Commission Nationale pour la Protection des Données

COMMISSION NATIONALE
POUR LA PROTECTION
DES DONNÉES

Conférence de Presse

Rapport d'activité 2008

Présentation version longue

Luxembourg, le 17 juin 2009

Décembre 2002-2008 : 6 années d'existence et d'activités de la Commission nationale pour la protection des données

- 1er décembre 2002: une nouvelle autorité de surveillance indépendante
- Règles légales à faire connaître : Rôle à faire reconnaître par les acteurs
- Au début, focalisation excessive sur les formalités de déclaration des traitements de données dans la perception du public et dans son organisation
- Phase dépassée après la simplification de la législation (loi du 27 juillet 2007) apportant un certain nombre de clarifications et un allègement des formalités
- 2008: La Commission nationale a vu enfin ses effectifs de personnel renforcés (aujourd'hui : 3 membres, 3 juristes, 4 collaborateurs administratifs et 1 attaché à la communication et à la documentation) et a optimisé son fonctionnement
- La Commission nationale déploie désormais des efforts accrus de guidance des entreprises/ administrations, de prise en charge des plaintes et demandes des citoyens et elle mène des contrôles et des investigations sur le terrain
- Elle est de plus en plus consultée préalablement et ses recommandations sont mieux prises en compte; elle a acquis une expertise qu'elle sait mieux communiquer (renseignements quant à la conformité de traitements, avis, recommandations)
- Elle continue ses actions de sensibilisation et d'information du public, en particulier auprès des jeunes. (Séances d'information, conférences, exposés)

Les activités de la Commission nationale en 2008 (1)

Supervision de l'application de la loi: moins de formalités administratives

- Aujourd'hui, la Commission nationale a trouvé un meilleur équilibre entre ses différentes tâches et attributions qui sont :
  - Le travail administratif et la tenue du registre public
  - La sensibilisation du public et la veille de l'évolution technologique
  - La guidance des acteurs privés et publics et la promotion des bonnes pratiques
  - Le traitement des plaintes, les contrôles et investigations sur le terrain
  - Les avis et prises de position sur des dossiers concrets
- Nombre de dossiers traités au total:14.000 déclarations émanant de de 4.357 responsables de fichiers

Nombre moyen annuel	2003-2008	2008	Σ 2003 - 2008
Traitements de données notifiées	1.760	**1.327**	**10.130**
Engagements formels de conformité	184	**220**	1.139
Demandes d'autorisations préalables	435	**606**	**2.781**
Plaintes et vérifications de licéité, investigations	32	**63**	220

Les activités de la Commission nationale en 2008 (2)

Supervision de l'application de la loi: davantage de contrôles & d'examens de cas

- Engorgement en voie d'être résorbé: 450 demandes d'autorisation/ Vidéosurveillance l'an
- Autorisation en cas de transferts de données vers des pays tiers
  - 34 entreprises voulant transférer des données vers des pays sans protection adéquate
  - Analyse de 3 chartes de règles contraignantes d'entreprises nouvellement soumises par les autorités de protection des données des Etats membres où elles sont établies.
  - Examen approfondi d'un dossier d'un groupe multinational d'entreprises de commerce et services offerts sur Internet : la Commission Nationale s'est vue reconnaître le rôle de chef de file dans la procédure d'approbation des BCRs en coordination avec les autorités de protection des données de 15 autres pays européens où il est également établi
- Plaintes et investigations
  - Nette augmentation du nombre de plaintes et demandes de vérification de licéité : 63 en 2008.
  - Différentes actions d'investigation: p.ex. traitements de données d'envergure ou particulièrement sensibles (en 2005/2006 au Centre Commun de la Sécurité Sociale et dans l'Assurance Maladie)
  - Etude similaire en 2008/2009 dans le secteur des communications électroniques avec vérification de la conformité des traitements de données du département "Télécommunications" de l'entreprise des P&T et des opérateurs privés, notamment de téléphonie mobile.
  - Vérifications sur place d'installation de dispositifs vidéosurveillance ou de leur suppression.

