Mercredi 9 octobre 2013

Intervention de NURPA dans le cadre de l'audition organisée par la commission de la Justice

Examen de DOC 53 1540 [1] et DOC 53 1509 [2]

À propos

Fondée en 2010, NURPA (Net Users' Rights Protection Association) est une organisation pluridisciplinaire qui rassemble des citoyens désireux de promouvoir et défendre les droits de l'Homme dans l'environnement numérique.

Préambule

Notre intervention se concentrera sur la proposition de loi modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, en ce qui concerne les sanctions administratives, la notification de fuites de données, le droit de consultation et les conseillers en sécurité de l'information (DOC 53 1509).

Dans le contexte de la révision européenne de la directive relative à la protection des données, il est pertinent de continuer les travaux sur la proposition (DOC 53 1509) à l'échelle nationale. Les différentes affaires ayant ponctué ces derniers mois ont montré qu'il était urgent d'assurer la protection de la vie privée des citoyens belges sans attendre une éventuelle issue au dossier européen. Par ailleurs, la loi du 8 décembre 1992 adaptée par la proposition examinée aujourd'hui pourrait servir de référence pour la Belgique au sein du Conseil de l'Union européenne.

1 http://www.ericjadot.be/uploadedfiles/13076166542011090 6%20R%C3%A9solution%20Google%20Street%20View.pdf
2 http://www.dekamer.be/FLWB/PDF/53/1509/53K1509001.pdf

Droit de consultation - droit à la portabilité des données (chapitre 2)

« L'obligation de communiquer les données à caractère personnel sous une forme intelligible, prévue dans la loi sur la protection de la vie privée, n'est actuellement pas toujours interprétée comme étant l'obligation de fournir une copie de ces données sous une forme électronique utilisable. » Développements - § 5

Remarque 1. Le droit à la portabilité des données introduit dans la proposition est une matérialisation et une précision du droit d'accès tel que défini par l'article 10 § 1er b) de la loi du 8 décembre 1992. Le droit d'accès pourrait être considéré comme un droit de portabilité envers l'utilisateur. Nous recommandons que le droit d'accès soit renommé en droit à la "portabilité des données" et défini de telle manière qu'il existe dans le chef de l'auteur d'un traitement, une obligation de fournir les données récoltées dans un format standard et interopérable.

« En cas de traitement automatisé, la personne concernée peut demander la communication par la voie électronique des renseignements archivés électroniquement. » Proposition - Art. 2, 1

Remarque 2. Le terme "renseignements" est vague, nous recommandons que l'article 2, 1 soit reformulé comme suit : "En cas de traitement automatisé, la personne concernée peut demander la communication par voie électronique de l'intégralité des informations archivées, dans un format standard et interopérable."

Conseiller en sécurité de l'information (chapitre 3)

« Le responsable du traitement désigne, seul ou avec d'autres responsables, un conseiller en sécurité de l'information. Cette obligation ne s'applique pas aux personnes physiques et aux personnes morales privées qui n'occupent en permanence pas plus de neuf personnes pour le traitement automatisé de données à caractère personnel. » Proposition - Art. 6

Remarque 3. Le terme "conseiller en sécurité de l'information" est vague, il pourrait formellement s'appliquer à toute personne chargée de protéger une infrastructure informatique. Nous recommandons qu'il soit remplacé par le terme "préposé/délégué à la protection des données à caractère personnel" ce qui correspondrait aux termes utilisés dans les pays auxquels cette proposition de loi fait référence ("Datenschutzbeauftragter" en Allemagne, "Data protection official" en anglais).

Remarque 4. Il est trivial de développer et d'opérer seul un service pouvant supporter des milliers d'utilisateurs. Plutôt que de fonder l'obligation sur le nombre de personnes en charge du traitement des données, nous recommandons que celle-ci soit relative au nombre d'utilisateurs d'un service, 250 par exemple.

Sanctions administratives (chapitre 4)

« Une solution consiste à permettre à l'autorité de contrôle d'infliger des amendes administratives. » Développements - § 2

Remarque 5. Nous soutenons pleinement la proposition d'extension des compétences de la CPVP et notons que ces nouvelles fonctions devront nécessairement s'accompagner d'une réévaluation du budget alloué à cette autorité.

