Big Brother

Surveillance : cet article 13 qui entache la loi de programmation militaire

De nombreux acteurs estiment que la protection des libertés individuelles sur Internet est remise en cause

Publié le lundi 09 décembre à 18h26
Par Hugo Sedouramane, Journaliste

@Indixit

Les faits - «Dictature numérique», «Prism à la française», «loi dangereuse»... les experts critiquent la loi de programmation militaire qui devrait être adoptée ce 10 décembre. En cause : une disposition qui élargit la possibilité d'intercepter des communications électroniques sans accord d'un magistrat.

Après l'Assemblée nationale, le Sénat devrait voter ce mardi la loi de programmation militaire 2014-2019. Une loi dont une disposition inquiète de nombreux acteurs de l'écosystème du web et des défenseurs des libertés individuelles, certains allant jusqu'à dénoncer la mise en place d'un système de surveillance généralisé digne du système Prism de la NSA, dont les échos du scandale résonnent toujours. Bien que les termes et le ton employé par les organisations comme la Cnil, le Conseil national du numérique (CNNum) ou l'Association des sites internet communautaires diffèrent, tous les reproches portent sur les dispositifs de surveillance des communications électroniques introduits par l'article 13, qui suppose un élargissement de l'utilisation de ces dispositifs sans autorisation de la part d'un magistrat. Ce sont les agents «chargés de la sécurité intérieure, de la défense, de l'économie et du budget» qui pourront procéder à ce type de surveillance de données géolocalisées, en temps réel. Outre les opérateurs, les hébergeurs de services pourront également être sollicités par les autorités.

Selon Guy Mamou-Mani, qui préside le Syntec Numérique, «la direction prise par ce texte ouvre la voie à un certain nombre d'utilisations quant à la surveillance des donnée sans véritable régulation». S'il ne se reconnaît pas dans les violentes réactions à l'encontre de cette loi, il regrette ne pas avoir été consulté, tout comme la Cnil et le CNNum. «Ce qui il y a dans le texte permet à Bercy d'aller plus loin en matière de surveillance, estime la députée UMP Laure de La Raudière. Il est logique d'étendre le champ des acteurs concernés tant qu'on se restreint à la lutte antiterroriste, mais le

reste relève de l'atteinte aux libertés individuelles. Je suis par exemple choquée de voir le champ d'action élargi à la criminalité organisée. Cela ne met pas forcément la sûreté de l'Etat en jeu.» poursuit-elle. Et d'ajouter qu'il y a «une différence entre une fadette qui contient des informations sur l'état d'une communication et l'interception d'une communication électronique et de son contenu». Certains, comme l'avocat spécialisé dans le numérique Alain Bensoussan, jugent qu'il «était nécessaire de clarifier juridiquement l'accès aux données via la régulation de l'accès aux informations. Par ailleurs, la traçabilité des surveillances permet un contrôle démocratique a posteriori». Car si aux Etats-Unis l'interception des données dépend d'un pouvoir juridictionnel indépendant, ce n'est pas le cas en France.

Autre point contesté dans ce texte, la possibilité d'autoriser «des interceptions de correspondances émises par la voie des communications électroniques ayant pour objet (...) la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France». Pour Nicolas Arpagian, le directeur scientifique du cycle Sécurité numérique à l'Institut national des hautes études de la sécurité et de la justice (INHESJ) «la défense des intérêts économiques de la France était déjà inscrite dans l'ordonnance de 1959 portant sur l'organisation de la Défense. Ce qui n'est pas satisfaisant au sujet de ce texte de loi est qu'il se soit fait sans la Cnil et le CNNum». Il s'étonne également «qu'on ne sache pas comment les entreprises pourront tirer profit des informations récoltées. Il faudrait demander à Fleur Pellerin et Jean-Yves Le Drian s'ils comptent mettre à disposition l'appareil d'Etat au service des entreprises». Quant à la protection des données personnelles : «le modèle de l'économie numérique gratuite se base sur la captation de données personnelles à grande échelle : le consommateur-citoyen a déjà conscience que la notion de confidentialité de ses données est très relative», conclut-il.