Interview de Bertrand Warusfel,

Professeur de droit à l'Université Lille 2 et avocat au barreau de Paris*

♦ SDBR: Le règlement européen sur l'identification électronique vient d'être publié le 28 août dernier au JO de l'UE. Ce nouveau texte représente-t'il une avancée notable dans le domaine de la sécurité numérique?

BW : Oui, car ce règlement du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques, comporte deux volets complémentaires importants. D'un côté, les Etats s'engagent – enfin – à mettre en place des schémas d'identification électronique nationaux qui seront reconnus mutuellement au sein de l'Union européenne. De l'autre côté, ce règlement abroge la directive du 13 décembre 1999 sur les signatures électroniques, laquelle n'avait jamais rencontré le succès escompté, et met en place un nouveau cadre en la matière reposant sur des prestataires de certification (dit « prestataires de services de confiance ») contrôlés par les pouvoirs publics.

♦ En quoi cette évolution, en matière de signature et d'identification électronique, peut-elle renforcer la sécurité numérique en Europe ?

Assurer la sécurité de nos systèmes d'information impose le renforcement de deux instruments. Le premier est d'utiliser des moyens d'identification numérique fiables, qui renforcent à la fois la sécurité juridique des transactions (par l'effet probatoire de la signature électronique) et la sécurité technique (en se prémunissant notamment par l'authentification contre les intrusions). Le règlement va nous y aider et ce sous la responsabilité des Etats qui vont contrôler les prestataires de confiance, alors qu'en 1999 on avait retenu une approche nettement plus libérale dans laquelle les Etats n'intervenaient pas. L'expérience a montré que cela n'a pas fonctionné. Aujourd'hui, on a compris que la question des identités numériques est un sujet trop sensible (y compris pour les libertés publiques et la protection des données personnelles) pour le laisser entièrement entre les mains du marché.

♦ Vous travaillez sur les problématiques de cryptologie depuis 25 ans, quelle est selon vous l'autre volet de la sécurité des systèmes d'information à renforcer ?

C'est l'usage de moyens de chiffrement. En France, comme aux Etats-Unis, nous avons vécu avec une politique publique qui ne faisait, en réalité, rien pour promouvoir le recours à de tels outils, de peur qu'un surarmement cryptographique ne donne un avantage technique aux délinquants et affaiblisse les possibilités de décryptement de nos services de sécurité. Je pense que cette politique défensive, qui a sans doute donné du temps à nos services pour se doter des moyens de renseignement technique nécessaires, est dépassé et que la protection des citoyens et des entreprises contre la cyberdélinquance, tout comme la protection du patrimoine national français contre les interceptions étrangères, impose que l'Etat et les entreprises concernées favorisent une offre légale et fiable de chiffrement des données et des communications.

♦ Est-ce une retombée de l'affaire Snowden ?

D'une certaine manière, oui. Le renforcement du recours à des moyens de chiffrement fiables (c'est-à-dire, qui n'ont pas été affaiblis par des pratiques de type « backdoors ») a d'ailleurs été recommandé par la commission que le Président Obama avait réunie, suite aux révélations de R. Snowden en décembre 2013. Mais c'est aussi le développement rapide du recours au Cloud computing qui impose de disposer de moyens de chiffrement efficaces: on ne peut envisager que chacun accepte de délocaliser ses données professionnelles ou personnelles sans aucune garantie de confidentialité et de contrôle d'accès. Chiffrement et identification électronique vont donc être les deux clés de la sécurité du Cloud.

