services financiers (19 p. 100 des inspections);
- les organismes publics (11 p. 100 des inspections).

Occasionnellement, les organisations des secteurs public et privé demandent une vérification, même si elles ne font pas l'objet d'une enquête de l'Agence. Elles sont parfois confrontées à une nouvelle technologie ou utilisation des données à caractère personnel, et ils demandent des conseils à l'Agence. Par exemple, Telefonica (la principale société de télécommunications) a demandé la vérification de sa nouvelle carte d'identité numérique, qui suscite des inquiétudes relativement à la protection de la vie privée. L'École nationale d'administration (ENA), l'institut du secteur public qui forme les fonctionnaires, a également demandé une vérification.

Publication des résultats de vérification
Les résultats des vérifications sectorielles et les recommandations qui en découlent sont publiés pour aider à améliorer les normes dans l'ensemble du secteur.

Si une vérification entraîne une amende, le nom de l'organisation en question est publié. Par exemple, il y a eu un cas sérieux de brèche dans la sécurité des données associée à un service bancaire en direct.
L'Agence publie sur son site Web (www.agpd.es)

Further information is available from the following sources:

UK
http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/data_protection_complete_audit_guide.pdf

The Netherlands
http://www.dutchdpa.nl/downloads_audit/PrivacyAuditFramework.pdf

European Committee for Standardisation (CEN)
http://www.cen.eu/cenorm/businessdomains/businessdomains/isss/cwa/dppcwa.asp

les noms des organisations qui font l'objet d'une vérification, ainsi que le texte intégral des résolutions de l'Agence. Lorsqu'une organisation reçoit une sanction, l'information est dépersonnalisée; elle ne contient pas les noms des personnes physiques, mais seulement ceux des personnes morales (comme les sociétés). Le rapport annuel présente les cas les plus importants en termes généraux et renvoie les lecteurs au site Web. L'Agence indique le numéro d'identification de la procédure de sanction, de sorte que les lecteurs peuvent le retrouver sur le site Web de l'Agence, mais non les noms des organisations, même si les secteurs sont indiqués au besoin. Cette politique résulte d'une directive donnée par l'Agence en 2004 selon laquelle une décision communiquée aux parties concernées doit être rendue publique le mois suivant.

Résultats des enquêtes/vérifications
En 2006, 1 282 enquêtes liées à la mise en application ont débuté, dont :

- 281 ont entraîné des procédures judiciaires menant à des sanctions pénales;
- 103 ont mené à un avertissement public à des organismes administratifs publics (car la politique est de ne pas imposer d'amende à un organisme public, étant donné qu'en définitive, cela fait monter l'impôt des contribuables);
- 632 cas traitaient du refus de l'accès d'une personne à des dossiers qui la concernaient.

Vérifications internationales relatives à la protection de données
L'Espagne a une certaine expérience de coopération avec d'autres organismes nationaux responsables de la protection de données, en particulier des enquêtes et des poursuites concernant le marketing par courriels non sollicité, ou les pourriels. Par exemple, l'Agence a coopéré avec l'autorité de protection de données des Pays-Bas pour enquêter sur un site Web, hébergé par une entreprise hollandaise, qui affichait des données à caractère personnel recueillies illégalement. Cette collaboration a entraîné le retrait du contenu illégal du site Web.

L'an dernier, le Groupe de travail de protection des données de l'article 29 de l'Union européenne a entrepris une vérification de plus grande envergure. Le Département des affaires internationales de l'Agence a dirigé la plus grande partie du projet de vérification du secteur de l'assurance-maladie dans les 27 États membres

de l'UE.

Ce secteur a été choisi parce que les difficultés posées par la comparaison entre les divers États membres semblaient raisonnables et qu'il traitait des données de nature sensible concernant des millions de personnes. La vérification a été effectuée en collaboration avec les associations d'assurance-maladie nationales de chaque pays et la confédération européenne des sociétés d'assurance-maladie. La recherche a porté sur de nombreuses questions, y compris celles liées à l'emploi — comme la mesure dans laquelle les données médicales sont transmises aux employeurs lorsque l'assurance-maladie constitue un avantage social. Par exemple, à qui les sociétés d'assurance-maladie communiquent-elles les données à caractère personnel dans différentes circonstances?

