Voltairenet.org Réseau Voltaire

LOI DE PROGRAMMATION MILITAIRE

L'État français est-il en guerre contre les Français ?

par Jean-Claude Paye

La loi de programmation militaire française étend les pouvoirs des Armées à la « *la prévention de la criminalité* ». Ce faisant, elle abroge, sur le modèle de ce qu'ont fait les États-Unis après le 11-Septembre, la distinction classique entre défense et sécurité intérieure, entre armée et police. Du coup, elle soumet les citoyens français à un régime de surveillance autrefois réservé à des agents d'une puissance étrangère.

RÉSEAU VOLTAIRE | BRUXELLES (BELGIQUE) | 26 MARS 2014

Jean-Yves Le Drian (ministre de la Défense) et Manuel Valls (ministre de l'Intérieur)

L'espionnage massif de ses citoyens par les services secrets d'un pays est aujourd'hui devenu la norme. À la faveur de la « *lutte contre le terrorisme* », la notion de guerre s'est introduite dans le Code pénal de l'ensemble des pays occidentaux. La dernière loi française de programmation militaire, qui vient d'être promulguée le 19 décembre 2013 [1], s'inscrit dans cette tendance de fusion du droit pénal et du droit de la guerre.

Elle illustre une évolution du droit occidental qui, tout en concentrant l'ensemble des pouvoirs aux mains de l'Exécutif, place l'exception à la place de la norme et pose l'anomie comme base de reconstruction d'un nouvel ordre de droit. Cette mutation enregistre la fin d'une organisation, propre à la forme nationale de l'État, basée sur l'articulation de deux systèmes relativement séparés, État de droit à l'intérieur du pays et violence pure à l'extérieur.

Une loi militaire comme « prévention de la criminalité »

La loi de programmation militaire sert habituellement à encadrer les budgets des forces militaires de l'Hexagone. Cette année, elle sort du cadre de la défense pour englober « *la lutte contre le crime* ». Portant diverses dispositions, concernant à la fois la Défense et la Sécurité nationale, elle comprend un article 20 (l'ancien article 13) qui étend les pouvoirs de surveillance des autorités administratives françaises à « *la prévention de la criminalité* », fusionnant ainsi droit de la guerre et droit pénal en généralisant la tendance déjà imprimée par la lutte « *antiterroriste* » à l'ensemble du champ pénal. En visant génériquement la « *prévention de la criminalité* », ce régime s'appliquera à toutes les infractions. En soumettant les citoyens français à un régime de surveillance autrefois réservé à des agents d'une puissance étrangère, la loi ne sépare plus intérieur et extérieur de la nation et ne distingue plus infraction pénale et gestion de l'hostilité. Ce processus omniprésent n'est pas seulement identifiable à l'intérieur du pays, mais aussi au niveau des conflits internationaux. Les engagements de la France en Libye et en Syrie procèdent à une indifférenciation entre action de guerre et fonction de police. La guerre n'est plus engagée, afin de se défendre ou de procéder à une conquête, mais pour « *punir un dictateur* ».

Afin de procéder à cette fusion du pénal et du militaire, la loi de programmation évince le pouvoir judiciaire et concentre les

pouvoirs aux mains de l'exécutif. Non seulement le troisième pouvoir est totalement contourné, mais le seul dispositif de contrôle *a posteriori* (Commission de contrôle des écoutes et interceptions) relevant de l'Exécutif ne pourra émettre qu'une « *recommandation* » au Premier ministre .

La collecte de données porte sur les numéros de téléphone, les adresses IP, ou les listes de contact de correspondants téléphoniques, ainsi que sur les données de géolocalisation en temps réel. Seulement dans ce dernier cas, l'autorisation préalable du Juge des libertés ou de la CNCIS, l'autorité de contrôle relevant du pouvoir Exécutif, reste nécessaire.

Ainsi, l'article 20 de la loi donne à l'administration le droit de collecter, en temps réel, sans recours à un juge et même sans autorisation préalable de l'organe administratif de contrôle, des informations sur les utilisateurs de réseaux de communication. Des agents individuellement désignés, relevant des ministères de la Défense, de l'Intérieur, de l'Économie et du Budget, ainsi que des « *chargés de mission* », peuvent désormais accéder directement aux données. La loi étend également le droit de regard à toutes informations et aux documents stockés par l'hébergeur et plus seulement aux données techniques.

De plus, les administrations vont pouvoir exiger des données pour des motifs très larges, notamment ceux prévus à l'article 241-2 du Code de la sécurité intérieure, c'est-à-dire concernant : « *la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées* »

Ainsi, l'article 20, qui entrera en vigueur en janvier 2015, permet la capture en temps réel sur simple demande administrative, sur « *sollicitation du réseau* », des informations et documents traités dans ceux-ci et non plus seulement les données de connexion des utilisateurs . La collecte directe d'informations se fera, non seulement auprès des fournisseurs d'accès (FAI et opérateurs de télécommunication), mais aussi auprès de tous les hébergeurs et fournisseurs de services en ligne. Aucune disposition ne limite le volume des collectes. Celles-ci pourraient passer par l'installation

directe de dispositifs de capture de signaux ou de données chez les opérateurs et les hébergeurs. L'inscription des termes « *sollicitation du réseau* » signifie que les autorités souhaitent donner un cadre juridique à une interconnexion directe. Cette loi rend également permanents des dispositifs qui n'étaient que temporaires. Si cette loi française peut être comparée aux dispositions du *Patriot Act* états-unien [2], on doit alors faire référence au *Patriot Act Improvement and Reautorisation Act of 2005* [3], promulguée en 2006 et qui rend permanentes les mesures temporaires prises immédiatement après les attentats du 11 septembre 2001.

