



Commission Consultative des Droits de l'Homme

**Avis sur le rapport annuel 2007 de la Commission
nationale pour la protection des données**

Avis 04/2008

Avis de la Commission Consultative des Droits de l'Homme (CCDH) sur le rapport annuel 2007 de la Commission Nationale pour la Protection des Données (CNPD)

Le gouvernement luxembourgeois a saisi la Commission Consultative des Droits de l'Homme par voie d'un courrier émanant du ministre des Communications, M. Jean-Louis Schiltz, de rendre son avis sur le rapport d'activité de la Commission nationale pour la protection des données (CNPD) à l'année 2007.

Conformément à l'art. 32 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, la CCDH est censée aviser le rapport annuel de la Commission nationale de protection des données mise en place en 2002.

Le rapport de la CNPD constate que l'année 2007 a constitué « à plus d'un titre une année charnière sur son jeune parcours. »

La CNPD a eu à prendre position sur un certain nombre de dossiers importants, dont

- les systèmes d'alertes professionnels « Whistleblowing »,
- l'interconnexion de divers fichiers publics,
- la collecte de données pour l'établissement des cadastres des loyers par les Communes)

Sur le plan européen, elle a participé au travail sur des dossiers sensibles comme

- les dossiers électroniques de santé,
- les mineurs et la protection des données,
- la décision-cadre européenne sur la protection des données dans les domaines du 3e pilier,
- la transmission de données des passagers aériens vers des pays tiers

Parmi les dossiers techniques figuraient

- le e-ticketing,
- l'identification par radiofréquence (RFID),
- les moteurs de recherche Internet,
- les règles contraignantes d'entreprises (BCR).

Les autres axes d'activité de la CNPD ont été

- l'information du public souvent insuffisamment sensibilisé aux risques et peu au fait des droits que la loi accorde aux personnes concernées
- une guidance des entreprises, administrations et autres professionnels
- la coopération avec un nombre croissant de ministères et d'organismes publics qui l'ont consultée avant d'opérer leurs choix finaux sur des questions susceptibles d'impacter de façon substantielle l'envergure et la mise en œuvre de la collecte et de l'utilisation de données à caractère personnel engendrées par de nouveaux développements opérationnels et législatifs.

La CCDH constate avec satisfaction que toutes les activités de la CNPD ont été guidées par le souci de la protection des données à caractère personnel en accord avec les principes de protection de la vie privée et du principe de proportionnalité en accord avec l'article 8 de la

Convention européenne des droits de l'homme. Ces activités ont mis en exergue à quel point les droits des personnes à la protection des données les concernant peuvent être mis en péril par des démarches de collecte de données qui a priori sont d'une apparente innocuité.

Ainsi, vu le **recours accru aux données biométriques** dans le cadre des traitements de données à des fins de surveillance sur le lieu de travail, la CNPD déclare s'efforcer « de limiter, respectivement d'encadrer sérieusement la prolifération de bases de données biométriques et les accès et échanges de données entre les administrations publiques poursuivant des missions distinctes. » (p. 20) Et elle ajoute : « De façon générale, la Commission nationale n'est pas convaincue de la nécessité de voir se répandre trop rapidement les systèmes d'identification/ d'authentification des personnes par leurs caractéristiques biométriques ; à plusieurs égards la fiabilité et la sécurité de tels systèmes ne sont pas totalement garanties. » Et elle conclut : « Une saine prudence apparaît donc être toujours de mise avant une généralisation précipitée du recours à ces technologies. » La CCDH suit la CNPD dans cette appréciation.

L'échange et le partage de données entre administrations publiques est un autre enjeu.

Au cours de l'année 2007, la CNPD a émis cinq avis à ce sujet. A chaque fois, il s'agissait d'arbitrer entre les critères de nécessité et de proportionnalité. Pour la CNPD, cet exercice « revêt généralement un caractère très délicat », car constate-t-elle, « l'intérêt public (besoin de connaître tous les renseignements pertinents et exacts) et la simplification administrative (amélioration de la rapidité et de l'efficacité des procédures avec allègement des démarches demandées aux citoyens et aux entreprises) plaident fortement contre les impératifs de limitation inhérents à la protection des données. »