La vérification a été effectuée à l'aide d'un questionnaire écrit. La rédaction du questionnaire et sa révision ont pris beaucoup de temps. Le processus a été plus difficile en raison de différences entre les pays; par exemple :

1. la mesure dans laquelle une langue commune était comprise;
2. les concepts juridiques relatifs à la protection des données;
3. l'existence ou le manque de pouvoirs de vérification;
4. la méthode de vérification appropriée;
5. les règles nationales sur la confidentialité médicale;
6. les règles nationales concernant les liens entre la loi sur la protection des données et celle de l'accès à l'information;
7. les règles nationales sur l'utilisation de l'information génétique, comme facteur d'évaluation des risques d'assurance qui entraîne la discrimination de personnes ayant des prédispositions à certaines maladies;
8. les relations entre les autorités publiques et les entreprises privées;
9. l'enthousiasme à l'égard de la tâche.

À ces difficultés s'ajoutait le manque d'expérience de certains organismes responsables de la protection des données dans la rédaction et la conduite de vérifications, ainsi que dans la gestion d'un projet international de cette envergure.

Les autorités nationales coopèrent plus facilement lorsqu'elles engagent des mesures d'application,

parce que celles-ci ne mettent habituellement en jeu que quelques pays à la fois.

L'Espagne est maintenant en train de collaborer à un projet de vérification distinct de l'OCDE, qui comprend des pays non européens comme le Canada et le Japon.

L'Agence a aussi commencé à effectuer des vérifications en Amérique latine pour vérifier les procédures de protection des données en place dans les pays où le traitement de données, transférées de l'Espagne, ne respecte pas les conditions de « conformité » énoncées dans la directive de l'UE sur la protection des données.

- L'Agence a conclu :que la coopération internationale pour des vérifications, et bien d'autres activités, était plus facile lorsque les autorités concernées disposaient des mêmes outils et capacités de mise en application;
- que la pénurie de ressources humaines et financières fait en sorte que les vérifications les plus efficaces sont celles qui traitent de questions prioritaires pour tous les partenaires nationaux.

Méthode de vérification

L'équipe d'inspection de l'Agence doit suivre les directives du Décret royal (voir ci-dessus) dont le texte est accessible à tous. Elle doit respecter ces procédures, car l'enquête peut se solder par une lourde amende, ce qui peut inciter la société visée à se tourner vers un tribunal si la procédure n'a pas été suivie scrupuleusement.

L'équipe d'inspection ou de vérification est composée de deux inspecteurs, ce qui suppose que les observations de l'un sont toujours comparées à celles de l'autre. Il n'y a aucune différence entre les méthodes de vérifications relatives à la protection de la vie privée et celles relatives à la sécurité des données, dans la mesure où les inspecteurs effectuent les deux vérifications en une seule visite. Ils arrivent sur les lieux munis d'un ordinateur portable et rédigent un résumé de la vérification qu'ils présentent au directeur de la société à la fin de leur visite. Les inspecteurs fournissent au (à la) gestionnaire de l'organisation une liste des points pratiques qui réclament une attention particulière, qu'une sanction pénale soit prévue ou non. Il ou elle doit signer le document afin de confirmer qu'il ou elle l'a bien reçu.

L'approche est plus souple lorsqu'aucune plainte n'a été déposée contre la société, car la sanction pénale est alors moins probable.

Aucune modification de la méthode de vérification n'est envisagée actuellement, mais l'Agence espère que les nouveaux règlements donneront une plus grande marge de manœuvre au directeur et à ses inspecteurs pour décider de vérifier ou non une organisation. Une équipe d'inspection est composée de spécialistes en TI qui connaissent les lois relatives à la protection des données. Pendant la vérification, les inspecteurs chargent l'un des employés de l'organisation d'interroger et de consulter les ordinateurs et tous les systèmes informatiques. Cette mesure permet d'éviter que la société accuse un inspecteur d'avoir endommagé son matériel.

