Décryptage : le regard de Nicolas Arpagian sur la loi de programmation militaire

Vendredi 13 Juin 2014 - RN

En décembre dernier a été votée la très controversée loi de programmation militaire. Aujourd'hui, Renaissance numérique se penche à nouveau sur ce sujet dans sa note de décryptage mensuelle.

Pour explorer les différents enjeux de cette loi, nous interrogeons tout d'abord Nicolas Arpagian, directeur scientifique du cycle « Sécurité Numérique » de l'Institut National des Hautes Etudes de la Sécurité et de la Justice (INHESJ).

Nicolas ARPAGIAN est le directeur scientifique du cycle « Sécurité Numérique » de l'Institut National des Hautes Etudes de la Sécurité et de la Justice (INHESJ) et le rédacteur en chef de la revue Prospective Stratégique. Retrouvez le sur Twitter : @cyberguerre

La LPM a été votée en décembre dernier sous la contestation de nombreux acteurs du numérique et des défenseurs des droits dénonçant une "société de surveillance". Ces réactions étaient-elles selon vous fondées ?

Tout d'abord, ces réactions sont bienvenues. Leur existence témoigne du fait que la discussion et l'adoption de mesures nouvelles concernant un possible suivi encadré des communications se font ouvertement, sur la place publique. Il n'y a pas de régime de secret ni de législations d'exception qui, comme c'est le cas dans d'autres pays, empêchent de discuter de ces textes dans les médias. Toutefois, le placement de ces articles relatifs au Code de Sécurité Intérieure dans la Loi de Programmation Militaire n'était sans doute pas idéal. Cela a donné une teinte « kaki » à ce dispositif, alors qu'il s'agit bien d'un sujet de la sécurité du quotidien. Ce dernier aurait mérité un texte spécifique, lequel aurait été discuté dès l'origine et au-delà de la seule sphère des connaisseurs de la Défense. C'est une problématique de sécurité des personnes et des biens, à la mesure des systèmes d'information et de l'Internet qui irriguent désormais nos vies personnelles et professionnelles et l'ensemble des organisations civiles, économiques ou militaires.

Ensuite, il est toujours plus souhaitable, quand des outils techniques existent et permettent de conduire des opérations de surveillance des communications, qu'ils soient encadrés par la loi. Il vaut mieux que des modes opératoires soient prévus, décris précisément, et contrôlés par un texte débattu par des élus pour éviter que des pratiques ne se généralisent en dehors de toute règle de droit, au gré des potentiels techniques. Le principe d'un système de surveillance, s'il est défini par la loi et effectué sous l'autorité d'un magistrat n'est pas a priori mauvais ou condamnable. Dans un régime démocratique, les pouvoirs s'équilibrent par une séparation claire et lisible. Dès lors que ces usages sont proportionnés et justifiés par le but à atteindre, pourquoi refuser à des services enquêteurs d'accéder à des technologies pour faire aboutir leurs investigations et conduire des suspects au tribunal ? Selon les circonstances, plusieurs entités (Commission Nationale des Interceptions de Sécurité, Commission Nationale de l'Informatique et des Libertés, Défenseur des droits, magistrats de l'ordre judiciaire ou administratif...) peuvent être saisies par le justiciable qui s'estimerait victime d'une surveillance abusive.

Les opinions publiques sont très exigeantes à l'égard des services de sécurité, notamment face à la menace terroriste. Quelques heures à peine après que Mohamed Merah a commis ses meurtres, les journalistes et les séquences de libre-antenne des médias se tournaient vers les pouvoirs publics en réclamant qu'ils livrent les informations en leur possession sur d'éventuelles menaces visant notre

pays. On ne peut pas exprimer une attente de disposer d'une cartographie complète et à jour des organisations criminelles ou terroristes potentiellement actives sur notre territoire, et dans le même temps refuser aux services de police ou de gendarmerie la possibilité d'intervenir en amont – sous l'autorité d'un juge – pour intercepter les communications numériques ou la navigation Internet de tel ou tel individu au comportement sujet à caution.

Enfin, au nom de quoi interdirait-on par principe à des services de police d'un pays démocratique d'utiliser – sous l'autorité d'un magistrat - des moyens d'investigation fondés sur des outils du quotidien (téléphones mobiles, messageries électroniques…) concernant une minorité de personnes pouvant être impliquées dans des activités illicites? Alors que dans le même temps les équipes marketing et commerciales des fournisseurs d'accès Internet balaient en permanence l'intégralité des e-mails de l'ensemble de leurs utilisateurs. Par exemple, quand Google passe au tamis et archive les courriers électroniques de millions de titulaires de compte Gmail, l'historique de déplacement GPS de millions de détenteurs de téléphones ou tablettes Android, l'intégralité de la navigation Internet des ordinateurs utilisant Chrome, YouTube et autres services, les conditions générales d'utilisation ont-elle été débattues devant un quelconque parlement élu démocratiquement ? Si de telles clauses vous déplaisent, quelle est votre chance de pouvoir vous y soustraire si vous souhaitez utiliser les technologies proposées par Google ou Facebook ? Voyez-vous un magistrat sollicité systématiquement pour valider et encadrer le recours à une telle surveillance généralisée et permanente ?

