Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Préposé fédéral à la protection des données et à la transparence
PFPDT

A2015.06.22-0004 / 2014-00045 22.06.2015/WJ

Conférence Octopus 2015, Coopération contre la Cybercriminalité

Panel : Sécurité, vie privée et état de droit dans le "cloud" – Est-ce que nous progressons ?

Jean-Philippe Walter
Préposé fédéral suppléant à la protection des données et à la transparence
Président du Comité consultatif de la Convention 108 (T-PD)

1. A titre liminaire, je tiens à rappeler et à souligner que la protection des données n'a pas pour objectif d'empêcher le traitement légitime de données personnelles et en particulier d'entraver le travail des autorités de poursuite judiciaire. Elle fixe un cadre à respecter pour garantir le respect des droits et des libertés fondamentales et notamment le droit à la vie privée. Tant le comité consultatif de la Convention 108 que le Groupe de l'article 29, qui communiquera sous peu ses réponses aux scénarios, réaffirment leur volonté et leur disponibilité à dialoguer et à chercher des solutions avec le T-CY.

2. Comme le relevait Thomas Duke, nous sommes tous gouvernés par les principes des droits de l'homme et l'un des objectifs de la convention de Budapest est la défense des droits de l'homme. Il en va de même de la Convention 108 du Conseil de l'Europe.

3. De manière générale, il me parait fondamental de renforcer le cadre juridique de la protection des données et la collaboration au niveau international pour garantir le respect des droits et libertés fondamentales lors de traitement de données personnelles et lutter contre le cybercrime. Dans un monde globalisé où les traitements de données personnelles ne connaissent plus de limites et de frontières, la protection de la vie privée et du droit à la protection des données passe par la mise en place d'un cadre commun de protection des données basé sur un standard universel. En ce

sens, le Conseil de l'Europe joue un rôle crucial et incontournable. La Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et son protocole additionnel concernant les autorités de contrôle et les flux transfrontières de données sont à l'heure à actuel les seuls textes juridiquement contraignants de portée universelle. La Convention est ouverte à la signature des Etats tiers. Aujourd'hui 46 Etats membres du CoE sur 47 sont partie à la Convention. L'Uruguay est le premier Etat tiers à y avoir adhéré. Le Maroc, le Sénégal et Maurice devraient suivre très prochainement. D'autres Etats ont manifesté leur intérêt. Il serait ainsi nécessaire, voire même une condition que les pays partie à la Convention de Budapest adhèrent également à la Convention 108. J'attends du Conseil de l'Europe qu'il agisse en ce sens en promouvant systématiquement l'adhésion aux deux instruments.

4. Le recours au cloud ou l'infonuagique ne doit pas aboutir à un affaiblissement des droits des personnes dont les données sont traitées et stockées quelque part dans un nuage souvent opaque.

5. De manière plus concrète par rapport au cloud, il est important que l'individu ou le responsable de traitement qui recourt à l'infonuagique garde la maîtrise sur les données qui le concerne ou sur les données qu'il souhaite placer dans le nuage. En ce sens, la meilleure protection serait encore de renoncer à des solutions en nuage non transparentes et de continuer à traiter les données dans son propre environnement ou de les stocker auprès d'entreprises spécialisées dans le stockage des données offrant des garanties de sécurité élevé ou pour le moins de recourir à des prestataires de service situés dans des pays assurant un niveau de protection des données conforme à la Convention 108.

6. Il est particulièrement important que les fournisseurs de services dans le nuage offre des garanties élevés de sécurité sous l'angle organisationnelle et technique et qu'en particulier les utilisateurs de ces services aient la garantie que les données qui y sont traités ne sont accessibles qu'à eux-mêmes, ou à ceux avec qui ils les partagent. Cela passe par l'utilisation de systèmes de cryptage de données fort. Je dirais que cette exigence ne vise pas seulement la protection des données, mais aussi la lutte contre

le cybercrime. De nombreuses attaques pourraient être évitées avec des mesures de sécurité élevées.

7. Il est nécessaire de renforcer les devoirs de diligence et de responsabilité de ceux et celles qui recourt à l'infonuagique. Le choix du service d'infonuagique est ainsi essentiel. On ne recourra pas à Dropbox pour placer des données sensibles ou relevant du secret des affaires.

    - Le responsable de traitement doit ainsi procéder à une analyse de risques en matière de respect du droit à la protection des données avant de recourir à telle ou telle solution infonuagique.

    - Les données et les traitements qui se feront dans le nuage doivent être clairement identifiés

    - Les exigences de sécurité technique et juridique doivent être définies : trop souvent les prestataires de service infonuagiques imposent leurs conditions et ne laissent pas de place au client pour faire valoir ses exigences et ses attentes. Le client doit pouvoir négocier ses exigences et les inclure dans un contrat de prestation ou avoir la possibilité de recourir à un service répondant à un niveau d'exigence suffisamment élevé :

8. Le prestataire de services cloud doit être transparent à savoir :

    - Il doit pouvoir être localisé : indication claire et exhaustive des pays hébergeant les centres de données
    - Il doit afficher s'il est soumis à une législation de protection des données ou quelle garantie de protection des données il offre et pouvoir démontrer comment il respecte les exigences en la matière.
    - Les clauses de protection des données devraient être clairement accessibles et non pas noyées dans clauses générales
    - Il doit donner des informations sur les technologies qu'il utilise
    - Il doit indiquer les moyens de protéger les données et également comment les personnes peuvent exercer leurs droits.

9. Parmi les garanties que le prestataire devrait remplir, mentionnons en particulier la :
    - Fixation les durées de conservation des données limitées à ce qui est nécessaire au regard des finalités du traitement
    - Destruction ou restituer les données en fin de prestation ou rupture de contrat (garantie d'un droit de portabilité pour les personnes concernées)
    - Garantie des droits des personnes concernées
    - Obligation d'assurer la sécurité des données, notamment pour assurer la disponibilité, l'intégrité et la confidentialité des données (chiffrement des données, garantie que le prestataire n'a pas accès aux données confiées, liaison chiffrée, etc.)
    - Garantie d'audits réguliers pour vérifier mises en œuvre des exigences de protection et sécurité des données
    - Recours à la certification
    - Annonce des failles de sécurité (data breaches)
    - Acceptation du contrôle d'une autorité indépendante de protection des données

10. Enfin un soin particulier doit être accordé à la formation et à la sensibilisation des différents acteurs sur les risques, le cadre juridique et les moyens d'assurer la sécurité des données et garantir le droit à la protection des données.