« En cas d'infraction à la législation ou à la réglementation dont elle contrôle le respect, la Commission de la protection de la vie privée notifie ses griefs au contrevenant ainsi que le montant envisagé de l'amende administrative au profit du Trésor public d'un montant maximal de 10 000 euros. L'amende précitée peut être doublée en cas de nouvelle infraction à la législation ou à la réglementation susmentionnées dans les trois ans qui suivent la première condamnation. » Proposition - Art. 13

Remarque 6. Le montant de la proposition (10 000 euros ; le double en cas de récidive) n'est pas plus dissuasif eu égard au chiffre d'affaire de certains géants du Web (Google > 50 milliards de dollars ; Facebook > 5 milliards de dollars). Afin d'éviter toute disproportion et d'accentuer la nature dissuasive de la sanction pécuniaire, nous recommandons que le montant soit fixé à 2 pour cent du chiffre d'affaire annuel mondial (comme le prévoit, par ailleurs, le projet de règlement européen en la matière).

Remarque 7. La perspective que le profit de l'amende revienne partiellement ou intégralement à la CPVP devrait être envisagée.

Notification des fuites de données (chapitre 5)

« Lorsque le responsable du traitement constate que des données à caractère personnel qu'il a traitées ont été transmises indûment ou que des tiers en ont pris connaissance indûment d'une autre manière, et que les personnes concernées risquent de subir des dommages graves, il informe ces dernières et la Commission selon les modalités défi nies au présent article » Proposition - Art. 14

Remarque 8. La divulgation de données personnelles sans le consentement d'un utilisateur est un dommage en tant que tel, la gravité du dommage est toujours complexe à évaluer. Nous recommandons de supprimer "et que les personnes concernées risquent de subir des dommages graves".

« La notification est requise en cas de violation concernant les données à caractère personnel suivantes: [...] » Proposition - Art. 14 § 2

Remarque 9. Nous recommandons que la notification soit requise dès lors que des données personnelles font l'objet d'une divulgation non consentie. Tenter d'en dresser une liste exhaustive revient à renoncer sciemment à traiter un certain nombre de cas particuliers.

« La Commission est informée sans délai. » Proposition - Art. 14 § 4

Remarque 10. Le délai de notification à l'autorité de protection des données et aux utilisateurs doit être défini clairement. Nous suggérons une échéance 72h. Nous recommandons par ailleurs que la-dite autorité mette à disposition du public une base de données contenant toute information utile sur les fuites, leur nature et l'auteur du traitement. Cela va dans le sens des obligations d'information prononcées par les tribunaux ou certaines autorités de protection des données (en France notamment) et crée une motivation supplémentaire pour les auteurs de traitement à mettre en œuvre les dispositions adéquates pour protéger les données personnelles traitées.

« La notification aux personnes concernées d'une violation de données à caractère personnel n'est pas nécessaire si le responsable du traitement a prouvé, à la satisfaction de la Commission, qu'il a mis en œuvre les mesures de protection technologiques appropriées et que ces dernières ont été appliquées aux données concernées par ladite violation. Par mesures de protection technologiques, on entend les mesures qui rendent les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès et qui permettent d'éviter un préjudice grave consécutif à une éventuelle utilisation abusive des données à caractère personnel. » Proposition - Art. 14 § 4, 2

Remarque 11. La sécurité informatique est un process, pas un produit. Les "mesures de protection technologiques" efficaces aujourd'hui ne le seront peut-être plus demain (voir par exemple le cas de l'algorithme de hashage MD5 qui était considéré comme l'état de l'art et qui a été rendu inutile par la cryptanalyse). Toute divulgation non consentie de données personnelles devrait faire l'objet d'une information au public.

« Le responsable du traitement tient à jour un inventaire des violations de données à caractère personnel, notamment de leur contexte, de leurs effets et des mesures prises pour y remédier, de manière à permettre à la Commission de vérifi er le respect des dispositions du présent ar ticle. Cet inventaire compor te uniquement les informations nécessaires à cette fin. » Proposition - Art. 14 § 5

Remarque 12. Voir notre remarque 10.

Nous nous tenons à la disposition des membres de la commission pour toute information complémentaire.

E-mail : contact@nurpa.be