Les activités de la Commission nationale en 2008 (3)

Conseil et guidance : soutenir une culture de la protection des données

- Chargés de la protection des données : une fonction à promouvoir
- Concertation avec les organisations représentatives sectorielles, les principaux acteurs économiques, l'Etat et les organismes publics
  - Poursuite de la politique de dialogue constructif avec les acteurs publics et privés
  - De nombreuses réunions avec les autorités, organismes et administrations publics (52 en 2008) et les entreprises et organisations représentatives du secteur privé (44 en 2008)
  - Ministères (Affaires étrangères, Santé, Education, Finances, Transport, Fonction publique,…) CTIE, BCL, Communes, CRP-Santé, CEPS, Biobanque, ALAD, entreprises
  - Participation régulière aux travaux du Comité National d'Ethique de Recherche (CNER) et du Comité National pour la Simplification Administrative en faveur des Entreprises
    Séances d'information, conférences, exposés
  - 11 séances d'information, de conférences et d'exposés en 2008 (14 en 2007)
  - Séminaire EPON (CPO de 17 multinationales) à Luxembourg (les 20 et 21 mai 2008)
- Réponse aux demandes de renseignements
  - Nombre de demandes de renseignements toujours à un niveau élevé : 1.724 en 2008, la plupart par téléphone ou courriel (citoyens, responsables d'entreprises, avocats, chargés)

Les activités de la Commission nationale en 2008 (4)

Avis & recommandations : analyser les risques et promouvoir les bonnes pratiques

7 avis émis en 2008 sur des projets de loi ou des dispositions réglementaires:

- Avis sur le projet de loi n° 5802 portant sur la libre circulation des personnes et l'immigration et avis du 18 juillet 2008 sur le projet de règlement grand-ducal autorisant et réglant certains traitements de données dans le cadre de l'exécution des dispositions de la loi du 29 août 2008
- Avis concernant le projet de règlement grand-ducal relatif à la fixation des conditions et modalités de délivrance de la documentation cadastrale ;
- Avis sur un avant-projet de loi modifiant la loi modifiée du 29 avril 1983 concernant l'exercice des professions de médicales et
- Avis sur un avant-projet de règlement grand-ducal déterminant les procédés à suivre pour constater la mort en vue d'un prélèvement
- Consultation directe par la Chambre des Députés à l'initiative de la commission parlementaire saisie d'une modification de la loi électorale;
- Avis émis sur demande de l'Institut Luxembourgeois de Régulation et de la V.d. Luxemb.
- Avis sur demande sur l'enregistrement d'appels téléphoniques d'urgence en vertu de l'article 4 § 3 de la loi du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques

Les activités de la Commission nationale en 2008 (5)

Information du public : stimuler la vigilance et la responsabilité des citoyens

- Actions de sensibilisation du public
  - 2e 'Journée européenne de la protection des données', 28 janvier 2008: campagne de communication
  - Exposés et ateliers dans les lycées et écoles
  - Participation avec un stand d'information aux journée organisées (8 & 9 octobre 2008) par LuSI – Luxembourg Safer Internet, LISA
- Site Internet (www.cnpd.lu)
  - Moyen d'information important pour la Commission nationale : choix d'utiliser cet outil pour informer de manière permanente et continue sur ses activités et les évolutions en la matière
  - 60% des notifications ont été remplies en ligne par le biais du formulaire électronique
  - Au total 224.833 visites en 2008, en moyenne de 614 visites par jour (sur 365 jours)
- Formation, exposés & conférences publiques
  - Université de Luxembourg, INAP, Clussil, 'Luxembourg Internet Society'.
  - Présentations de la loi modifiée : Collège médical, Chambre des Métiers, FNCTTFEL
  - Intervention dans le cadre de la formation 'Management de la Sécurité des Systèmes d'Information' (MSSI) à l'Université de Luxembourg
  - Explications et interviews donnés à la presse sur des sujets d'actualité

Les activités en de la Commission nationale 2008 (6)

Participation aux travaux européens: contribuer et développer notre expertise

- Participation à différents groupes de travail au niveau européen
  - Groupe « Article 29 » sur la protection des données (établi en vertu de l'article 29 de la directive 95/46/CE) qui regroupe toutes les CNPD européennes
  - Sous-groupe 'Flux internationaux de données', données de santé, secteur financier;
  - Sous-groupe 'Technologies'
  - 'Groupe de Berlin', dédié à la protection des données privées dans le secteur des communications électronique
  - Séminaire européen biannuel d'échanges d'expériences dans le traitement des cas pratiques ('Case Handling Workshop')
  - Comité consultatif de la Convention 108 du Conseil de l'Europe (T-PD)
  - Conférence annuelle des Commissaires à la protection des données
- Documents d'orientation élaborés:
  - Protection de la vie privée des enfants et des adolescents (WP 147)
  - Avis sur les aspects de la protection des données liés aux moteurs de recherche (WP 148)
  - International Working Group on Data Protection in Telecommunications: Report & Guidance on Privacy in Virtual Social Network Services
  - Avis sur le projet de norme internationale de protection de la vie privée du code mondial antidopage (WP 156)
  - Conseil de l'Europe (T-PD) : Rapport sur le profilage à travers l'internet et les terminaux bavards

Temps forts et thèmes marquants en 2008 (1)

