PRIVACY HORIZONS: TERRA INCOGNITA

29th International Conference of Data Protection and Privacy Commissioners

September 25 to 28, 2007
Montreal, Canada

LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE : TERRA INCOGNITA

29e Conférence internationale des commissaires à la protection des données et de la vie privée

du 25 au 28 septembre 2007
Montréal, Canada

Terra Incognita

Atelier sur la vérification en matière de protection de la vie privée : Observations du président

Conférence internationale de 2007 des commissaires à la protection des données et de la vie privée

Montréal, Québec (Canada)

Troisième atelier – La vérification
Le mercredi 26 septembre 2007
De 13 h 30 à 16 h

M. Artemi Rallo Lombarte
Directeur, Agence espagnole de protection des données

Qu'est-ce que la vérification?

- La vérification par rapport à l'inspection
  - La vérification est effectuée à l'initiative d'une autorité de protection des données (APD) ou d'un contrôleur des données
    - aperçu axé sur une démarche préventive visant à assurer une **conformité générale** et débouchant habituellement sur des recommandations
  - L'inspection fait suite à une plainte ou à une préoccupation d'une APD
    - enquête portant sur un **domaine particulier** d'une présumée brèche dans la protection des données pouvant déboucher sur des sanctions
- Une application efficace nécessite une approche proactive et réactive
  - Dans le contexte de cet atelier, nous utiliserons généralement le terme « vérification » – un concept inclusif

Processus de vérification de l'Espagne

- **Application préventive : 20 %**
  - **Vérifications systématiques** – secteurs public et privé
  - Débouche sur des recommandations, mais également sur une résolution
  - Inclut des mesures non liées à une vérification : lignes directrices, consultations, publicité
- **Application réactive : 80 %**
  - La loi oblige l'Agence espagnole de protection des données à **régler toutes les plaintes des citoyens**
  - Les plaintes sont généralement réglées à la suite d'une demande de communication volontaire d'information
    - **La vérification peut se faire sur place ou au moyen d'une assignation à témoigner**
  - Des amendes pour violation sont fixées selon la nature de l'infraction (mineure, grave ou très grave), tel que défini par la loi

→ Les **inspections** sont effectuées par des experts en TI, qui soumettent un rapport factuel au Service juridique

→ Le **Service juridique** analyse le rapport, entame les procédures de sanction, au besoin, et formule des recommandations en vue d'une résolution

→ Le **directeur** approuve la résolution, qui est susceptible d'appel en cour

Collaboration en matière d'application : Collaboration bilatérale au sein de l'UE

- 2000 – L'Agence espagnole de protection des données inflige une amende à un fournisseur de contenu pour avoir affiché des renseignements personnels concernant des agents de police sur son site Web
  - Aucune amende n'a été infligée au fournisseur d'accès Internet (FAI) – les données ont été retirées immédiatement après réception de l'injonction
- 2006 – L'Agence espagnole de protection des données apprend que le contenu est toujours affiché sur un site miroir des Pays-Bas
  - **L'Agence espagnole collabore avec l'autorité de protection des données des Pays-Bas (la CBP) pour que le contenu soit retiré**
  - La CBP adresse une demande d'information au FAI des Pays-Bas avec, en annexe, une résolution de l'Agence espagnole de protection des données stipulant que les données sont affichées illégalement
  - Le FAI **retire immédiatement** le contenu

<u>Stratégie et outils de collaboration</u>

- **Échange d'information** sur les mesures prises par l'Espagne et sur les résultats obtenus
- **Vérification** du site par la CBP, et analyse juridique et factuelle (annuaire Internet)
- **Collaboration à l'élaboration d'une stratégie d'application**
- **Communication** continue des mesures prises et de l'état d'avancement du dossier

Collaboration en matière d'application : Pourquoi synchroniser les vérifications ?

