**Les divergences transatlantiques dans l’exploitation des fichiers privés pour la lutte contre le terrorisme : droit positif et prospective**

Philippe Ch.-A. Guillot

*Professeur de relations internationales à l’École de l’Air*

**Résumé**

Comment les fichiers privés peuvent-ils être exploités par les autorités publiques dans le cadre de la prévention du terrorisme ? Différentes conceptions du bon équilibre entre la liberté individuelle et les mesures sécuritaires opposent d’un côté l’Union européenne et ses États membres qui consacrent la protection des données à caractère personnel comme un droit fondamental et, de l’autre côté, les États-Unis d’Amérique qui font relativement peu de cas du respect de la vie privée en dépit du quatrième Amendement et de la théorie de la *privacy*. La coopération entre l’Europe et les États-Unis en matière de lutte contre le terrorisme doit donc concilier des approches divergentes, voire contradictoires.

La communication, en un premier temps, revient sur les péripéties ayant entouré deux types d’accords euro-américains concernant les fichiers de passagers aériens (*Passenger name Record* – P.N.R.) et ceux des messageries bancaires (*SWIFT-Terrorist Finance Tracking Program*) qui ont donné lieu non seulement à une controverse « transatlantique », mais aussi à un conflit au sein des institutions de l’Union européenne du fait des différences d’appréciation sur les concessions à faire par la Commission et le Conseil, d’une part, et, d’autre part, par la Cour de justice et le Parlement, lesquels s’avèrent d’ardents défenseurs de la protection des données à caractère personnel – opposition qui perdure face au projet de directive visant à créer un P.N.R. européen – alors même que certains États membres ont adopté des mesures permettant à leurs services de sécurité d’avoir accès aux données des passagers aériens, à l’instar du « système API-P.N.R. France ».

En un second temps, la communication élargit la question à l’équilibre à construire dans le cas du recueil de métadonnées auprès des entreprises de communications électroniques et des fournisseurs d’accès à l’internet par certains États membres (notamment la France avec les dispositions de la loi de programmation militaire et de celle relative renseignement), inspiré des pratiques de la *National Security Agency* que le récent *USA Freedom Act* vient pourtant de restreindre, et le droit fondamental à la protection des données personnelles tel qu’interprété par l’arrêt de la Cour de justice *Digital Rights Ireland* & *Seitleinger* du 8 avril 2014.

En guise de conclusion, la communication plaide pour une approche de la lute antiterroriste plus respectueuse de la protection des données personnelles.