Si la loi d'un pays démocratique vous déplaît, vous pouvez et devez interpeller votre parlementaire, voire en changer si vous réussissez à mobiliser une majorité d'électeurs en faveur de vos idées. C'est en impliquant le plus grand nombre d'élus sur les sujets relatifs aux évolutions numériques que l'on pourra en faire un sujet largement débattu dans les enceintes politiques et parlementaires et le sortir enfin des cercles professionnels ou corporatistes. Internet est désormais dans la poche de nos compatriotes avec des mobiles ou des connexions haut débit qui se généralisent. Mais on compte sur les doigts de trois mains les parlementaires au Sénat et à l'Assemblée nationale véritablement au fait des questions numériques. Et de leurs enjeux économiques, géopolitiques, juridiques, stratégiques et techniques.

Avec ces nouveaux pouvoirs donnés à l'administration en matière de surveillance, la France se donne-t-elle les moyens de la NSA, mis en lumière par Snowden ?

Aucun Etat moderne ne peut plus se priver d'expertise en matière de sécurité numérique. C'est aussi une condition pour se tenir le plus possible à l'abri des opérations offensives menées par d'autres administrations étrangères. C'est en ayant une culture de l'attaque que l'on peut soigner sa propre sécurité. Par leurs effectifs, leurs moyens financiers et son cadre juridique limité, les moyens mis en œuvre par l'Administration française n'ont rien de commun avec les capacités étatsuniennes en matière de collecte d'informations. En plus, Washington dispose d'alliés de poids avec les industriels du Net comme Google ou Facebook. Lors de la conférence TechCrunch Disrupt de septembre 2013, Marissa Mayer la présidente de Yahoo! a été catégorique : « Ce serait une trahison de désobéir à la NSA ».

Ces entreprises sont donc des alliés de fait et en droit de la puissance économique et stratégique des Etats-Unis. Leur expertise et leur implantation dans le domaine des technologies de l'information constituent un renfort sans équivalent pour les autorités de Washington. Par exemple, le chairman de Google, Eric Schmidt, participe aux côtés de nombreux industriels à l'Office of Science & Technology Policy directement placé à la Maison Blanche. Soit une imbrication public-privé inconnue de notre côté de l'Atlantique. Ce sont donc des situations bien différentes en France et aux Etats-Unis.

Constate-t-on à l'échelle internationale, une réaction post-Snowden des administrations en charge de la surveillance qui, dans différents Etats, chercheraient à renforcer leurs pouvoirs en réponse aux actions de la NSA ? Si oui, sous quelle forme ? La loi de programmation militaire entre-t-elle dans cette logique ?

Un des grands mérites de Snowden a été de faire connaître le programme PRISM dont le champ d'action va bien au-delà de la lutte contre le terrorisme. L'illustration emblématique fut l'annonce de la mise sur écoute du téléphone mobile personnel de Mme Angela Merkel, qui ne pouvait naturellement pas se justifier par une traque contre le terrorisme.

Cela a confirmé que les Etats utilisent bel et bien leurs services de renseignement et leur attirail technologique pour espionner des alliés politiques et que la quête de renseignements économiques et diplomatiques sont des priorités pour tous les gouvernements. Dans ces domaines, il n'y a pas d'allié : chaque gouvernement veut défendre ses intérêts et ceux des entreprises qui emploient des salariés et paient des impôts sur son territoire. Le volume des données collectées, tel qu'il a été détaillé par Snowden, témoigne de l'ampleur de la captation des informations. Il est donc cohérent que les gouvernements tentent de s'en prémunir. Reste à savoir s'ils en ont les moyens en période budgétaire contrainte et dès lors qu'ils ne disposent pas dans leur propre pays de technologies de substitution. A ce titre, on peut regretter la capacité très limitée des Européens à être des acteurs du marché numérique. Malgré sa puissance financière et intellectuelle, l'Europe se contente largement du rôle d'utilisateur de technologies développées par d'autres, tandis que les Chinois ont su créer de toutes pièces des poids lourds comme Alibaba dans l'e-commerce, le moteur de recherche Baidu ou le site de micro-blogging Weibo. Idem pour les Russes qui, avec Yandex disposent d'une alternative nationale aux grands moteurs de recherche étatsuniens. La taille de la population ou la langue pratiquée ne sont pas des explications convaincantes quand on constate que les quelque dix millions de Tchèques ont su créer avec Seznam.cz un moteur de recherche national dont les audiences rivalisent les multinationales du Net. Les annonces de Snowden ont suscité l'émergence d'un débat sur la question stratégique de la souveraineté technologique. Il ne faudrait pas qu'il reste sans

effet.