Conclusion de la CNPD : « L'expérience des dossiers examinés et en cours laisse la Commission nationale avec des sentiments mitigés. » Elle se réjouit d'être de plus en plus souvent consultée et impliquée dès les travaux préparatoires, mais elle évoque aussi les difficultés qu'elle ressent « à véhiculer le message d'autolimitation » face à cette « voie de la facilité consistant à rendre accessibles tous azimuts l'ensemble des renseignements le cas échéant disponibles dans d'autres parties de l'administration étatique ou para-étatique. »

Il lui faut donc être créative et « suggérer des solutions pragmatiques adaptées aux situations concrètes. » Dans la protection des données, la CNPD met donc en avant que « les solutions techniques et mesures de sécurité revêtent souvent une importance cruciale. »

La CCDH constate que l'échange et le partage de données entre administrations publiques peut devenir un facteur de grande pression sur les libertés des citoyens. Elle souligne le rôle important d'une CNPD indépendante dans ce contexte qui signale pourtant qu'elle a, malgré le fait d'être souvent consultée et impliquée, des difficultés à faire passer son message. Autre élément dont le suivi du respect des droits fondamentaux dans le domaine de la protection des données doit tenir compte : le haut degré de technicité des façons de les protéger tout en tenant compte des intérêts légitimes des acteurs publics et privés du traitement des données.

En ce qui concerne **la géolocalisation**, la CNPD constate que « parmi les technologies nouvelles qui connaissent un essor fulgurant et dont il faudra suivre attentivement les effets à long terme », figurent les étiquettes de radio-identification d'objets « RFID » comprenant des puces à lecture sans contact et le traçage des déplacements, notamment par la géolocalisation ou la reconnaissance automatisée des immatriculations des voitures, qui menacent d'exposer progressivement les citoyens à une surveillance de plus en plus poussée. »

Ici, la mise en garde de la CNPD est on ne peut plus claire : « La liberté des citoyens de se déplacer librement et anonymement sans être surveillés dans tous leurs mouvements va au-devant de plus en plus de restrictions. »

Ce qui précède conduit la CCDH à lancer un appel aux autorités compétentes pour qu'elles tiennent compte de cette évolution et n'adoptent pas de mesures qui restreignent dans ce domaine la liberté des citoyens.

Le nombre de demandes d'autorisation pour des traitements à des fins de surveillance au moyen de la géolocalisation est lui aussi en augmentation et s'inscrit pour la CNPD dans la même logique. D'un côté, la CNPD pense que ce type de demandes peut être légitime dans la mesure où il s'agit d'assurer un suivi de sa flotte de véhicules par l'employeur/l'entreprise, mais de l'autre côté, « la géolocalisation par l'employeur des véhicules utilisés par les salariés peut être ressentie par ces derniers comme très intrusive ». Sa nécessité devrait donc être justifiée, comme c'est actuellement la pratique en France, si ces données apparaissaient nécessaires pour assurer une meilleure allocation des moyens pour des prestations à accomplir en des lieux dispersés : le suivi et la facturation d'une prestation, le suivi de temps de travail, lorsque ce suivi ne peut être réalisé par d'autres moyens. Mais il se trouve qu'actuellement, la CNPD ne peut « fonder ses autorisations que sur les besoins de sécurité et santé des travailleurs et de protection des biens de l'entreprise, ainsi que le suivi du temps de travail dans certains cas. »

La CNPD a également analysé un autre dossier d'une apparente innocuité, le **projet e-go** du Ministère des Transports, en se basant sur l'expertise développée par le « groupe de Berlin » auxquels participe l'un de ses membres. Ce groupe a récemment adopté un papier d'orientation relatif aux enjeux et aux précautions qu'il faut prendre dans le domaine de l'« e-ticketing ». L'intervention de la CNPD a permis que dans un premier temps, les données contenues dans les cartes e-go - des données à caractère personnel relatives aux déplacements des personnes titulaires d'un abonnement prépayé ou d'une carte de privilèges ainsi que date, heure et lieu de la validation du titre de transport - ne seront pas dans un premier stade relevées sur base nominative « de sorte qu'il reste du temps pour résoudre les problèmes étudiés. »

La CCDH tient à souligner que le traitement du dossier e-go par la CNPD montre que la vigilance est nécessaire dans toutes les collectes de données qui permettent de retracer les déplacements a priori libres et anonymes des personnes.