- **L'application vise à accroître la conformité**
- Le plus grand obstacle à l'application est la pénurie de ressources
- Une application synchronisée pourrait permettre l'harmonisation des pratiques de protection des données
  - La mise en commun de l'information et la collaboration peuvent réduire les écarts dans les "MS "
    - Simplification de l'application, utilisation de pratiques exemplaires, application plus efficace
  - Unification des pratiques pour permettre l'autoréglementation, comme les règles contraignantes pour les entreprises
    - Réduire le fardeau de l'application
    - Améliorer la conformité dans tous les secteurs
- **Essentiel à l'amélioration de notre approche et à l'instauration de mesures communes**

Collaboration en matière d'application : Collaboration multilatérale au sein de l'UE

- **La conformité est généralement bonne**, mais certains points suscitent des inquiétudes

Aller de l'avant :

- **Recommandations** pour combler les écarts dans la conformité
- Les contrôleurs des données non participants devraient noter les conclusions
- Analyser et améliorer la méthodologie en vue des futures démarches
  - Continuer à coordonner l'application avec les organisations représentantes telles que "CEA"
  - Outiller les APD de façon appropriée pour assurer une application efficace
  - Améliorer l'instrument d'enquête – questions plus claires et mieux ciblées
  - Effectuer des enquêtes de suivi approfondies afin d'améliorer la conformité, et ne pas se limiter à évaluer le degré de conformité

Collaboration en matière d'application : Collaboration avec des pays tiers

- Mesure d'application sans précédent à l'extérieur de l'UE : inspections sur place visant des données transférées en Colombie
- Fondement juridique : **clause contractuelle type** pour les transferts de données internationaux
  - Là où les données sont transférées dans d'autres pays, l'APD peut soumettre l'importateur à une vérification **en recourant aux mêmes outils et techniques utilisés pour la vérification de l'exportateur** dans la juridiction de l'APD
- Une entreprise de télécommunication a inclus une clause dans son contrat d'impartition d'un soutien technique à la Colombie
  - L'Agence espagnole de protection des données était consciente du risque d'utilisation inappropriée des données ou de brèches dans la sécurité de celles-ci; **il a été décidé que des vérifications seraient effectuées sur place**

Collaboration en matière d'application : Collaboration avec des pays tiers

- Collaboration et **facilitation par l'exportateur** (contrôleur des données)
  - Il a coordonné les inspections
  - Il a servi de point de contact pour les vérifications
  - Il a soumis à une vérification tous les importateurs de données concernés en Colombie
- **La vérification en Colombie** a duré 5 jours
  - 3 inspecteurs + 1 sous-directeur de l'inspection
    - Accès aux documents et examen
    - Vérifications sur place des systèmes techniques
    - Accès aux données stockées dans le système et évaluation de ces données
    - Vérification sur place des mesures de sécurité
- Conclusions : **conformité générale** aux exigences techniques et organisationnelles en matière de sécurité
  - Les importateurs ont perçu **la vérification comme un moyen utile** d'améliorer leurs pratiques

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

M. Artemi Rallo Lombarte
Directeur, Agence espagnole de protection des données
http://www.aepd.es

Participants au troisième atelier

- M. Chris Turner
  - Chef, Vérification et recours, Bureau du commissaire à l'information (Royaume-Uni)
- M. Joel Winston
  - Directeur adjoint, Privacy and Identity Branch, Bureau of Consumer Protection, Commission fédérale du commerce (États-Unis)
- M. Nicholas Cheung
  - Directeur, Services de certification, Institut canadien des comptables agréés
- M^{me} Yim Chan
  - Directrice exécutive du service mondial de protection des renseignements personnels et chef du service de protection des renseignements personnels, IBM (Canada)

Vérification de la protection des données
Perspective du Royaume-Uni

Chris Turner
Chef, vérification et recours
Commissariat à l'information

Contexte

- **Adoption de la 1998 Data Protection Act – Accorde le pouvoir de vérifier avec l'approbation du contrôleur des données.**
- **Au milieu de 2001, publication d'un manuel de vérification annoncé sur le site Web – Il s'agit d'une étape clé pour le Commissariat.**
- **À la fin 2003, une nouvelle initiative est lancée pour mettre en œuvre un programme d'essais de vérification et réfléchir à l'élaboration de plans d'accréditation des vérifications.**
- **Les vérifications sont effectuées par les membres d'une équipe de conformité.**
- **En mai 2005, une équipe de vérification permanente est créée et intégrée à une nouvelle Division des mesures réglementaires.**
- **En 2007, nous envisageons d'élargir l'équipe et d'en accroître les pouvoirs.**

