Édito

15e colloque Creis-Terminal

Les libertés à l'épreuve de l'informatique : fichage et contrôle social

Ce 15e colloque s'inscrit dans la continuité de l'activité du Creis, devenu récemment Creis-Terminal. Cependant, il nous faut remonter à 1970 pour voir un colloque du Creis consacré spécifiquement au thème très général : informatique, vie privée, libertés.

Depuis lors de nombreux changements se sont produits dans le monde et ce, dans différents domaines.

Evolutions techniques évidemment avec :

❑ le développement des réseaux informatiques et en particulier d'Internet ;

❑ la croissance exponentielle des capacités de stockage des informations et de la puissance de calcul des ordinateurs ;

❑ la mise au point des moteurs de recherche qui permettent de réaliser, de façon quasi instantanée, l'interconnexion à distance de fichiers et de données (à caractère personnel notamment) ;

❑ l'apparition, ces dernières années, de nouvelles applications sur Internet notamment, tels les réseaux sociaux qui permettent de diffuser et d'échanger des informations personnelles dont la confidentialité est loin d'être toujours garantie.

Mais, des changements très importants se sont aussi produits dans le domaine économique, avec une généralisation du processus de mondialisation, ainsi que dans le domaine politique avec le développement, au nom de la lutte contre le terrorisme et la délinquance, de politiques sécuritaires qui vont se concrétiser par la multiplication des applications informatiques de surveillance et de contrôle. À cette occasion, le concept de « prévention » va être systématiquement mis en avant : nécessité de prévenir, de détecter des suspects, des personnes « susceptibles » de commettre un crime ou un délit. Cela induit et alimente une idéologie de la suspicion généralisée.

Notons cependant que la perception des risques d'atteinte à la vie privée (réseaux sociaux et usage des données nominatives à des fins commer-

ciales), tend parfois à occulter les dangers pour les libertés et la démocratie que représentent les applications informatiques, disons plus traditionnelles, qui relèvent du secteur public (police, services de renseignement de l'État, fichiers du secteur social et de la santé ou de l'Éducation nationale…) ou du secteur parapublic (banques, assurances, compagnies aériennes…). Il faut réussir à tenir la balance égale entre les risques d'atteinte à la vie privée, à travers par exemple les réseaux sociaux, et les dangers que représentent les fichiers de données personnelles, publics et parapublics.

Face à cette réalité multiforme et en perpétuel changement, sommes-nous complètement démunis ? Non, si nous nous appuyons sur un certain nombre de lois et de principes fondamentaux qui, évidemment, doivent être actualisés et adaptés en permanence aux évolutions techniques, économiques, politiques et sociales. Il peut en être ainsi :

◆ des principes de « finalité » et de « proportionnalité » qui permettent de limiter la collecte des données personnelles, les destinataires et la durée de conservation de ces données ;

◆ du principe de la « présomption d'innocence » auquel on ne peut substituer le principe de « suspicion » ;

◆ du principe de « transparence » pour les traitements mis en œuvre dans les entreprises et les administrations et le droit à la non-transparence, à l'opacité, à l'anonymat pour les personnes, pour les citoyens.

Il en est ainsi également :

◆ de la « liberté d'information et de communication » ;

◆ de la « liberté d'aller et venir » ;

◆ de la « liberté de choix » qui doit être une liberté effective s'appuyant sur une information honnête et exhaustive. Par exemple, il devrait être possible de sortir d'un réseau social aussi facilement que de s'y inscrire, ce qui n'est pas le cas actuellement (sortir d'un réseau social est un véritable parcours du combattant).

Le respect de ces principes et de ces lois, dont la liste n'est évidemment pas exhaustive, constitue la « pierre de touche » en matière de protection de la vie privée, des libertés et de la démocratie.

Quels sont donc, succinctement, les objectifs de ce colloque ?

Le premier objectif est d'approfondir l'analyse des risques d'atteinte à la vie privée et aux libertés individuelles et publiques que présentent la prolifération, la diversification et la sophistication des traitements informatiques tant au niveau national qu'à l'échelle internationale, en particulier dans le cadre européen.

Un deuxième objectif serait de dégager un certain nombre de pistes d'intervention en direction de différents organismes concernés par les problèmes « Informatique et libertés », tant au niveau national qu'à l'échelle européenne.

Enfin, comment sensibiliser les citoyens à ces problèmes, les jeunes plus particulièrement, pourrait constituer un troisième objectif.

Pour ce colloque 2010, nous avions choisi une organisation qui permette à un maximum de participants d'intervenir et d'animer les débats.

Après chaque communication ou conférence, il était prévu un temps de questions-réponses : comme d'habitude, une dizaine à une quinzaine de minutes, selon le type d'intervention.

Les questions qui ne pouvaient être traitées, ou qui nécessitaient un approfondissement, ont été reprises lors de la dernière demi-journée du colloque, entièrement consacrée au débat. Au cours de ce débat, d'autres problèmes ont été abordés, même s'ils n'ont pas fait l'objet d'une communication ou d'une conférence.

Les résultats de ce débat conclusif font l'objet d'un ensemble de propositions et de recommandations qui ont été publiées dans le numéro 105 de *Terminal*. ■

Félix Paoletti