

Séminaire sur le thème "le programme de Stockholm: une stratégie de gestion de l'information améliorée pour l'espace de liberté, de sécurité et de justice"

Fondation Robert Schuman, Parlement européen, Bruxelles, le 12 novembre 2009

"La protection des données intégrée dans une stratégie de l'UE en matière de gestion de l'information"

Peter Hustinx

Contrôleur européen de la protection des données

I. Introduction

Pour commencer, j'aimerais souligner que la protection des données constitue un élément très positif, qui fait même partie intégrante de la stratégie de gestion de l'information pour la sécurité intérieure de l'UE, actuellement élaborée par le Conseil. Cette stratégie est envisagée dans le cadre du projet de programme de Stockholm, dont elle sera par conséquent l'un des premiers résultats. La grande importance accordée à la protection des données dans ces deux documents est pleinement conforme au traité de Lisbonne, qui doit entrer en vigueur le 1^{er} décembre 2009.

J'aimerais également faire observer non seulement que la protection des données est intégrée dans la stratégie, mais aussi que le CEPD en tant qu'institution a participé, à plusieurs stades, au processus d'élaboration de cette stratégie. Je tiens à mentionner la réunion de lancement du groupe de travail du Conseil qui a eu lieu en juillet, ainsi que la conférence COPE-09 qui s'est tenue à Stockholm en septembre. Je suis reconnaissant à la présidence suédoise d'avoir activement associé le CEPD à ce processus.

Dans cette brève contribution, je souhaiterais souligner, sur la base de nos contributions antérieures, ce qu'il convient d'entendre par une pleine intégration de la protection des données.

II. Le juste équilibre entre échange d'informations et protection des données

On a beaucoup parlé de la nécessité d'un équilibre entre répression et protection des données. Cet équilibre ne signifie pas pour autant que la protection des données ferait obstacle à l'utilisation d'informations nécessaires à l'élucidation d'un crime. Toutes les informations qui sont réellement nécessaires à cette fin peuvent être utilisées, conformément aux règles relatives à la protection des données.

Dans le cadre de l'État de droit, la protection des données peut restreindre la collecte d'informations, en l'absence d'élément de preuve établissant que ces informations peuvent être nécessaires. Il importe, et il est même essentiel à mon avis, de sélectionner les informations avant de les collecter. Il convient de recueillir les informations à des fins spécifiques. Il ne serait pas judicieux de créer d'immenses bases de données contenant des données à caractère personnel dans l'éventualité où elles pourraient s'avérer utiles à l'avenir.

Dans ce contexte, le droit à la protection des données en tant qu'élément essentiel de la politique de l'UE est réaffirmé dans le traité de Lisbonne, ainsi qu'à l'article 8 de la Charte, en tant que droit fondamental de toute personne. L'importance de la protection des données et de la vie privée dans le domaine de la police et de la justice a également été confirmée par la jurisprudence, notamment, pour ne mentionner qu'un cas récent, dans l'arrêt rendu par la Cour européenne des droits de l'homme dans l'affaire S. et Marper concernant l'utilisation de données relatives à l'ADN.

III. La protection des données peut contribuer à l'efficacité du travail de la police

J'aimerais souligner que la sélection des informations avant leur collecte favorise également le travail de la police elle-même, notamment car la démarche consistant à limiter les données et les bases de données est rentable. Par ailleurs, si les informations recueillies sont fondées sur des considérations fiables concernant les besoins effectifs, cela aura une incidence positive sur les informations collectées et

permettra également d'éviter ce qu'on désigne parfois sous le nom de surcharge ou de trop-plein d'informations.

D'une manière plus générale, la protection des données et les besoins de la police vont de pair à divers égards. Je vais en donner quelques exemples:

- La législation relative à la protection des données exige que les données soient exactes et mises à jour. La transparence à l'égard des personnes concernées, exigée au titre de cette législation, peut même contribuer à améliorer l'exactitude des données, à condition que cette transparence ne perturbe pas les enquêtes en cours.

- Un niveau élevé de sécurité est exigé pour protéger les données des citoyens. La récente décision-cadre 2008/977/JAI relative à la protection des données prévoit que "les autorités compétentes mettent en œuvre les mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés". Parmi ces mesures, on pourrait envisager une réaction adéquate ou des sanctions adéquates en cas d'atteintes à la sécurité. Toutes ces questions s'inscrivent dans la perspective de la protection des données. Mais ces mesures ne sont-elles pas également des exigences logiques qui devraient être intégrées dans toute stratégie rationnelle de gestion de l'information?