Cybersurveillance des salariés par l'employeur

- Elaboration en 2008 d'une décision type visant à concilier respect de la sphère privé des salariés sur le lieu de travail et les intérêts légitimes des employeurs:
- Autorisation seulement, si besoin avéré (moyens alternatifs insuffisants?)
- assortie de conditions > Nécessité d'une proportionnalité des mesures de surveillance:

  Individualisation des données collectées « Progressive Kontrollverdichtung »
- Critères, limitations, conditions et recommandations dégagés des éléments concrets des nombreuses demandes d'autorisation et en tenant compte du cadre tracé par le catalogue limitatif de finalités pour lesquelles des mesures de surveillance sont admissibles (Art.L.261-1 Code du Travail)

  Notamment certains traitements visant la sauvegarde du fonctionnement technique des systèmes informatiques de l'entreprise, la protection des droits de propriété intellectuelle, des secrets d'affaires et de fabrications, des informations auxquelles est attachée un caractère de confidentialité et la prévention d'actes de concurrence déloyale
- Document d'orientation détaillé et décision-type publiés sur notre site Internet

Temps forts et thèmes marquants en 2008 (2)

Accès de tiers aux données personnelles des fichiers publics

- Echanges de données entre autorités/administrations poursuivant un intérêt public différent ou Faculté de consultation instaurée, ou
- Interconnexion de fichiers publics (finalités identiques ou compatibles)
- Dossiers examinés: Immigration, Fisc, Famille: FNS, allocations familiales Boni enfant/chèques accueil, Police, Transport, Cadastre, Logement,…
- Réutilisation dans l'intérêt de la recherche (domaines social, population, diversité, conditions de vie, éducation, santé,…)
- Avis (à l'égard des projets de texte légal) ou autorisation à délivrer
- Facteurs clé dans la mise ne balace des intérêts en présence:
  1. Légitimité: consentement éclairé, nécessité pour motif d'intérêt public,
  2. Proportionnalité, non discrimination,
  3. Anonymisation des données personnelles si possible,
  4. Information loyale des personnes concernées,
  5. Sécurité et confidentialité,
  6. Traçabilité des consultations: prévention des abus et détournements de finalité.

Temps forts et thèmes marquants en 2008 (3)

Quelques sujets délicats et arbitrages ardus : l'identifiant personnel unique

- Elaboration de son avis sur le PL 5950 relatif à l'identification des personnes physiques, au registre national des personnes physiques et à la carte d'identité
  - Longues discussions menées en amont avec les représentants des ministères impliqués et au sein du CNSAE (Comité National pour la Simplification Administrative en faveur des Entreprises)
  - Dossier d'une importance majeure: refonte du système de la loi du 30 mars 1979 =dépassé en pratique: dilution progressive de la ligne de démarcation entre usages licites et illicites
  - Tendance à l'élargissement du N° (en principe limité à l'usage administratif interne dans les actes, documents et fichiers déterminés par règlement grand-ducal et aux relations de l'administration avec les titulaires) et du cercle des utilisateurs (Autorités et administrations publiques)
  - Confidentialité du numéro de moins en moins respectée
  - Structure de l'identifiant inadaptée aux besoins et qui révèle l'âge, le sexe, l'époque
  - Nouvelles attentes: simplification des démarches administratives
  - Sécurisation des transactions combinée à la facilité et rapidité d'usage
- Possibilité de parvenir à un équilibre entre modernisation/simplification administrative et protection des données à caractère personnel des citoyens tout en conservant un numéro d'identification unique multisectoriel des personnes

Temps forts et thèmes marquants en 2008 (4)

Quelques sujets délicats et arbitrages ardus : l'identifiant personnel unique

- Enjeu du recours à un Identifiant unique multisectoriel: « Gläserner Bürger »
  - Rapprochement excessif d'informations multiples contenues dans les différentes base de données publiques , Interconnexions illicites, échanges de données non autorisées; CNIL:« traçage des individus dans tous les actes de la vie courante »,;
- Beaucoup d'États européens y renoncent par principe: France (Projet Safari), RFA (Volkszählungsurteil :1983) Portugal (Constitution), Autriche, …
- Recommandation (86)1 du 23/01/1986 du Conseil de l'Europe: Juste équilibre
- Directive 95/46/CE du 24 octobre 1995: Article 8 § 7: la loi doit déterminer les conditions dans lesquels un traitement peut avoir lieu: garanties adéquates.
- La CNPD à appelé de ses vœux le recours à des solutions innovantes mettant à profit les technologies les plus avancées: modèle autrichien?
- Pistes de réflexions dégagées également des exemples belges et suisses:
  - Banques carrefour placées sous la surveillance de Comités sectoriels présidés par un membre de la Commission de la protection de la vie privée;
  - Numéro non parlant: pas de problèmes de transition en Suisse et aux Pays-Bas;
  - Traçage des accès (qui, quand, pourquoi) passant à travers ces plaques tournantes;
  - Droit d'information sur les consultations pouvant être exercé par les concernés.