De retour à l'Agence, les membres de l'équipe montrent leur rapport factuel à un conseiller juridique, qui l'analyse d'un point de vue juridique et recommande une sanction au directeur. S'il n'existe aucune preuve d'infraction, le conseiller juridique consigne cette conclusion dans les archives de l'Agence. Les conseillers juridiques n'effectuent pas de visites d'inspection ou de vérification. L'Agence n'emploie que ses inspecteurs; elle ne fait appel à aucun inspecteur à l'externe. L'équipe de vérification et d'inspection comprend 19 inspecteurs ayant des compétences en TI, 14 experts juridiques et 17 employés auxiliaires.

La société qui fait l'objet d'une vérification délègue un employé-cadre pour accompagner les inspecteurs ou les vérificateurs et vérifier la bonne marche de l'inspection ou de la vérification. Cette présence garantit que la société comprendra la manière dont les preuves auront été recueillies et les raisons qui auront mené aux observations et aux mesures prises par la suite. Une vérification prend en général un ou deux jours, mais il s'écoule souvent environ six mois (durée maximum autorisée par la LOPD) entre la réception de la plainte et l'achèvement d'un rapport et la décision de sanction qui en découle formulée par le directeur.

Rapports et résolutions

Le rapport factuel est communiqué à l'organisation vérifiée, qui peut alors soit proposer des modifications, soit présenter une version différente pour exposer son point de vue. La réponse de l'organisation est examinée par les

conseillers juridiques au moment où ils préparent la résolution de l'Agence. Une fois que le directeur a signé la résolution finale, celle-ci est publiée sur le site Web de l'Agence. Elle peut être contestée devant un tribunal. Les conclusions les plus courantes sont les suivantes :

- une protection insuffisante des données permettant à un pirate d'infiltrer facilement le système;
- une mauvaise utilisation des données par les employés;
- l'absence ou l'insuffisance de registres, donc peu de pistes de vérification.

À la suite de sa vérification nationale de la protection des données dans les écoles, l'Agence a publié une liste de secteurs qui suscitent des préoccupations. Ceux-ci comprennent :

1. des faiblesses dans l'information et le consentement concernant le traitement des données;
2. une piètre qualité des données à toutes les étapes de traitement;
3. un manque de dispositifs adéquats pour respecter les droits liés à la protection des données à caractère personnel, comme l'accès à l'information, la possibilité d'y apporter des correction ou de l'éliminer, et de contester le traitement des données;
4. un niveau de sécurité trop faible surtout en ce qui concerne les données de nature sensible.

Néanmoins, cette vérification nationale des écoles a conduit à la formulation et à la diffusion à plus de 14 000 écoles de conseils sur l'utilisation des données à caractère personnel.

Le site Web de l'Agence donne des conseils sur la protection des données à l'intention des contrôleurs des données, ainsi que des conseils spécifiques à chaque secteur découlant de vérifications sectorielles.

Avantages des vérifications

L'Agence estime que les inspections et les vérifications sont précieuses, car elles constituent « un moyen de garantir la conformité à la loi sans entraîner d'amende ». Les recommandations ainsi formulées contribuent à sensibiliser tous les secteurs sur les avantages des pratiques exemplaires de protection des données dans la gestion de données à caractère personnel, pour les organisations et les particuliers, et pour répondre aux attentes de la société, telles qu'elles

sont exprimées dans la loi.