- Un élément essentiel de la protection des données - même dans le traité de Lisbonne lui-même - est le contrôle externe exercé par les autorités chargées de la protection des données. À mon avis, ce contrôle externe n'est pas destiné à se substituer à la responsabilité et à l'obligation de rendre compte de ses actes au sein des organisations elles-mêmes, mais il peut contribuer à assurer leur niveau élevé. En outre, le contrôle externe peut contribuer à instaurer la confiance.

IV. L'architecture adéquate

Comme cela a déjà été expliqué à plusieurs reprises, il convient avant tout de choisir l'architecture adéquate. Dans ce cadre, le concept de vie privée "intégrée", plus connu sous le nom de "prise en compte du respect de la vie privée dès la conception" ou de

"vie privée par défaut" devrait être pleinement appliqué. Ce concept est actuellement élaboré pour le secteur privé, mais il doit jouer un rôle important dans le domaine de la police et de la justice. Dans mon avis concernant la communication de la Commission dans la perspective du programme de Stockholm, j'ai recommandé qu'il existe une obligation légale pour les constructeurs et les utilisateurs de systèmes d'information d'élaborer et d'utiliser des systèmes respectant le principe de la prise en compte du respect de la vie privée dès la conception.

Pour être plus précis, la prise en compte du respect de la vie privée dès la conception est une notion qui recouvre plusieurs éléments. J'en mentionnerai quelques uns à titre indicatif. Les systèmes de traitement de données devraient être conçus et choisis dans le but de collecter et d'utiliser le moins possible de données à caractère personnel. Ces systèmes devraient fournir aux personnes concernées des moyens de contrôle ciblés. Seuls les entités ou fonctionnaires habilités devraient avoir accès à certaines données à caractère personnel. Les systèmes informatiques susceptibles d'être utilisés pour des tâches ou objectifs différents devraient entièrement séparer les données et les procédures concourant à la réalisation de ces tâches ou objectifs différents.

V. Les résultats: le programme de Stockholm et la stratégie de gestion de l'information

Où en sommes-nous aujourd'hui? Comme nous le savons, et comme nous l'avons entendu aujourd'hui, l'élaboration du programme de Stockholm est à son dernier stade. Le dernier texte publié, en date du 16 octobre 2009, suscite l'espoir que la stratégie de gestion de l'information intègre pleinement la protection des données. Il demande un régime vigoureux de protection des données. En outre, le texte contient des dispositions claires sur la protection des données elles-mêmes, qui devraient être envisagées en liaison avec la stratégie de sécurité et qui doivent aboutir à un cadre juridique solide et global relatif à la protection des données, recouvrant tous les domaines d'activité de l'UE. Le traité de Lisbonne demande également l'instauration d'un tel cadre global.

Le texte souligne que les nouvelles propositions législatives ne devraient être présentées qu'après une préparation minutieuse, comportant notamment des analyses

d'impact permettant de déterminer les besoins et les conséquences financières, et tenant compte des instruments juridiques existants.

Pour conclure, nous envisagerons la situation actuelle de la stratégie de gestion de l'information. Il ne fait aucun doute que la protection des données en fait partie intégrante, ainsi que de nombreux éléments mentionnés précédemment. Pour finir, la question est de savoir si cette intégration est suffisamment solide et si l'intégration de la protection des données dans cette stratégie de sécurité contribuera à - et sera suffisamment efficace pour - équilibrer les besoins en matière de sécurité et de protection des données dans le cadre de l'évaluation de la législation existante dans le domaine de l'utilisation et de l'échange des informations, et dans le cadre de l'élaboration de nouvelles mesures.

Il va de soi qu'il me reste encore à attendre le texte définitif du programme de Stockholm et de la stratégie de gestion de l'information et surtout, à jouer mon rôle dans un avenir proche, lorsque ces deux documents seront mis en œuvre sous forme de mesures concrètes. Dans ce cadre, j'évaluerai bien entendu attentivement le respect et la mise en œuvre en pratique des normes élevées prévues dans la stratégie de gestion de l'information.