Suite de l'interview page 3

**FWPA : Cabinet Feltesse Warusfel Pasquier & Associés http://fwpa-avocats.com*

Interview de Bertrand Warusfel,

Professeur de droit à l'Université Lille 2 et avocat au barreau de Paris

♦ **Comment les services de sécurité vont-ils pouvoir continuer à mener leurs enquêtes ou leurs activités de renseignement, nécessaires à la sécurité nationale, dans ce nouveau contexte de renforcement de la sécurité numérique ?**

Cela va passer certainement par la continuation des investissements importants que le contribuable consent à nos services de renseignement et de sécurité, afin de développer leurs capacités de surveillance du cyberespace et de décryptement. Mais cela passe aussi par un mouvement, déjà engagé, qui consiste à s'intéresser plus aux «métadonnées» qu'aux seuls contenus de communication. C'est, par exemple, ce qui a été l'objet de la loi du 28 mars 2014 sur la géolocalisation judiciaire ou bien de l'article 20 de la loi de programmation militaire** de décembre 2013.

♦ **Cet article de la LPM a semé un peu d'émoi à propos des possibilités renforcées de recueil des données de connexion offertes à tous les services de renseignement. Quel est votre point de vue sur le sujet ?**

Je pense qu'il était légitime de renforcer la possibilité pour nos services de renseignement de collecter ces données techniques, mais j'ai regretté – comme d'autres – que la loi n'ait pas donné l'ensemble du contrôle de ces opérations à la Commission nationale de contrôle des interceptions de sécurité. Dans l'état actuel du texte (qui va entrer en vigueur en janvier 2015), seule la géolocalisation «en temps réel» est suivie par la CNCIS, le reste passe toujours par le seul filtre d'une personnalité qualifiée. A mon sens, un renforcement des moyens techniques d'investigation doit aller de pair avec un renforcement de l'encadrement juridique de ces pratiques intrusives, comme le Conseil d'Etat vient de le recommander, dans son nouveau rapport sur «le numérique et les droits fondamentaux». Ce devrait d'ailleurs être la logique de la future loi sur le renseignement qui – je l'espère – verra le jour, maintenant que les travaux de la mission d'information Urvoas-Verchère*** de 2013 ont permis de formuler des propositions assez équilibrées.

♦ **Du côté des entreprises, les pratiques d'intelligence économique ne doivent-elles pas être, elles aussi, encadrées ?**

La situation est nécessairement différente entre les pratiques de l'Etat et celles des entreprises. Dans une démocratie, l'Etat ne peut agir que dans le cadre strict des prérogatives que lui autorise la loi. A l'inverse, dans une économie ouverte, les entreprises doivent pouvoir librement s'informer et travailler tant qu'elles ne violent pas le droit d'autrui (la vie privée, la propriété intellectuelle, les règles de concurrence, par exemple). On a donc échoué à organiser un contrôle public des activités d'intelligence économique. Pour autant, cela ne veut pas dire qu'il ne faille pas poser des limites aux pratiques d'acquisition d'informations. Comme je le répète depuis longtemps en effet, il est trop simpliste de dire – comme le rapport Martre l'avait affirmé en 1994 – que l'intelligence économique est toujours légale puisqu'elle se contente d'exploiter de l'information ouverte.

♦ **De ce point de vue, la relance du projet d'adopter une loi sur le secret des affaires, après la tentative inaboutie de la proposition de loi Carayon en 2012, va-t-elle dans le bon sens ?**

Tout à fait. La nouvelle proposition de loi qui vient d'être déposée, en juillet dernier devant l'Assemblée nationale, sur la protection du secret des affaires pourrait apporter, à mon sens, un complément utile au droit de la sécurité économique des entreprises et de leurs pratiques d'information. D'un côté, cette loi – si elle est adoptée - légitimera la protection par l'entreprise de ses secrets économiques (y compris par les moyens techniques du chiffrement) mais, de l'autre, elle définira les limites des pratiques intrusives à l'encontre de ses concurrents et fixera la frontière entre la collecte licite d'informations ouvertes et l'espionnage économique répréhensible.

Interview réalisée par Alain Establier

*** Cf. Interview de Constant Hardy, Commissaire aux Communications Electroniques de Défense (CCED), dans SDBR n°101 du 11/03/2014*
**** Cf. Interview de Patrice Verchère, député, dans SDBR n°85 du 11/06/2013*