Conférence Le Point «Maison connectée et intelligente»

Paris, 28 mars 2013

Peter Hustinx

Contrôleur européen de la protection des données

«Le partage des données à caractère personnel et le respect de la vie privée à domicile»

Je suis particulièrement heureux de pouvoir contribuer à cette conférence, consacrée à un thème d'une grande importance pratique et symbolique: comment préserver notre vie privée à domicile, dans un monde de plus en plus connecté?

La vie privé à nos domiciles a toujours été au cœur des protections constitutionnelles et représente désormais un élément clé du droit fondamental à la protection de la vie privée. Pénétrer dans une maison sans permission ou intercepter des communications privées est, pour des raisons légitimes, soumis à des garanties particulières.

Dans une société de l'information reposant sur l'utilisation systématique des technologies de l'information et de la communication – tant à domicile qu'ailleurs –, nous devons investir dans la mise en place de garanties renforcées afin d'assurer la protection des données à caractère personnel en général. C'est la raison pour laquelle le cadre juridique de la protection des données dans l'Union européenne est actuellement examiné.

À défaut d'être soumise à d'importantes garanties, l'introduction de «maisons intelligentes» pourrait gravement compromettre les protections existantes. Bien que les systèmes de mesure intelligents puissent offrir des avantages significatifs, ils permettent également de recueillir de grandes quantités de données à caractère personnel permettant de savoir ce que font les membres d'un ménage dans l'intimité de leur foyer.

Ces données peuvent être utiles pour analyser notre consommation d'énergie, mais en corrélation avec des données issues d'autres sources, le potentiel d'une large exploration de données est très important.

Ce phénomène sera d'autant plus évident si l'«Internet des objets» devient réalité et si tous les objets que nous utilisons couramment à domicile sont connectés en ligne et se mettent à communiquer, les uns avec les autres et avec des prestataires extérieurs, sur nos habitudes et nos besoins.

Qui sera responsable de cette information: est-ce que ce sera vraiment nous? Ou serons-nous obligés de vivre dans des «maisons transparentes», où la protection de la vie privée à domicile a perdu sa signification. Comment pouvons-nous nous assurer que ce *ne* sera *pas* le cas?

Permettez-moi d'abord d'expliquer quelles mesures sont prises actuellement pour renforcer les garanties de la protection des données à caractère personnel. Notre cadre juridique actuel, qui constitue la base de toutes les lois nationales dans l'UE, a été adopté en 1995, alors qu'Internet existait à peine. Il est donc clairement nécessaire d'innover, principalement pour assurer une meilleure protection contre les défis actuels.

Un autre problème est celui de la diversité et de la complexité, toutes les deux excessives, étant donné que le cadre juridique a été transposé dans 27 lois nationales différentes. Renforcer l'harmonisation et la cohérence dans l'UE contribuerait à rendre la protection plus efficace. Enfin, le traité de Lisbonne a introduit une base permettant une protection plus efficace et plus complète dans tous les domaines politiques.

Par conséquent, la Commission européenne a proposé une réforme profonde du cadre juridique actuel en janvier 2012. Cette proposition est actuellement débattue au Parlement européen et au Conseil. Bien que l'ensemble de mesures proposé soulève encore de nombreuses questions, ses principaux axes font l'objet d'un large consensus.

En premier lieu, le cadre législatif de l'UE sera étendu: la législation européenne s'appliquera également à l'offre des biens et services sur le marché européen ou au contrôle des résidents de l'UE. Des règles équitables seront ainsi établies concernant la couverture des activités des fournisseurs de services Internet et des autres acteurs clés, qu'elles soient exercées dans l'UE ou dans un pays tiers.

En deuxième lieu, la position des personnes concernées sera renforcée pour assurer un contrôle adéquat du recueil et de l'utilisation de leurs données à caractère personnel. Il conviendra à cette fin de rendre le traitement des données plus transparent, les règles en matière de consentement plus strictes et les droits d'accès, de rectification et d'effacement des données ainsi que les droits à l'oubli et à la portabilité des données plus efficaces.

En troisième lieu, la responsabilité de la personne responsable du traitement sera mise en avant en lui attribuant des fonctions visant à assurer et à démontrer le respect des exigences en matière de protection des données, à réaliser des analyses d'impact opportunes sur la protection des données et à veiller à ce que tous les aspects pertinents de la vie privée soient intégrés dès le début dans les nouveaux développements (*Privacy by Design* – vie privée dès la conception).

En quatrième lieu, la position des autorités indépendantes sera renforcée en leur attribuant des pouvoirs accrus et uniformisés en vue d'un contrôle et d'une application de la législation plus efficaces ainsi qu'en prévoyant la possibilité d'imposer des amendes importantes et d'autres sanctions efficaces.

