



le Journal

de la 23^{ème} Conférence internationale des commissaires à la protection des données personnelles

Publication de la Commission Nationale de l'Informatique et des Libertés / France

Avril 2001 / n° 2

FOCUS

Le pouvoir de sanction de l'autorité espagnole de protection des données :

Un vrai contrôle a posteriori des fichiers et des amendes de 601€ à 601.000 €.

Page 2

ENJEUX

Est-il vraiment possible d'exercer un contrôle indépendant sur les fichiers de police ?

Schengen, Europol, l'expérience européenne.

Page 3

Qui lit vos e-mails ?

ACTUALITÉ La surveillance des e-mails et l'accès à Internet au travail sont des sujets brûlants au Royaume - Uni.



par Elizabeth France

Commissaire à l'Information - Royaume - Uni

EDITORIAL

de Michel Gentot

Président de la Commission Nationale de l'Informatique et des Libertés

Yahoo, Toysmart...

Le rappel à l'ordre prononcé par un juge français à l'égard d'un site d'enchères hébergé aux Etats-Unis qui mettait en vente des emblèmes nazis dont la diffusion est interdite en France et le refus américain qu'un fichier de clients d'une société en faillite puisse être considéré comme élément de patrimoine, et donc à ce titre commercialisable, ont deux points communs : internet et le juge.

Ces confrontations, qui ne sont inédites dans aucun de nos pays, ont eu cependant un retentissement mondial qu'un paradoxe, au moins apparent, n'a fait qu'exacerber. Alors, le 'droit national' d'un pays de libertés serait opposable au réseau de diffusion mondial ? Alors, la protection des données personnelles serait assurée - et avec quel éclat ! - aux Etats-Unis ? Ces questions demeurent ouvertes de part et d'autre de l'Atlantique.



Les récents entretiens que j'ai pu avoir, à l'occasion d'un séjour aux Etats-Unis, avec les autorités judiciaires de l'Etat de New-York m'ont convaincu de l'intérêt d'en débattre ensemble lors de la conférence de Paris, puisqu'il n'est plus une décision se rapportant à internet qui ne concerne tous les citoyens du monde.



“ Les nouveaux pouvoirs qui permettent aux employeurs d'espionner vos e-mails pourraient vous coûter votre emploi ” : telle est la manchette des journaux. Ces informations trompeuses sont à l'origine d'une incertitude générale quant aux limites des pouvoirs des employeurs.

La législation britannique a traditionnellement traité l'interception non autorisée des communications sur un réseau public comme une infraction criminelle mais n'évoquait pas leur interception sur les réseaux privés comme ceux de la plupart des lieux de travail. La Directive “ Protection des données personnelles et Télécommunication ” de l'UE et la Convention Européenne des Droits de l'Homme ont modifié la situation.

La Loi sur la Réglementation des Pouvoirs d'Investigation d'octobre 2000 rend illégale cette forme d'interception, sauf en cas de consentement ou si l'inter-

ception se fait dans le cadre d'une “ pratique commerciale légitime ”. De telles pratiques relèvent de réglementations distinctes, mais sont vastes et incluent à la fois la surveillance à des fins de respect des normes commerciales et de détection des usages non autorisés. La publication de ces réglementations est à l'origine de ces titres mensongers et a amené des employeurs à croire qu'il y avait peu de restrictions, s'il y en avait, à leur pouvoir de surveillance des e-mails et des accès à Internet.

La nouvelle loi ne fait que mettre en place, pour la première fois, une base légale claire à l'interception.

L'interception, qui implique l'obtention de données personnelles, le stockage et l'usage ultérieur de ces données, reste soumise à la loi générale sur la protection des données. Mais la surveillance n'implique pas nécessairement l'interception. Elle peut, par exemple, être fondée sur l'examen des messages e-mail qui ont déjà été

reçus, ouverts et ensuite stockés par le destinataire.

Le Code Pratique sur l'Usage des Données Personnelles dans les Relations employeur/ employé. Alors quel impact le RIP Act a-t-il sur la protection des données, la surveillance des e-mails et l'accès à Internet sur le lieu de travail ? C'est là qu'entre en jeu le Code Pratique que nous avons mis en consultation publique. Toute surveillance doit être une réaction de l'employeur proportionnée aux risques qu'il encourt.

En présentant un guide pratique sur ce qu'on entend par réaction proportionnée, l'avant-projet du Code propose des normes que les employeurs devraient suivre.

Les normes proposées par le Code

Fixer l'objectif spécifique pour lequel on doit engager une surveillance.