Tout en déclarant que « la protection des données ne reconnaît pas seulement dans le développement technologique son effet de multiplication des risques » mais qu'elle « reconnaît aussi son aspect positif et son potentiel à constituer des remèdes et sauvegardes », la CNPD met en garde contre « **la multiplication des intrusions externes sous forme de notification spontanée par les logiciels (fonction « calling home ») et du traçage de l'utilisation des terminaux IT et de communication électronique qui s'opèrent de plus en plus souvent à l'insu de l'utilisateur (on parle d'« ubiquitous computing»)** ». La CCDH fait sienne cette mise en garde de la CNPD.

L'affaire « SWIFT », qui a été déclenchée par des révélations de la presse américaine en juin 2006 sur le fait que la CIA et le département du Trésor américain avaient surveillé pendant des années des millions de données transitant par le réseau de la société SWIFT, a causé un

vif émoi dans l'opinion publique. La CNPD note : « Les institutions européennes avaient conclu à la probable irrégularité de la surveillance du réseau par les autorités américaines au regard des règles européennes de protection des données personnelles. »

Les discussions entre la Commission européenne et les autorités américaines ont abouti en juin 2007 à un échange de courrier relatif au respect de la protection des données, et le ministère des Finances des Etats-Unis (« United States Treasury Department ») a pris certains engagements, comme quoi les données ne seront utilisées qu'à des fins de contre-terrorisme, que le ministère identifiera et supprimera endéans les 5 ans de leur réception toute donnée qui n'est pas nécessaire pour des investigations en matière de contre-terrorisme, qu'un superviseur chargé par l'UE aura le droit de contrôler annuellement si le ministère américain tient ses engagements et que ces engagements seront publiés dans le journal officiel de l'UE et dans le registre fédéral des Etats-Unis.

La société SWIFT a été conduite à prendre différentes mesures afin de se conformer aux prescriptions européennes relatives à la protection des données, mais elle a aussi adhéré aux accords « Safe Harbor » - un code de conduite relatif à la protection des données à respecter par les sociétés américaines qui s'y soumettent volontairement.

Du côté luxembourgeois, la CNPD a été, depuis l'affaire SWIFT, « en contact régulier avec l'Association des Banques et Banquiers (ABBL) et l'ALMUS, l'Association des utilisateurs SWIFT au Luxembourg, avec notamment une entrevue d'ordre général en octobre 2006 à laquelle participaient en outre l'ABBL, l'ALMUS et une représentante de la direction générale de SWIFT. » Elle a invité en 2007 les banques et autres établissements financiers luxembourgeois à améliorer l'information fournie à leurs clients et à les avertir en toute transparence de l'accès des autorités américaines à certaines données relatives aux transactions financières mondiales, donc également européennes. Cette recommandation fut suivie par l'ensemble des établissements de la place grâce à la collaboration active de l'ABBL et de l'ALMUS.

La CCDH constate que cette transparence n'empêche pas que les autorités américaines continuent à avoir un accès à des données sensibles – une démarche auparavant qualifiée d'« irrégulière » – et que le fond du problème n'est pas réglé, dans la mesure qu'un superviseur de l'Union européenne ne peut raisonnablement être en mesure de contrôler les engagements états-uniens. Mais cela dépasse évidemment de loin les possibilités d'intervention de la CNPD luxembourgeoise qui n'a pu que suivre l'évolution du dossier.

Dans le contexte révélé par l'affaire « SWIFT », **l'autorisation de flux de données vers des pays tiers ne disposant pas d'un niveau de protection adéquat** n'est pas une chose neutre.

En principe, les données à caractère personnel peuvent uniquement être transférées dans les pays de l'UE et dans les pays présentant un niveau de protection adéquat (article 18 de la loi modifiée du 2 août 2002). Cette même loi prévoit dans son article 19 diverses dérogations à cette interdiction.

Lorsqu'aucune de ces dérogations ne s'applique, l'autorisation préalable de la CNPD doit être sollicitée pour le transfert. Le responsable du traitement doit offrir des garanties suffisantes au regard de l'utilisation qui sera faite des données personnelles exportées par le destinataire établi dans un Etat tiers dont la législation n'assure pas une protection adéquate ainsi que relativement à l'exercice des droits correspondants des personnes concernées.

Au Luxembourg, un nombre croissant de sociétés internationales qui sont des leaders dans le domaine du commerce électronique, se sont récemment implantées. La CNPD est donc intervenue en 2007 à plusieurs reprises pour analyser des demandes d'autorisation.

En 2007, la CNPD a donné deux autorisations à des entreprises disposant de « binding corporate rules » et une dizaine d'autorisations à des entreprises disposant de clauses contractuelles appropriées avec les entreprises susceptibles de recevoir les données personnelles.