Programme de vérification

- **Le programme est fondé sur :**
  - **les bénévoles**
  - **un thème**
  - **Les questions et les cas de non conformité cernés**
- **Participation**
  - **Invitation et demandes**
  - **Évaluation et Recours**
  - **Engagement**
- **Composition**
  - **Principalement les pouvoirs publics, les entreprises privées, le plus souvent à la suite de projets**

Méthodologie de la vérification

- **Fondée de façon générale sur le manuel de vérification**
- **Les 2/3 des membres de l'équipe, composée d'hommes, ont une expérience en matière de conformité**
- **Établissement de relations clés afin de faciliter la coopération et d'établir les avantages mutuels**
- **Délimitation et planification (renseignements généraux)**
- **Vérification du caractère adéquat**
  - **Politiques, procédures, lignes directrices, matériel didactique**
  - **Évaluation de la liste de contrôle**
- **Vérification de la régularité**
  - **Système de protection des données**
  - **Processus opérationnels**
  - **Opérations et applications sur ordinateur**

Résultat de la vérification

Méthodologie du CI

- **Vérification du caractère adéquat**
  - **Rapport sommaire**
  - **Rapport d'observations (document de travail)**
- **Vérification de régularité**
  - **Rétroaction sur place (principales conclusions)**
  - **Rapport de conformité (observations, évaluation, recommandations)**
- **Suivi**

Défis

- **Aucune vérification sans consentement**
- **Expérience de l'équipe (vérification / technique)**
- **Approche relative au questionnaire – formuler les bonnes questions**
- **Disponibilité de l'information documentaire; par exemple, processus et descriptions de poste**
- **Établir un calendrier adéquat!**
- **« Profond et étroit » par opposition à « large et superficiel »**
- **Rapports et recommandations**
- **Équilibrer la charge de travail – points à examiner en petits groupes**

Avantages

CI

- **Occasion de cerner les problèmes systémiques et d'en tenir compte**
- **Fournit une solution de rechange aux mesures d'exécution**
- **Accroît la compréhension qu'acquiert le CI du traitement**
- **Précise le besoin d'orientation**
- **Fait mieux connaître la protection des données**

Organisations

- **Sensibilise davantage les personnes et les organisations à la protection des données**
- **Fournit une perspective sur le point de vue des autorités de réglementation**
- **Est un catalyseur du changement**
- **Assure une solution de rechange aux mesures d'exécution**

Protection de la vie privée – Le modèle américain

Joel Winston
Division de la protection de l'identité et de la vie privée
26 septembre 2007

Je vous présente la FTC

- La seule agence de protection du consommateur américaine exerçant une compétence générale
- Mission : promouvoir le fonctionnement efficace du marché par la protection des consommateurs contre les pratiques injustes et trompeuses

Cadre juridique américain en matière de protection de la vie privée

- Aucun droit général du respect de la vie privée ni obligation d'appliquer des pratiques particulières dans ce domaine
- Divers règlements et lois régissent des industries précises
  - l'industrie financière
  - l'industrie des soins de santé
  - l'industrie de l'information financière
- Les lois des États sur la sécurité des données et la notification des brèches
- La FTC Act – « pratiques injustes ou trompeuses »

Cadre juridique américain en matière de sécurité des données

- Aucune loi générale sur la sécurité ni obligation d'appliquer des pratiques particulières en matière de sécurité
- Divers règlements et lois régissent des industries précises
  - l'industrie financière
  - l'industrie des soins de santé
  - l'industrie de l'information financière
- Les lois des États
- La FTC Act – « pratiques injustes ou trompeuses »

La FTC Act

- Interdit « les pratiques ou actes trompeurs ou injustes dans le commerce ou influant sur ce dernier »
- « Pratique trompeuse » – pratique susceptible d'induire en erreur des consommateurs raisonnables de manière évidente
- « Pratique injuste » – qui porte atteinte ou qui est susceptible de porter atteinte à un consommateur, et que ce dernier ne peut raisonnablement éviter, et qui n'est pas compensée par des avantages offerts aux consommateurs ou à la concurrence