...suite page 2

Qui lit vos e-mails

...suite de la page 1

Calculer l'impact de la surveillance non seulement sur les libertés des employés, mais aussi sur d'autres personnes, comme les destinataires, les expéditeurs et celles mentionnées dans ces messages. Ne pas oublier que des messages professionnels peuvent aussi contenir des informations d'ordre privé.

Rechercher s'il est raisonnablement possible d'atteindre l'objectif de l'entreprise par d'autres méthodes moins indiscretes.

Ne pas engager de surveillance quand l'impact négatif est disproportionné par rapport aux avantages.

Cibler la surveillance sur des secteurs à risques spécifiques.

Limiter autant que possible la surveillance au débit plus qu'au contenu des messages.

Utiliser une surveillance automatisée pour réduire l'importance de la divulgation des informations.

Eviter d'ouvrir des messages qui sont de nature manifestement personnelle plus que professionnelle.

Informier tout le personnel soumis à cette surveillance de sa mise en place et de sa finalité.

Ne pas utiliser à d'autres fins des informations personnelles obtenues grâce à la surveillance sauf si un employeur ne pouvait pas raisonnablement les ignorer.

Notre avant-projet de Code statue sur de nombreux sujets en dehors de la surveillance, mais c'est celui qui a suscité de loin le plus d'intérêt. Plus de 100 réponses reçues après consultation sont à l'étude. Nombres d'entre elles sont hostiles à nos propositions sur la surveillance.

Nous tiendrons compte des opinions exprimées, organiserons d'autres discussions et publierons alors une version définitive du Code.

Le défi consiste à convertir cette proposition générale, que peu de personnes pourraient désapprouver, en des normes claires pour les employeurs. ■

INTERVIEW



Malcom Crompton - Australie



Commissaire Fédéral à la Protection de la Vie Privée depuis le 20 avril 1999 et responsable de l'application du Privacy Act de 1988.

Quel est l'objectif de la nouvelle loi sur la protection de la Vie Privée et les nouveaux droits qui entreront en vigueur le 21 décembre 2001 ?

La nouvelle loi du 6 décembre 2000, qui amende la loi sur la Protection de la Vie Privée de 1988, concerne les organismes du secteur privé. Ils doivent agir conformément aux Principes Nationaux de Protection de la Vie Privée qui sont eux-mêmes fondés sur les lignes directrices de l'OCDE.

Pour la première fois, cette loi permet aux particuliers de connaître les raisons pour lesquelles un organisme du secteur privé recueille leurs informations personnelles, quelles informations ils détiennent sur eux (et le droit de corriger les informations erronées), quel usage en sera fait, et qui d'autre pourra les obtenir. Les consommateurs peuvent porter plainte auprès du Commissaire à la Protection de la Vie Privée ou demander aux juridictions fédérales d'enjoindre aux organismes de rectifier leurs pratiques pour les rendre conformes aux Principes Nationaux de Protection de la Vie Privée

A qui vont s'appliquer les nouvelles dispositions concernant le secteur privé ?

La loi va s'appliquer aux organismes du secteur privé, y compris aux œuvres de bienfaisance, aux clubs sportifs et aux syndicats professionnels, dont le chiffre d'affaires est supérieur à 3 millions de dollars¹, aux sous-traitants du

gouvernement fédéral, aux prestataires de service dans le domaine de la santé et aux entreprises dont l'objet social consiste à faire commerce de données personnelles (quel que soit le chiffre d'affaires). La loi s'applique également facultativement aux petites entreprises qui choisissent de se soumettre à la nouvelle législation.

Qui n'est pas couvert par les nouvelles dispositions ?

Ne sont pas couverts par la loi les partis politiques, la plupart des petites entreprises dont le chiffre d'affaires annuel est inférieur à 3 millions de dollars, les données collectées dans le cadre de la gestion courante du personnel et les médias dans leur activité de journalisme.

Quelles sont les innovations prévues par la loi ?

La loi incite les entreprises à adopter leur propre code de déontologie qui doit être approuvé par le Commissaire à la Protection de la Vie Privée. Cette approbation ne pourra intervenir que si le code est au moins équivalent aux principes nationaux. Le code peut désigner un délégué indépendant à la protection des données, chargé d'instruire les plaintes. Si le code ne prévoit aucune disposition à cet égard, c'est le Commissaire à la Protection de la Vie Privée qui sera compétent, par défaut. Les organismes qui n'ont pas leur propre code devront se conformer aux principes établis par la loi. Nous travaillons très activement avec le secteur privé pour promouvoir des bonnes pratiques de protection de la vie privée et inciter à l'adoption de codes de déontologie. Je suis très impatient de partager vos expériences à Paris et vous invite à consulter mon site : www.privacy.gov.au.