Elle dit dans son rapport qu'il s'agit à chaque fois de dossiers demandant « une analyse approfondie, (..) pondérée et prudente » de sa part, qui tient compte « aussi bien de la sensibilité des dossiers, de l'importance des acteurs que du nombre des personnes concernées. »

La CCDH mesure les enjeux économiques et légaux d'une telle autorisation et relève que la CNPD ne fait état d'aucune pression exercée sur elle. La CCDH espère que l'indépendance, l'autorité et les arbitrages de la CNPD continueront à être ainsi respectés par les secteurs dans laquelle elle intervient, et ce quelque soient les intérêts en jeu.

L'identifiant unique (N° de matricule national) pose également problème pour la CNPD. Depuis juin 2006, un groupe interministériel a été chargé d'élaborer un projet de loi dans le but de réformer la loi du 30 mars 1979 ayant introduit le répertoire général des personnes et le numéro d'identification national à l'usage de l'administration publique luxembourgeoise. Ce groupe de travail collabore étroitement avec la CNPD.

La CNPD écrit : « Au cours de deux réunions, la Commission nationale a exprimé ses préoccupations sur le fait que la loi de 1979 n'est plus appliquée de manière rigoureuse, et que le recours au numéro national est de plus en plus incontrôlé. Elle a demandé que les orientations pour l'introduction d'un nouvel identifiant national, davantage sécurisé que le matricule actuel qui fait ressortir la date de naissance et le sexe des personnes, soient arrêtées le plus rapidement possible. » Le problème central du dossier est pour la CNPD « d'éviter que l'identifiant national puisse rendre possible des interconnexions ou accès illicites de données ou de fichiers. »

La CCDH soutient la CNPD dans sa démarche qui consiste à créer un matricule qui permette d'éviter des interconnexions et des accès illicites à des données et fichiers sensibles pour les droits des personnes.

La CNPD s'est fixée un certain nombre **de priorités** qui s'inscrivent dans la logique du travail déjà effectué et des objectifs atteints à ce jour :

1. information du public, sensibilisation et explication des règles légales,
2. guidance à fournir aux entreprises, organismes et administrations publics et promotion des bonnes pratiques
3. simplification et accélération du traitement des formalités administratives avec focalisation sur les traitements et situations comportant des risques notables
4. coopération avec les autorités et les professionnels dans la recherche des solutions praticables et publication de recommandations thématiques et sectorielles

5. contrôles ponctuels concentrés sur des cas graves et des investigations menées spontanément à titre préventif pour des fichiers importants et sensibles où la confiance du public dans certaines institutions exige que le respect de la loi soit parfaitement assuré.

Elle déclare, à l'issue des cinq premières années de son existence, avoir « atteint son rythme de croisière ». Elle est satisfaite du renforcement du nombre de ses collaborateurs permanents, pour lequel elle avait reçu le soutien de la CCDH. Autre facteurs de succès : « l'expérience acquise par ses membres et les simplifications intervenues au niveau des formalités administratives prévues par la loi » Ce qui lui permet de dire que « pour l'essentiel, les étapes qu'elle s'était fixées dans la feuille de route tracée dans son rapport d'activités relatif à l'année 2003 ont été franchies ou au moins abordées », des orientations stratégiques que la CCDH avait lors de son avis émis le 7 mars 2005 approuvées avec force.

La CNPD se dit « consciente de l'importance de son rôle dans la préservation des libertés et droits fondamentaux des citoyens, notamment de la protection de la vie privée tout en ne voulant pas pour autant freiner le développement technologique, la compétitivité des entreprises (en particulier de celles qui emploient des collaborateurs au Luxembourg) et la modernisation de l'administration publique. » La CCDH ne peut que la suivre dans cette appréciation d'elle-même qu'elle estime juste et justifiée.

Conclusion :

La CCDH :

- constate le caractère exhaustif du rapport d'activités 2007 de la CNPD
- approuve les orientations stratégiques générales de la CNPD
- félicite la CNPD pour la rigueur et la créativité dont elle met en pratique son souci de la protection des libertés et droits fondamentaux des personnes, notamment de leur vie privée
- appelle les autorités et les professionnels actifs dans le secteur du traitement des données à continuer de respecter l'autorité et l'indépendance de la CNPD qui est devenue en six ans un pilier essentiel de l'architecture de la protection des droits fondamentaux des citoyens au Luxembourg

Octobre 2008