Temps forts et thèmes marquants en 2008 (5)

Quelques sujets délicats et arbitrages ardus : autres sujets

- E-restauration
  - Saisie des données relatives à la consommation des utilisateurs des cantines scolaires; de l'enregistrement Intervention de la Commission nationale faisant suite à quelques plaintes reçues de la part d'utilisateurs ; Introduction d'une faculté d' opt-out en faveur des adultes etélèves âgés de 16 ans et plus; réduction sensible du nombre de données enregistrées et de la durée de conservation
- Traitement ultérieur à des fins statistiques, scientifiques ou historiques
  - Arbitrage délicat du juste équilibre entre deux intérêts : le principe du respect strict de finalité et les intérêts éminents de la recherche qui peut avoir besoin de données collectées initialement à d'autres fins.
  - Etudes cliniques et statistiques du CRP-Santé: accidents vasculaires cérébraux (AVC) ;
  - évaluation de politiques publiques p.ex. en matière d'emploi , d'éducation, de sécurité sociale et d'environnement
- Traitement de données sensibles, biométriques et génétiques
  - Statistiques ethniques (table ronde avec le président de la CNIL à ce sujet à Luxembourg)
  - Accès aux dossiers médicaux, hospitaliers, des prestataires de soin :Registre du cancer ou de néphrologie, Biobanque
  - Projet e-Santé: dossier médical et carte patient électroniques
- Géolocalisation
  - Téléphonie mobile, HotCity, Surveillance parentale ou de personnes dépendantes
  - Tracage des déplacements de véhicules de l'entreprise utilisés par les salariés

Priorités pour les années à venir. Perspectives

- Information du public sur les risques et les droits en matière de protection de la vie privée: sensibiliser les jeunes en particulier en relation avec l'usage d'Internet
- Guidance à fournir aux entreprises, organismes et administrations publics ;
- Publication de recommandations thématiques et sectorielles
- Promouvoir le rôle du chargé de la protection des données, inciter entreprises, associations et organismes publics à l'instituer dans leurs établissements
- Contrôles ponctuels et des investigations spontanées et à titre préventif pour des fichiers importants et sensibles où la confiance du public dans les institutions exige que le respect de la loi soit parfaitement assuré
- Accompagnement des projets publics ayant un impact sur la protection de la vie privée des citoyens : radars/caméras sur les routes, Identifiant unique, e-Government, e-Santé, …
- Vers une révision de la directive 95/46/CE: modernisation, simplification, plus grande efficacité de l'action des autorités de contrôle dans un monde globalisé.

Vos questions ?

Adresse et contacts

Commission Nationale pour la Protection des Données

MM. Gérard Lommel (président)
Thierry Lallemang & Pierre Weimerskirch (membres effectifs)

Mme Josiane Pauly, M.MarcHemmerling et M Wirion (membres suppléants)

41, avenue de la Gare
L-1611 Luxembourg
Siège : L-4100 Esch-sur-Alzette

Tél.: 26 10 60 - 1
Fax.: 26 10 60 - 29
E-Mail: info@cnpd.lu
www.cnpd.lu

Commission Nationale pour la Protection des Données

Des failles et des pannes rapportées par les médias

- Phishing: banque luxembourgeoise est attaquée sur son Internet-banking.
- Un cheval de Troie sur un site luxembourgeois très fréquenté: risque élevé de vol de mots de passe.
- Piratage de clients eBay. Des pirates ont trouvé le moyen d'accéder à la base de données des serveurs.
- AOL publie 500.000 demandes de recherche sur Internet de ses abonnés américains. Ces recherches couvrent une période s'étalant sur trois mois, soit environ 20 millions d'entrées, non censurées ni filtrées.
- Le gouvernement britannique reconnait la perte de deux disques contenant les données personnelles (allocations familiales avec noms, dates de naissance, numéros de sécurité sociale et coordonnées bancaires des bénéficiaires) de 25 millions de Britanniques.
- Un militaire de la Royal Navy, s'est fait voler un ordinateur contenant des informations sur 600.000 britanniques. Les informations bancaires de 3.500 personnes figurent également dans le disque de la machine.
- L'administration fiscale et douanière britannique a perdu un ordinateur portable renfermant les données personnelles de 400 personnes et a égaré dans le courrier postal un disque contenant les dossiers de retraite de 15 000 individus.
- Les déclarations de revenus de 40 millions d'Italiens ont été mises en ligne et consultables par tout un chacun.