Délibération n° 166/2008 du 20 juin 2008 de la Commission nationale pour la protection des données relative à la demande de l'Institut Luxembourgeois de Régulation concernant la procédure « article 41 » de la loi du 2 août 2002

I. Contexte

Dans sa délibération du 25 mai 2007, la Commission nationale pour la protection des données a autorisé, à la demande de l'Institut Luxembourgeois de Régularisation (ILR), la mise en place du système entièrement automatisé de l'accès de plein droit prévu par l'article 41 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, en jugeant suffisantes les mesures de sécurité détaillées dans les documents soumis par l'ILR.

Avant la mise en service de ce système, l'ILR avait fait réaliser un audit externe par la société Ernst & Young. Cet audit avait pour mission d'identifier d'éventuelles faiblesses du système dénommé « Article 41 ». Le rapport conséquent du 22 octobre 2007 avait ensuite conclu que certains objectifs de sécurité n'étaient pas atteints, notamment pour la raison que l'ILR avait encore entièrement mainmise sur le système Anti-Abus.

Suite à ce rapport, l'ILR s'est efforcé de mettre en œuvre certaines recommandations lui soumises (rapport du 6 décembre 2007) et a également fait réaliser une étude intitulée « Analyse des risques et des impacts » par Fujitsu Services et Ubizen concernant le système d'information « Article 41 ». Ces conclusions sont reprises dans un rapport datant du 8 février 2008.

Ces rapports ont ensuite été envoyés à la Commission nationale pour la protection des données par le biais du Ministère des Communications afin de l'analyser d'un *«point de vue de la nécessité des mesures proposées et du respect du principe de proportionnalité ».*

Le présent document reprend les conclusions de ces premières analyses.

II. Les conclusions du rapport d'audit d'Ernst & Young

Ce rapport statue par des conclusions bien précises sur les points ayant été soumis à contrôle sur les limites de l'étude ainsi que sur les failles et faiblesses identifiées.
Un des défauts majeurs restant à corriger et résultant de la conception du système était le fait que l'IRL ne devait plus avoir la possibilité d'avoir accès aux informations à caractère personnel qui font l'objet d'une recherche par les autorités dans le cadre de l'application de l'article 41 de la loi.

La Commission nationale, tout en n'ayant pas analysé la totalité des recommandations dans leurs moindres détails, constate néanmoins certains problèmes :
- la possibilité aux administrateurs réseaux ILR de prendre le contrôle complet des serveurs, des bases de données et des applications du système d'information « Article 41 » ;
- la possibilité aux administrateurs réseaux ILR de lire, modifier et restaurer des backup du système d'information « Article 41 » ;
- la présence de données issues de tests ou lors du développement des applications dans l'environnement de production ;
- l'utilisation d'une imprimante non-sécurisée pour imprimer des rapports PC-SAA (PC for anti abuse system) ;
- la protection insuffisante contre des attaques internes concernant les clés d'encryptions enregistrés dans le « Hardware Security Module » ;
- la protection insuffisante des serveurs contre des incidents environnementaux comme le feu, l'inondation, etc. ;
- la protection insuffisante contre un « capacity overrun » ;
- l'insuffisance de la documentation des procédures organisationnelles ;
- l'insuffisance de personnes ILR pouvant garantir une maintenance du système 24 h/24 et 7 jours/7.

III. Les réponses de l'ILR face aux recommandations d'Ernst & Young

Le 6 décembre 2007, l'IRL a pris position par rapport à chaque recommandation présentée dans ledit rapport d'audit. Or, il n'est pas très clairement mentionné combien de recommandations ont effectivement été acceptées, combien ont déjà été mises en place ou bien encore combien doivent être mises en place.

Même si chaque recommandation est abordée par l'ILR, cette dernière n'en tire pas toutes les conclusions quant aux différents points. Il semble d'ailleurs que, même si l'ILR entend suivre ces recommandations, les modifications n'ont pas encore été mises en œuvre (ceci résulte notamment des points 2.2, 2.3, etc.).