¹ 3 millions de dollars australiens soit 1.737.918 euros.

Le pouvoir de sanction de l'agence espagnole de protection des données

FOCUS Un vrai contrôle a posteriori des fichiers : l'expérience de l'autorité espagnole.

Par Juan Manuel Fernández López,

Directeur de l'Agence de Protection des Données - Espagne



Des amendes de 601 € à 601.000 €

Le législateur espagnol a attribué à l'Agence de protection des données le pouvoir d'infliger des amendes allant de 601 € à 601.000 €, selon la gravité des infractions en cause, et celui d'ordonner la cessation de traitements de données et la destruction pure et simple de fichiers ne correspondant pas aux dispositions légales.

Ces pouvoirs doivent être exercés seulement en dernier recours.

Des inspections par secteur d'activité sont effectuées chaque année afin de sensibiliser les responsables des fichiers aux obligations qui leur incombent. A la suite de ces inspections, l'agence émet des recommandations ciblées et largement diffusées dans les secteurs concernés.

Une procédure de sanction

n'est ouverte que dans le cas où de graves infractions sont détectées.

En 2000, les secteurs visés ont été les fichiers de commerce électronique, les cartes de fidélisation des grandes surfaces et la téléphonie mobile. L'Agence a infligé un total d'amendes s'élevant à 11.293.000 €, les secteurs les plus sanctionnés étant l'internet, la téléphonie, la solvabilité patrimoniale, le crédit et la santé.



Mais la sanction n'est pas tout !

La loi espagnole est de mieux en mieux connue comme en témoigne l'accroissement considérable de toutes nos activités : déclarations de fichiers (enregistrement, modification et suppression) + 500%, nombre de saisines de particuliers + 40% et accès à notre site web (plus d'1 million) + 132%. ■

Un contrôle indépendant des fichiers de police : Schengen, Europol, l'expérience européenne

LE CHIFFRE DU JOUR

10 milliards d'euros

C'est le coût annuel mondial, pour les internautes, des messages non sollicités ou "junk-e-mails".

Source : Commission européenne.

ENJEUX Est-il vraiment possible d'exercer un contrôle indépendant sur les fichiers de police ?

C'est la question que se posent, dans chacun de nos pays, bien de nos concitoyens.



Alex Türk,

Sénateur, membre de la CNIL (Fr) et Président de l'autorité de contrôle commune Europol.

La coopération policière en Europe s'appuie principalement sur deux fichiers. Le système d'information Schengen concerne essentiellement les personnes recherchées et les étrangers ayant fait l'objet d'une mesure d'éloignement de "l'espace Schengen". Les fichiers d'Europol concernent, eux, la grande criminalité internationale (le trafic de stupéfiants, le terrorisme, etc.) et comportent, non seulement un index, mais aussi des fichiers d'analyse.

La reconnaissance d'un véritable socle juridique de garanties

La crainte qui s'est développée à la fin des années 80, lors des premières discussions relatives à la création de fichiers européens de police, était de voir ces fichiers échapper à chacune des lois nationales de protection des données des pays de l'Union européenne. Fort heureusement, les autorités nationales de protection des données ont su se faire entendre des gouvernements européens pour que les conventions ayant créé ces fichiers prévoient des dispositions en matière de protection des données personnelles.

Un droit d'accès qui doit s'exercer

S'agissant du système Schengen, le droit d'accès s'exerce selon les règles nationales applicables dans le pays où la demande est déposée.

En France, il s'exerce par l'intermédiaire de la CNIL. En 2000, la CNIL a reçu près de 400 demandes de droit d'accès qui ont abouti, dans 30 % des cas à la suppression de toute «fiche Schengen».

En revanche, pour le moment, très peu de demandes de droit d'accès aux fichiers Europol ont été exercées. Pourtant, la Convention Europol comporte une innovation majeure : la création d'un véritable comité des recours, instance indépendante chargée d'examiner les plaintes formées par les personnes qui ne sont pas satisfaites de la réponse - ou de l'absence de réponse ! - apportée à leur demande de droit d'accès.

Une autorité de contrôle indépendante

Dans les deux cas, une autorité de contrôle commune indépendante, exclusivement composée de représentants des autorités nationales de protection des données, est chargée de vérifier le fonctionnement des fichiers mis en place.

Ainsi l'autorité de contrôle commune Schengen a déjà effectué quatre contrôles du système central, installé à Strasbourg, qui l'ont conduit à prôner le renforcement des mesures de sécurité.