France / US : quels éléments de comparaison serait-il pertinent de relever pour comprendre le fonctionnement de notre administration dans son activité de surveillance (par rapport à celle américaine) ?

Pour commencer la France ne dispose pas de capacités d'écoute de l'ampleur de celles décrites par Snowden. Nous ne sommes pas dans une mécanique d'interception des échanges d'un très grand nombre de personnes, sur de longues durées et sur une large variété de supports (téléphone, mobile, Internet…). Ensuite, la France ne fait pas partie d'alliances techniques de dimension planétaire, telle Echelon qui rassemble entre autres les Etats-Unis, le Canada, le Royaume-Uni, l'Australie ou la Nouvelle-Zélande. Enfin, des procédures légales encadrent et limitent les écoutes administratives et judiciaires. Ce qui restreint les éventuelles velléités de surveillance tous azimuts ou en continu.

Avec PRISM, la frontière qui existe entre le monde économique et celui de l'Administration a de facto disparu. Nous avons ainsi appris à cette occasion que le Droit des Etats-Unis s'applique à une entreprise, quelle que soit sa localisation géographique, dès lors que plus de la moitié de son actionnariat est de nationalité étatsunienne. Dis-moi qui est ton actionnaire majoritaire, je te dirai à quelles lois tu es soumis. Cela montre bien que même dans la sphère numérique, la notion d'intérêt national est très vivace. C'est donc la nationalité de l'actionnaire qui en l'espèce détermine le droit applicable, en dehors de toute considération pour la localisation géographique.

Disposons-nous en France de contre-pouvoirs suffisants pour exiger à l'Etat français de rendre des comptes sur ses actions de luttes contre le terrorisme en ligne (mise sous surveillance, blocage de contenus, etc.) ? Si non, quelles instances pourraient être chargées de ce rôle ?

Il faut que le sujet de la sécurité numérique soit discuté auprès de l'opinion publique, laquelle ne doit pas se comporter en simple consommatrice passive des technologies. La généralisation de l'enseignement du code informatique fait partie de cette ré-appropriation de l'outil informatique par les citoyens. Il y a quelques années, j'avais écrit dans un ouvrage que « *c'est en sachant ce que l'on risque de perdre sur la Toile que l'on peut entreprendre de sécuriser nos données sensibles* ». Depuis, les modes de connexion se sont multipliés et les sources de captation d'informations se sont généralisées. Cette connaissance permet de rendre tangible dans les esprits la notion de surveillance numérique. Ensuite il est indispensable que l'Etat dispose d'un moyen d'évaluation neutre et fiable de la menace numérique. La mesure de celle-ci, et la communication sur de prétendues statistiques d'attaques informatiques, émanent encore très largement des seuls éditeurs et fournisseurs de solutions commerciales. La légitimité de dispositifs de sécurité se justifie par leur proportionnalité de la menace. C'est en disposant d'une photographie la plus précise possible des offensives et de la criminalité numériques que l'on pourra justifier le principe des technologies de surveillance, avec toujours en tête un principe de juste proportionnalité.

Cela suppose que les victimes (particuliers, entreprises, administrations…) transmettent à l'Etat – en l'occurrence l'ANSSI est l'organe ad hoc – les descriptifs des attaques subies afin que la cartographie soit la plus complète possible, même si le caractère souvent indolore des intrusions informatiques rend l'idée d'exhaustivité illusoire. En effet, la cible ignore souvent qu'elle a fait l'objet d'un vol ou d'une altération de ses données dans son système d'information.

Les médias ont certainement un rôle utile et souhaitable pour susciter le débat sur la place et l'usage des technologies afin de garder au cœur des discussions le principe de juste équilibre entre les principes de liberté et de surveillance. Dans une démarche encore plus structurée, des associations comme La Quadrature du Net, le French Data Network (FDN) ou l'Electronic Frontier Foundation (EFF) sont désormais des parties prenantes incontournables pour nourrir la réflexion politique sur les enjeux de société liés au numérique. On constate également la réactivité grandissante d'instances comme la Commission Nationale Informatique et Libertés (CNIL) ou le Conseil National du Numérique (CNNum) qui sont des lieux où se discutent les sujets qui mêlent le Droit, l'économie et la technologie. Enfin, des parlementaires n'hésitent plus à suivre ces thématiques, alors même qu'elles sont encore- et c'est regrettable – d'un apport électoral quasi nul. Là encore, il revient à chaque citoyen-électeur de solliciter l'avis de son élu, ou son candidat, sur ces équipements techniques qui peuplent nos existences, bousculent nos modèles économiques et transforment nos modes d'appréciation du monde qui nous entoure… et accessoirement peuvent restreindre, si l'on n'y prend pas garde, le champ de nos libertés individuelles à la portion congrue.

Article Précédent Article Suivant

COMMENTEZ