Mesures de protection

- Règle de protection – les exigences en matière de sécurité des données pour les institutions financières
- Doivent comprendre « des procédures raisonnables » pour protéger les renseignements personnels de nature délicate
- Normes souples et adaptables – la sécurité comme processus
- Pas d'exigences « techniques » particulières

Voir www.ftc.gov/infosecurity

Application par la FTC

- Enquêtes
- Mesures d'application de la loi
  - Cas de tromperie
  - Affaires liées à des mesures de protection
  - Affaires liées à la Fair Credit Reporting Act
  - Affaires liées à la Gramm-Leach-Bliley Act
  - Dossiers portant sur une injustice

Application par la FTC

- Exercer des recours – exigences en matière de vérification
- Redressements financiers – moyens de recours du consommateur, sanctions civiles

Autres efforts de la FTC

- Formation commerciale
- Éducation des consommateurs
- Établissement de règles
- Aide législative

Voir www.ftc.gov/privacy

Autres mesures gouvernementales d'application

- Les « agences bancaires » (OCC, FDIC, FRB, OTS, NCUA) – pouvoirs d'examen et d'application de la loi
- Application contrôlée par l'État

Principes généralement reconnus en matière de protection des renseignements personnels

Un cadre de référence mondial

Nicholas F. Cheung, CA, CIPP/C

L'Institut Canadien des Comptables Agréés

En quoi la protection des renseignements personnels (PRP) concerne-t-elle la profession comptable?

- La PRP relève de la gestion des risques
  - Les comptables sont des conseillers d'affaires de confiance
  - Ne peut être dissociée de l'évaluation du contrôle interne
- Les organisations ont besoin d'une certification indépendante quant à leurs pratiques de PRP
  - Les CA sont reconnus pour leur expertise en vérification
  - Toute vérification s'appuie sur des «critères appropriés»
- Expérience en normalisation
  - L'ICCA établit des normes de comptabilité et de certification pour les entreprises, les OSBL et le secteur public

Que sont les Principes généralement reconnus en matière de PRP (PPRP)?

- **Un cadre de référence pour aider toutes les entités, tant ouvertes que fermées, à concevoir leur programme de PRP et à évaluer les risques liés à la PRP**
- Mis au point par l'ICCA et l'AICPA
  - Pour établir une norme nord-américaine commune
  - Avalisés par :
    - l'ISACA – Information System and Audit Control Association
    - l'IIA – The Institute of Internal Auditors

Principes généralement reconnus en matière de PRP

- Gestion
- Avis
- Choix et consentement
- Collecte
- Utilisation et conservation
- Accès
- Communication à des tiers
- Sécurité
- Qualité
- Suivi et application

PPRP	Australie	Canada (LPRPDE)	Directive UE Protection des données	Norme mondiale
Gestion		Reddition de comptes	Avis	Reddition de comptes
Avis	Transparence	Fins, Transparence	Information à donner à la personne concernée	Fins, Transparence
Choix / con-sentement	Utilisation et communication	Consentement	Critères à satisfaire pour rendre légitime le traitement des données, Droit d'opposition de la personne concernée	Consentement
Collecte	Collecte, Renseignements sensibles, Anonymat	Limitation de la collecte	Principes relatifs à la qualité des données, Exemptions et restrictions	Collecte, Limitation
Utilisation et conser-vation	Identificateurs, Utilisation et communication	Limitation de l'utilisation, la communication et la conservation	Rendre légitime le traitement des données, Catégories spéciales de traitement, Principes relatifs à la qualité des données, Exemptions et restrictions, Droit d'opposition de la personne concernée	Limitation de l'utilisation, la communication et la conservation
Accès	Accès et rectification	Accès pour l'individu	Droit d'accès aux données pour la personne concernée	Accès
Communi-cation	Utilisation et communication, Flux transfrontières de données	Limitation de l'utilisation, la communication et la conservation	Transfert de données à caractère personnel vers un pays tiers	Limitation de l'utilisation, la communication et la conservation
Sécurité	Sécurité des données	Mesures de protection	Confidentialité et sécurité des traitements	Sécurité
Qualité	Qualité des données	Exactitude	Principes relatifs à la qualité des données	Exactitude
Suivi et application	(Application par l'Office of the Privacy Commissioner)	Contestation de la conformité	Recours judiciaires, responsabilité et sanctions, Codes de conduite, Autorité de contrôle et groupe de PRP en matière de traitement des données à caractère personnel	Conformité