Inutile de rappeler ici le combat que mène en ce sens le président de l'autorité de contrôle commune Schengen, Bart DE SCHUTTER, alors que l'autorité ne dispose toujours pas d'un budget autonome.



L'autorité de contrôle commune Europol a des attributions encore plus étendues. Ainsi, elle assure le contrôle sur place du fonctionnement des fichiers (le premier a eu lieu en novembre 2000). Elle est également chargée de donner son avis sur toute création de fichiers. Enfin le comité des recours présidé par notre collègue Peter HUSTINX, a pour mission d'instruire les plaintes présentées par les particuliers insatisfaits des suites données à leur demande de droit d'accès.

Une indépendance à renforcer et des campagnes d'information à mener

Reste que l'indépendance ne s'acquiert pas en un jour.

Enfin, les autorités de contrôle communes s'emploient à mieux se faire connaître grâce à des campagnes d'information. L'autorité commune de Schengen a donné l'exemple en faisant diffuser aux frontières et dans les aéroports des plaquettes d'information sur les finalités du fichier et le droit d'accès.

Impératif d'ordre public et protection des données personnelles ne doivent pas être incompatibles : telle est la conviction européenne. ■

BRÈVES

ROYAUME UNI Freedom of Information Act 2000.

Depuis le 31 janvier 2001, Elizabeth France et ses services sont chargés de l'application, non seulement de la loi de protection des données de 1998 (Data Protection Act 1998), mais également de la loi sur la liberté de l'information de 2000 (Freedom of Information Act 2000).

HONG KONG - "Il y en a pour tous" à Hong Kong pendant la Semaine sur la vie privée du 26 mars au 1^{er} avril 2001.

Notre dynamique collègue Stephen Lau, Commissaire pour la vie privée et les données personnelles de Hong Kong (PCO-Privacy Commissioner's Office) a organisé une semaine sur la vie privée du 26 mars au 1^{er} avril 2001, à l'occasion de Forum Asian Data Privacy : une conférence "e- vie privée dans la nouvelle économie", une " nuit de la vie privée ", à la télévision, un concours pour les étudiants du meilleur site favorisant la compréhension par les jeunes de la protection des données et de la vie privée, deux séminaires sur le nouveau code de bonne pratique du PCO sur la gestion des ressources humaines et, enfin, une caravane traversant Hong Kong les 28, 31 mars et 1^{er} avril. Quel talent !

ÉTATS UNIS -

Décisions judiciaires - **Quel contenu pour la future loi fédérale.** Début mars, le Comité de l'Assemblée des Représentants pour l'Énergie et le Commerce a procédé à des auditions sur les questions de protection de la vie privée. M. Stefano Rodotà, président du groupe des commissaires européens à la protection des données institué par la directive 95/46/CE, a été entendu le 8 mars 2001.

Eliot Spitzer, procureur de l'Etat de New York qui, avec 43 autres Etats et la Federal Trade Commission, s'était opposé à l'intention de la société de vente en ligne de jouets Toysmart, en faillite, de vendre son fichier de clients, a rendu public le 11 janvier 2001 l'accord finalement retenu par la Cour des Faillites de Boston. Cet accord prévoit que Disney donnera à sa filiale Toysmart 50.000 US\$ pour détruire

son fichier. L'intention de vendre des données n'ayant pas été notifiée aux personnes lors de la collecte, cette vente aurait constitué un délit de pratique déloyale et l'absence d'accord parental pour les enfants concernés un délit au terme de la loi de 1998 sur la "protection en ligne de la vie privée des enfants".

Selon le Financial Times du 27 février 2001, 300 propositions de loi dans les Etats et au moins une douzaine au niveau fédéral ont été générées par la nécessité de protéger les données personnelles.

ERRATUM

Deux erreurs dans le N° 1 : notre collègue le Dr Ewa KULESZA est spécialiste de droit de travail et de sciences sociales et l'orthographe exact du nom de notre collègue néo-zélandais est Bruce H. SLANE. Avec toutes nos excuses.