Enfin, il est probable qu'un règlement général sur la protection des données s'applique directement à l'ensemble des États membres en vue d'assurer une harmonisation et une cohérence accrue dans toute l'UE. Les autorités de contrôle coopéreront en outre plus étroitement sur les questions à dimension européenne ou internationale.

Alors, que signifie tout ceci pour les «maisons intelligentes», et plus particulièrement pour les systèmes intelligents de mesure? Simplement que la vie privée jouera un rôle beaucoup plus important que par le passé dans le développement et l'introduction de tous ces systèmes.

Il y a environ un an, la Commission européenne a adopté une recommandation relative à la préparation de l'introduction des systèmes intelligents de mesure. L'introduction de ces systèmes est actuellement prévue pour 2020 au plus tard, sous réserve d'une analyse d'impact économique des coûts et des bénéfices.

Elle ne devrait toutefois pas seulement être soumise à des considérations d'ordre économique. Étant donné qu'ils sont fortement susceptibles d'exercer un suivi intrusif du comportement

privé, tous les systèmes intelligents de mesure devraient également faire l'objet d'une analyse d'impact relative à la protection des données.

Le groupe de travail Article 29 a récemment été consulté concernant le modèle proposé pour cette analyse d'impact, telle que définie par le secteur. Le groupe de travail s'est d'abord montré très critique à l'égard du modèle proposé. Il lui reprochait d'être trop général, de comporter trop peu d'orientations pour être une véritable analyse des risques et de ne fournir aucune recommandation sur les meilleures pratiques pouvant être appliquées au contexte spécifique du réseau intelligent.

Le CEPD a adopté un avis en juin 2012 soulignant la nécessité d'introduire des garanties supplémentaires, y compris une éventuelle action législative au niveau de l'UE. Ces garanties devraient au moins comporter l'exigence obligatoire pour les responsables du traitement de mener une analyse d'impact relative à la protection des données ainsi que l'obligation de notifier les violations des données à caractère personnel.

Nous avons également recommandé que davantage d'orientations soient fournies concernant la base juridique relative au traitement des données, les choix qui s'offrent aux personnes concernées, la fréquence de la relève des compteurs et les périodes de conservation.

Il est en outre selon nous tout à fait logique d'introduire dans ce cadre l'application obligatoire des technologies renforçant la protection de la vie privée et d'autres bonnes techniques disponibles de limitation des données. En d'autres termes, le respect de la vie privée dès la conception devrait être la norme.

Les consommateurs devraient également pouvoir accéder directement à leurs données énergétiques, à leurs profils personnels, à la logique sous-tendant l'extraction des données ainsi qu'à toute information sur les fonctions d'accès à distance ON/OFF.

Un lien évident peut être établi avec l'utilisation de l'informatique en nuage. Dans ce cadre, il est essentiel de garder à l'esprit que le stockage des données «en nuage» ne signifie pas en dehors du champ d'application de la législation de l'UE sur la protection des données. En fait, les règles actuelles et futures en matière de protection des données s'appliquent également à l'informatique en nuage.

Par conséquent, il est essentiel de préciser qui sera chargé de veiller au respect des règles sur la protection des données dans cet environnement. Il ne s'agit pas seulement de savoir qui est responsable du traitement ou sous-traitant. Nous constatons de plus en plus que les clients et les fournisseurs de services d'informatique en nuage assument des responsabilités tous les deux. Il faut alors clairement décrire les responsabilités des deux parties pour éviter que la protection des données ne fasse gravement défaut dans la pratique.

En juillet 2012, le groupe de travail Article 29 a adopté un avis sur l'informatique en nuage qui a clairement démontré que des contrôles efficaces sont possibles pour assurer une protection adéquate des données. Il suffit que les parties responsables conviennent d'un commun accord de ces contrôles dans la pratique.

Selon moi, le problème actuel du déséquilibre des pouvoirs entre les clients et les fournisseurs des services d'informatique en nuage peut être résolu en fixant des termes et conditions types respectant les exigences en matière de protection des données et en établissant des normes et des régimes de certification incorporant pleinement les critères de protection des données.

La plupart des problèmes concernant le transfert international de données peuvent être résolus en instaurant des règles d'entreprise contraignantes. En novembre 2012, nous avons conseillé la Commission européenne en ce sens.

Tout cela révèle que la vie privée constitue désormais un sujet brûlant. Il convient de résoudre les problèmes du respect de la vie privée et de la sécurité en les incluant dès le début dans tous les projets pertinents. C'est le meilleur moyen d'assurer une protection efficace dans la pratique et d'instaurer la confiance dans la société d'information pour les années à venir.