

« Circulation transnationale et interception des données sur internet au service des activités de renseignement ».

Maxime KHELOUFI, *communauté juridique*.

Doctorant au Centre de Recherche et de Documentation Européennes et Internationales – Université de Bordeaux.

Actuellement doctorant travaillant sur « *les activités de renseignement et la protection des droits fondamentaux en Europe* », le projet Convergences du Droit et du Numérique a naturellement retenu tout mon intérêt.

En effet, depuis plus d’un an, j’ai eu l’occasion, lors de mes recherches, d’observer qu’au sein même des activités de renseignement, le principal élément déclencheur de bouleversements ces dernières années avait trait au numérique et notamment à la collection et au traitement généralisé de données, ceci permettant ensuite leur transformation en « renseignement » utile à la prise de décision politique, notamment de la part du pouvoir exécutif.

Ce volet très automatisé des activités de renseignement renvoie aux activités de renseignement dites « techniques », par opposition aux activités de renseignement dites « humaines ». Même si cette distinction reste dans une certaine mesure de l’ordre de la théorie, la technique ne pouvant se passer d’interventions humaines, elle trouve toutefois une pertinence pour ce qui concerne les nouveaux enjeux juridiques induits.

La question la plus générale consiste à savoir quel équilibre trouver entre d’une part, l’usage de nouvelles techniques numériques au service du renseignement, ce dernier restant essentiel dans la perspective d’assurer la sécurité d’un Etat et de ses citoyens, et d’autre part, la protection des droits et libertés fondamentaux qu’il convient, dans une société démocratique, de garantir le plus largement possible.

Ces dernières années, on assiste à la construction de cadres juridiques, à la fois nationaux et européens (Union européenne et Conseil de l’Europe), venant poser certaines règles et limites aux activités de renseignement. Toutefois, la technologie numérique, alliée à certains vides juridiques semble permettre un contournement très aisé de ces cadres.

C’est ici qu’une question plus précise apparait et opère le trait d’union entre droit et numérique. **Comment les données circulent-elles sur le réseau internet et peuvent-elles techniquement faire l’objet d’interceptions à l’insu de leur expéditeur et de leur destinataire ?**

Ceci peut être illustré très simplement par l’hypothèse suivante. Un individu A envoie un courriel à son collègue de bureau B. Quel chemin sera emprunté par ce courriel ? Un élément d’extranéité, entendu ici comme un transit par l’étranger, peut-il apparaître ? Le cas échéant, un service de renseignement étranger peut-il techniquement et aisément intercepter ce courriel entre nos deux collègues de bureaux ? Cette problématique étant par la suite renforcée par la possibilité pour le service de renseignement étranger ayant intercepté l’information de la transmettre aux services de renseignement de l’Etat dont les collègues de bureaux sont ressortissants.

Cet aspect technique est particulièrement intéressant pour mes recherches car il permettrait, si tel était le cas, de mettre en lumière un moyen de contournement du cadre juridique existant autour des activités de renseignement. Bien naturellement, cet aspect technique, m’est parfaitement obscur en tant que juriste et les connaissances d’un technicien sur la question seraient les bienvenues. Ceci démontre une nouvelle fois la nécessité pour les chercheurs de collaborer toujours plus afin d’apporter aux autres tout l’éclairage de leurs domaines respectifs. Aussi, je serais très intéressé de pouvoir apporter à un technicien certains éléments de réponse sur des points juridiques pouvant l’intéresser et l’aider dans ses recherches.