



Digital Enlightenment Forum

«Données personnelles et citoyenneté dans la société numérique»

Crowne Plaza, Bruxelles, 19 septembre 2013

Jour 2: Politique, vision et débat – Session d’ouverture

Peter Hustinx

Contrôleur européen de la protection des données

Discours d’ouverture

Je me réjouis de l'occasion qui m'est offerte de contribuer à cette édition 2013 du Digital Enlightenment Forum.

L'environnement numérique dans lequel nous vivons aujourd'hui est sans aucun doute un espace de créativité, d'innovation et de prouesse technique extraordinaires. Mais permettez-moi de souligner d'emblée que davantage de créativité est nécessaire pour assurer une meilleure gouvernance numérique et une citoyenneté réelle pour tous dans la société numérique.

De récents évènements – souvent désignés comme les révélations concernant entre autres le programme PRISM – ont mis en lumière la vulnérabilité de notre environnement numérique actuel, qui résulte de la surveillance licite ou illicite, de l'interception et du filtrage à grand échelle de presque tous, sinon de tous, les échanges de données électroniques dans le monde.

Les divulgations apparaissent par épisodes et les informations se précisent de semaine et semaine.

Mais le plus frappant au stade actuel de nos connaissances, c'est non seulement l'ampleur et la profondeur de la surveillance entreprise, mais également le nombre d'acteurs privés,

notamment des fournisseurs de services Internet bien connus, qui y ont apparemment participé de manière active ou passive, ainsi que l'introduction de portes dérobées dans les systèmes de cryptage, avec pour résultats des effets pervers considérables et une forte érosion de la confiance du public, sur laquelle reposent l'existence et l'avenir de notre environnement numérique.

Toute cette affaire a généré et continue de générer des ondes de choc dans le monde entier.

Toutefois, nous devrions être conscients du fait que cette vulnérabilité s'explique également par d'autres facteurs qui ont pris de l'ampleur plus progressivement au fil des années, tels que la répartition actuelle du pouvoir sur Internet, qui reflète à la fois son architecture et les conditions économiques de son fonctionnement.

Un autre facteur est le fait que de nombreuses personnes se sont habituées à la disponibilité de services gratuits en échange d'une large surveillance de leurs comportements, de manière quasi-permanente. Tout le monde n'a pas conscience du fait que les services gratuits n'existent pas en réalité. Ceci a créé la base pour l'implication à grande échelle des acteurs privés dans la surveillance du public.

Nous assistons à un changement de paradigme: la confidentialité de la communication qui était – il n'y a pas si longtemps – un principe fort et une pratique scrupuleusement protégée, a cédé la place à la transparence de la communication, en plein essor, célébrée même par certains, et cela sans aucun changement constitutionnel ni le moindre débat informé. Cette évolution paraît en effet principalement dictée par un effet de mode et par la fascination pour la technologie et la commodité qu'elle offre au quotidien.

Mais il n'en demeure pas moins que la confiance dans le numérique au cours des prochaines années dépendra amplement de notre aptitude à prévoir des infrastructures juridiques et techniques aptes à instaurer et à préserver justement cette approche de confiance fondée sur des pratiques et principes de civisme largement partagés dans la société numérique.

L'UE est actuellement engagée dans un ambitieux exercice de mise à jour de ses cadres juridiques en matière de respect de la vie privée et de protection des données, destiné à les rendre plus efficaces dans la pratique et à rehausser leur cohérence parmi les différents États membres de l'UE. Ce processus est basé sur la reconnaissance du fait que ces concepts sont

des droits fondamentaux inscrits dans la Charte des droits fondamentaux de l'Union européenne, qui ont été rendus contraignants par le Traité de Lisbonne, non seulement pour les institutions et les organes de l'UE, mais aussi pour les États membres lorsqu'ils agissent dans le cadre de la législation communautaire.

Améliorer l'efficacité de la protection des données dans la pratique requiert de renforcer les droits des personnes concernées, d'accroître les responsabilités des organisations utilisant des données à caractère personnel et de consolider les mécanismes de supervision et de mise en œuvre des autorités de protection des données. Le règlement proposé en vue du remplacement de la directive actuelle permettra d'instaurer beaucoup plus de cohérence au sein de l'UE. Il s'appliquera à tous ceux qui offrent leurs biens ou services sur le marché européen et permettra d'instaurer des règles du jeu plus équitables que celles du cadre juridique actuel.

La Commission, le Conseil et le Parlement déploient des efforts importants pour mettre au point ce nouveau cadre juridique avant les élections européennes du printemps 2014. La Commission LIBE (Commission des libertés civiles, de la justice et des affaires intérieures) du Parlement européen votera sur son rapport d'ici quelques semaines. Après ce vote, d'importants efforts seront probablement déployés en vue de parvenir à un texte commun bénéficiant du soutien du Conseil et du Parlement. Je suis convaincu que tout cela sera mené à bien en temps voulu.

L'adoption de ce nouveau cadre juridique permettra de remédier de manière plus efficace qu'à l'heure actuelle aux activités abusives de suivi et de traçage, de surveillance et de profilage des comportements sur Internet. Il agira également comme un contrepoids plus efficace face aux tendances actuelles sur Internet et pourra ainsi aider à rétablir un équilibre acceptable entre les intérêts en jeu et à instaurer plus de confiance à l'égard de l'environnement numérique.

Suite à ces efforts, les pratiques industrielles devraient aller dans ce sens en s'orientant vers la prise en compte du respect de la vie privée dès la conception, la transparence et la responsabilisation. Ne nous trompons pas d'objectif: il n'est ni possible ni souhaitable de «réglementer» l'innovation, mais la loi peut créer les responsabilités appropriées et prendre les mesures incitatives appropriées, et c'est précisément ce à quoi conduira le nouveau cadre juridique.

La question demeure de savoir dans quelle mesure les gouvernements et les entités agissant pour leur compte devraient être autorisés à intercepter les échanges électroniques, et le cas échéant, dans quelles conditions et avec quelles garanties? Il conviendrait de répondre à cette question, et ceci de manière spécifique à tous les niveaux concernés, mais en l'abordant de manière distincte.

La jurisprudence de la Cour européenne des Droits de l'Homme en la matière est très claire et a été établie il y a plusieurs décennies. Elle s'applique à tous les États membres et peut également être source d'inspiration pour les discussions transatlantiques lorsque le moment sera venu de progresser dans ce domaine également.