Avantages des PPRP

- Exhaustifs
  - Plus de 60 critères mesurables et pertinents
    - Plus qu'une liste de principes
- Objectifs
  - Élaborés par la profession de vérificateur
    - pour répondre aux attentes sur le plan international
    - pour créer une base de comparaison
    - entièrement accessibles, sans frais
- Pertinents
  - Généralisés et reconnus
  - Applicables pour l'évaluation des risques liés à la PRP à l'échelle de l'entreprise
- Critères appropriés pour une vérification de la PRP
  - Peut aussi servir de base pour une évaluation interne

Exemple de critères PPRP

Sec.	Critères de sécurité	Exemples et explications relatifs aux critères	Autres considérations
8.2.3	**Contrôles d'accès physique** L'accès physique aux renseignements personnels, quelle qu'en soit la forme, est restreint.	Systèmes et procédures mis en place pour : • gérer l'accès logique et physique aux renseignements personnels (RP), y compris en ce qui concerne les supports papier, les copies d'archives et les copies de sauvegarde; • enregistrer et surveiller l'accès aux RP; • empêcher toute destruction non autorisée ou accidentelle ou perte de RP; • enquêter sur les intrusions et les tentatives d'obtenir un accès non autorisé; • communiquer les résultats des enquêtes au responsable de la PRP; • exercer un contrôle physique sur la diffusion de rapports contenant des RP;	Parmi les mesures de protection physique, on peut citer l'utilisation de : • classeurs verrouillés, • cartes d'accès, • clés physiques, • journal d'accès avec signature, • autres techniques, permettant de contrôler l'accès aux bureaux, aux centres de données ainsi qu'à d'autres lieux où des RP sont traités ou stockés.

Rapports externes sur la PRP

- Avantages d'un certificateur externe
  - Indépendant
  - Objectif
  - Rompu aux techniques de vérification
- Pourquoi est-ce important?
  - Renforcer la confiance des clients
  - Fournir des rapports utiles aux parties prenantes internes et externes
  - Respecter certaines clauses contractuelles

Mission d'application de procédés de vérification spécifiés

- Qu'est-ce que c'est?
  - Un type de mission où les procédés sont convenus entre le client et l'expert-comptable
  - Le comptable fournit une liste de tous les écarts qu'il a relevés
    - Il ne s'agit pas d'une opinion de vérificateur
  - La diffusion du rapport est restreinte
- Quelle en est l'utilité?
  - Il se peut qu'une organisation ne soit pas prête à une vérification, mais qu'elle souhaite présenter un rapport indépendant sur la PRP
    - Possibilité d'utiliser certains critères parmi les PPRP
  - Plus économique qu'une vérification

Vérification externe

- Qu'est-ce que c'est?
  - Semblable au rapport du vérificateur utilisé pour les états financiers (PPRP plutôt que PCGR)
  - Fournit une assurance raisonnable
  - Diffusion non restreinte du rapport
- Quelle en est l'utilité?
  - Fournir une assurance aux
    - clients et clients potentiels
    - employés / membres du conseil d'administration
    - instances réglementaires et gouvernementales
  - Obtenir une assurance à l'égard des pratiques d'un fournisseur externe en matière de PRP (exigence contractuelle liée à l'externalisation)

Autres utilisations des PPRP

- Évaluation des risques liés à la PRP
  - Diagnostic des programmes de PRP nouveaux ou existants
  - Ne peut servir à la conformité aux lois
- Étalonnage
  - Par rapport aux PPRP, ou comparaison des résultats avec ceux d'évaluations précédentes
  - Utilisables en contexte local, national ou international
- Élaboration d'avis sur la PRP

Pour en savoir plus

www.icca.ca/prp

Nicholas F. Cheung, CA, CIPP/C
Directeur de projets, Nouveaux services de certification
ICCA

416-204-3251
nicholas.cheung@cica.ca

CA Comptables agréés du Canada