Le "Groupe de Berlin"

TRAVAUX DE GROUPE Un Groupe de Travail International sur la Protection des Données Personnelles dans les Télécommunications

Hansjürgen Gartska,

Commission d'accès à l'information et à la protection des données du Land de Berlin. - Allemagne



Le contexte

En 1983, le précédent commissaire à la protection des données du Land de Berlin-Allemagne, Joachim KERKAU, invita toutes les autorités de protection des données existantes à rejoindre à Berlin le Salon International des Techniques Audio et Vidéo, où étaient présentés les derniers produits de l'industrie des télécommunications, en particulier le videotex et la télévision par câble. Les commissaires, invités à participer à un atelier, préparèrent une résolution relative aux problèmes de protection des données sur ces matières. Ce texte fut adopté par la Conférence Internationale des Commissaires à la protection des Données de Stockholm le 18 octobre 1983. La Conférence avait alors déjà établi que "la collecte automatique de données personnelles permet de dresser les profils individuels de tous les utilisateurs. Les caractéristiques sociales et comportementales des utilisateurs devront pour cette raison faire l'objet de mesures particulières".

Le groupe se baptisa rapidement le "Groupe de Travail International sur les Télécommunications et les Médias". Durant la 11ème Conférence Internationale de Berlin, en août 1989, il fut décidé, sur proposition de la délégation française, d'étendre les activités du Groupe. Depuis lors, il se réunit deux fois par an, la réunion de printemps devant se tenir dans d'autres pays, y compris les USA, la Russie, Hong Kong ou l'Inde. En raison de la nature informelle du Groupe, la Conférence Internationale décida en 1993, à Manchester, de ne plus adopter les résolu-

tions soumises par lui, mais des comptes rendus de ses travaux sont présentés à chaque Conférence depuis cette date.

Les rapports du Groupe de Travail

Luxembourg, 1985 - Impact du développement des nouveaux médias électroniques, des réseaux cablés et de la numérisation des services de télécommunications sur la vie privée des utilisateurs.

Sydney, 1992 - Localisation et gestion de flotte. Problèmes relatifs aux secrets de télécommunications et des communications par satellites tant en matière de localisation que de gestion de flotte.

Budapest, 1996 - "Protection de la vie privée sur Internet", Memorandum qui traite de l'insuffisance du niveau de protection des données et des mesures destinées à son amélioration.

Hong Kong, 1998 - Moteurs de recherche sur Internet. La capacité des moteurs de recherche sur Internet à profiler l'activité des individus est discutée. Le Groupe présente des recommandations pour des pratiques plus respectueuses de la vie privée. Responsabilité publique sur l'interception des communications privées. L'accent est mis sur les mécanismes destinés à rassurer le public quant à l'utilisation licite, appropriée et proportionnée des pouvoirs d'interception.

Norvège, 1999 - Risques pour la vie privée de l'utilisation des agents intelligents. Le Groupe demande aux concepteurs d'incorporer à ces systèmes des mesures destinées à protéger la vie privée, par

exemple les PET (Technologies de renforcement de la protection de la vie privée)

Crète, 2000 - Traitement des données personnelles pour la détection des fraudes en télécommunication. Le Groupe a abordé diverses méthodes de détection et de prévention des fraudes au regard de leur impact sur la vie privée.

Gestion du copyright et protection de la vie privée. Recommandations relatives à la conception et à la mise en œuvre des systèmes de management du copyright électronique (ECMS) afin de respecter à la fois les détenteurs de droits et la vie privée des utilisateurs.

Berlin, 2000 - Projet de Convention "Cyber-crime" du Conseil de l'Europe. En particulier, le Groupe refuse explicitement la proposition du projet de convention qui consiste à obliger les opérateurs de télécommunication et les fournisseurs de services internet à stocker les données des trafics télécom et internet pendant une longue période, afin de les rendre disponibles pour l'autorité judiciaire.

Bangalore, février 2001 - Localisation des mobiles : principes de développement et de mise en œuvre des services basés sur la localisation des informations, respectueux de la vie privée.

Projets futurs

La 30^{ème} réunion sera organisée à Berlin, à l'occasion du Salon International des Techniques Audio et Vidéo qui s'y tiendra les 27 et 28 août prochains sous le titre "La vie privée et le droit de la propriété intellectuelle sur Internet". ■

Pour plus d'information : www.datenschutz-berlin.de

Conférence de Paris :

Quand ?

23 au 26 septembre 2001

Comment ?

Vous pouvez dès à présent vous inscrire en complétant le bulletin ci-joint ou bien sur le site paris-conference-2001.org

Attention, il est très difficile d'obtenir une chambre d'hôtel à Paris en septembre, réservez dès maintenant.

le Journal

Le Journal est une publication de la Commission Nationale de l'Informatique et des Libertés - France. Directeur de la publication, Michel GENTOT
Création — *Lebrun* —

Vos réactions et contributions :
Michel GENTOT
mgentot@cnil.fr
Thierry JARLET
tjarlet@cnil.fr
Marie GEORGES
mgeorges@cnil.fr