Les réponses de l'ILR indiquent en effet que des améliorations ont été apportées, mais le rapport ne permet pas encore de déterminer de façon certaine si l'ensemble des défauts soulevés dans le rapport d'audit ont été corrigés.

Pour cette raison, la CNPD préconise que l'Institut établisse un plan indiquant clairement les recommandations déjà mises en place et celles qui le seront ultérieurement, ainsi qu'un calendrier prévisionnel afférent.

Sous cet aspect, la Commission nationale ne peut pas constater si les mesures de sécurité proposées par le rapport sont opérationnelles et si le système répond aux exigences légales.

IV. L' analyse des risques et des impacts effectuée par Fujitsu Services et Ubizen

1) Avis sur la portée de l'analyse

Ce rapport fait état de plusieurs vulnérabilités découvertes lors de l'analyse des différentes parties du système. Cependant, ce rapport ne peut être considéré comme une « analyse de risques » au sens des normes ISO (cf. ISO 13335-2 ou 27005) car il fait défaut de certaines considérations :

1. L'envergure de l'analyse n'est pas indiquée.
2. Il n'y a pas d'estimation des différents paramètres des risques comme l'impact et la probabilité d'occurrence.
3. Le rapport ne décrit ni les menaces ni les scénarios d'éventuelles attaques.
4. Le rapport ne donne pas d'estimation du niveau des différents risques.

Étant donné qu'il y a absence de ces informations, tels que le niveau de risque sur le système actuel et l'absence d'une indication des coûts des contre-mesures, la Commission nationale n'est pas en mesure d'analyser la proportionnalité du traitement prévu par le système, sur base des conclusions de ce rapport.

Pour ce faire, la CNPD devrait disposer d'un plan de traitement de risques qui qualifierait les mesures déjà mises en place, les mesures retenues pour leur mise en place, les risques résiduels et une justification détaillée pour chaque mesure de sécurité initialement proposée mais non retenue. Un tel plan de traitement des risques est décrit dans la norme ISO 27005.

2) Avis sur le contenu du rapport

Malgré l'absence de précisions additionnelles concernant les points mentionnés ci-dessus, certaines conclusions de ce rapport apparaissent d'ores et déjà inquiétantes.

En particulier le fait qu'une réinitialisation du système suite à une panne nécessiterait une durée comprise entre 1 jour et 6 semaines (cf. p. 28). Si cela s'avérait exact, il parait indispensable à la Commission nationale à ce que l'Institut en charge prenne les mesures nécessaires pour rendre le système conforme aux attentes du législateur, étant donné que ledit système a été prévu pour protéger la vie des victimes devant être localisées ou qu'elle développe au moins une procédure d'urgence qui offrirait aux autorités une possibilité « manuelle » en cas de système hors fonction.

Certaines informations techniques ou conclusions suggérées dans le rapport nous apparaissent discutables, tel le calcul déterminant la nécessité d'une présence de 5,15 personnes pour assurer un service 24/24h sur 7/7 jours. Ce calcul se base notamment sur l'hypothèse dans laquelle le système tournerait en présence d'une personne. Or il nous semble qu'avec le système Alarmtilt, il suffit d'un service de permanence, mais non d'une présence pour assurer le service 24 h/24 sur 7 jours/7.

Conclusion

En vue d'une mise en place correcte des mesures de sécurité invoquées dans sa délibération du 25 mai 2007 la Commission nationale recommande de faire adapter le système d'information analysée de façon à pallier aux insuffisances mises en évidence dans les rapports d'audit et d'analyse de risques et d'impactes et de présenter un plan et un calendrier de mise en œuvre.

Luxembourg, le 20 juin 2008

La Commission nationale pour la protection des données

Gérard Lommel	Pierre Weimerskirch	Thierry Lallemang
Président	Membre effectif	Membre effectif

Indication des voies de recours

La présente décision administrative peut faire l'objet d'un recours en annulation dans les **3 mois** qui suivent sa notification à l'administré. Ce recours est à intenter par l'administré devant le tribunal administratif et doit obligatoirement être introduit par le biais du ministère d'avocat à la Cour inscrit auprès de l'un des deux tableaux de l'ordre des avocats.