Les vérifications de l'Agence peuvent conduire à une discussion sur les mesures de gestion pratiques que les sociétés doivent prendre pour se conformer à la loi et éviter ainsi de lourdes amendes. Il serait donc logique que les sociétés acceptent de bon gré les vérifications de l'Agence. Une vérification par un organisme responsable de la protection des données ne sera jamais la bienvenue, mais elle peut être considérée comme acceptable au même titre que les inspections dans d'autres domaines – inspections pour la lutte contre les incendies dans les usines ou inspections de l'hygiène alimentaire dans les restaurants. Cette approche permet d'améliorer les relations avec les entreprises, au fur et à mesure que la vérification définit les mesures qu'elles peuvent prendre pour adopter des pratiques de gestion conformes à la loi sur la protection des données.

Prochaines étapes

L'objectif le plus important de l'Agence est de pouvoir définir ses priorités et choisir ses méthodes de vérification, plutôt que d'être contrainte par la loi à enquêter sur chaque plainte – aussi négligeable soit-elle. Certaines plaintes pourraient être traitées par courrier alors que d'autres requièrent évidemment la visite d'une équipe de vérification.

À l'avenir, les plus petites sociétés pourraient confier leur gestion de la protection des données à des experts, qui pourraient proposer les services de spécialistes qu'elles ne peuvent s'offrir à l'interne. En effet, ces experts seraient bien mieux placés que les propriétaires de petites entreprises pour prendre des engagements face aux inspecteurs de l'Agence.

Le nouveau directeur de l'Agence souhaite se concentrer sur les organisations dont les activités de traitement de données personnelles a une incidence marquée sur de larges pans de la population; par exemple une organisation qui gère une banque de données biologiques ou une banque d'ADN. L'Agence a pu convaincre une société responsable d'une banque de données de 8 millions de donneurs de sang que la recherche était possible avec des données anonymes.

Le nouveau directeur aspire à des relations axées sur un dialogue plutôt que sur la confrontation et ne réserve cette dernière approche qu'aux cas où

des procédures judiciaires fermes sont requises en raison des faits et non de la loi. Les vérifications ont leur place dans un contexte plus large où [TRADUCTION] « l'avenir de la protection de la vie privée et des données dépend de la capacité des organismes de supervision d'assurer une protection efficace contre la non-conformité ».

Bibliographie

Cette analyse a été réalisée à partir des documents suivants :

1. *Étude sur la vérification*, commissaire à la protection de la vie privée du Canada, décembre 2006
2. OCDE – Groupe de travail sur la sécurité de l'information et la vie privée. Rapport sur l'application transfrontière de la législation relative à la vie privée, octobre 2006
3. Commission européenne. Communication de la Commission au Parlement européen et au Conseil – Suivi du Programme de travail pour une meilleure mise en application de la directive sur la protection des données, mars 2007
4. Groupe de travail « Article 29 » sur la protection des données. Déclaration du Groupe de travail Article 29 concernant la mise en application. [25 novembre 2004]
5. Organisation de coopération et de développement économiques. Groupe de travail sur la sécurité de l'information et la vie privée. Rapport sur l'application transfrontière de la législation relative à la vie privée. [16 octobre 2006]
6. Commission européenne. Communication de la Commission au Parlement européen et au Conseil. Suivi du Programme de travail pour une meilleure mise en application de la directive sur la protection des données. [7 mars 2007]
7. Groupe de travail « Article 29 » sur la protection des données. Document de travail (WP108) établissant une liste de contrôle type pour les demandes d'approbation des règles d'entreprise contraignantes.
8. Entrevue avec des représentants de la CNIL en France, juin 2007
9. Entrevue avec des représentants du UK Information Commissioner's Office (Bureau du commissaire à l'information du Royaume-Uni), juin 2007
10. Entrevue avec des représentants de l'Agence espagnole de protection des données, juin 2007

On trouvera des informations supplémentaires à partir des sources suivantes :

Royaume-Uni
http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/data_protection_complete_audit_guide.pdf

Pays-Bas
http://www.dutchdpa.nl/downloads_audit/PrivacyAuditFramework.pdf

Comité européen de normalisation (CEN)
http://www.cen.eu/cenorm/businessdomains/businessdomains/isss/cwa/dppcwa.asp