Une loi martiale numérique

Le pouvoir Exécutif a toujours soutenu que la nouvelle loi ne portait aucunement sur le contenu des messages interceptés, mais uniquement sur les données de connexion. Cette lecture a été démentie par la CNIL qui, à la suite de la promulgation de la loi de programmation militaire, a déploré l'adoption de certaines mesures d'accès aux données personnelles prévues par son article 20. Elle a tout d'abord à nouveau regretté de ne pas avoir été saisie sur cet article lors de l'examen du projet de loi. Elle déplore surtout que « *la rédaction définitive du texte et que le recours à la notion très vague d'informations et documents traités ou conservés par les réseaux ou services de communications électroniques, semble permettre aux services de renseignement d'avoir accès aux données de contenu, et non pas seulement aux données de connexion.* »

L'article, entré en vigueur dès janvier 2014, confie au Premier ministre le soin de conduire l'action du Gouvernement en matière de sécurité de l'information, en s'appuyant sur les services de l'ANSSI (Autorité Nationale de Sécurité des Systèmes d'Information). Il crée surtout un pouvoir de contre-attaque, aussi étendu que flou, qui autorise l'État à pirater des serveurs ennemis lorsque « *le potentiel de guerre ou économique, la sécurité, ou la capacité de survie de la Nation* » sont attaqués.

La loi ne définit pas ce qu'est une cybermenace et ne précise pas l'autorité compétente pour déterminer ce qui constitue une atteinte au « *potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation* ». Avec une terminologie aussi large, cette législation pourrait, par exemple, s'attaquer à une manifestation organisée et diffusée a travers les réseaux sociaux.

Quant à l'article 22, il crée une obligation, pour les FAI, hébergeurs et autres opérateurs dont les infrastructures sont considérées d'importance vitale pour le pays, de mettre en place à leurs frais. des outils de « *détection des événements susceptibles d'affecter la sécurité de leurs systèmes d'information* ». Ces outils étant exploités par des tiers certifiés ou par les services de l'État lui-même, la loi autorise, dans les faits, le pouvoir Exécutif à installer des sondes qu'il contrôle directement ou indirectement.

L'article 23 renforce l'insécurité juridique pour les auteurs ou vendeurs de logiciels qui pourraient permettre l'interception de données. Jusqu'à présent, l'article 226-3 du Code pénal interdisait les appareils ou dispositifs « *conçus pour* » intercepter des correspondances privées ou des données informatiques. Maintenant, seront interdits les dispositifs « *de nature à* » réaliser de telles infractions. L'intention ne sera plus à rechercher, seul le résultat , même accidentel, pourra compter.

Quant à l'article 23 bis, il donne accès aux fichiers d'abonnés à l'ANSSI qui pourra obtenir les coordonnées de tout abonné, hébergeur ou éditeur de site internet « *pour les besoins de la prévention des atteintes aux systèmes de traitement automatisé* » ou si l'agence estime que son système informatique est ou peut seulement être sujet à des attaques. L'ANSSI pourrait par exemple se faire communiquer les identités de tous les internautes dont les ordinateurs sont vulnérables, et identifier des cibles pour exploiter ces failles pour les propres besoins de la défense nationale.

Grâce à cette loi, les Français sont soumis à des procédures qui relevaient autrefois de la mise sous surveillance d'agents d'une puissance ennemie. Cette dernière législation n'est cependant que la dernière péripétie d'un ensemble de mesures débutant avec la loi d'Orientation et de Programmation de la Sécurité Intérieure (LOPSI

1), définitivement adopté le 29 août 2002 [4]. Cette législation permet déjà l'accès à distance de la police aux données conservées par les opérateurs et les fournisseurs d'accès Internet. Quant à la LOPPSI 2 [5], définitivement adoptée le 8 février 2011, elle permet de filtrer progressivement le Net et de légaliser l'introduction de mouchards (chevaux de Troie) au sein des ordinateurs privés.

Jean-Claude Paye

---

[1] « Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale », *Journal officiel de la République française* n°0294 du 19 décembre 2013, page 20570.

[2] « Final text of the Patriot Act ».

[3] H.R. 3199, Téléchargeable

[4] « Loi n° 2002-1094 du 29 août 2002 d'orientation et de programmation pour la sécurité intérieure, *Journal officiel de la République française*, Version consolidée au 01 mai 2012.

[5] La loi dite « LOPSI 2 », Loi d'Orientation et de Programmation pour la performance de la Sécurité Intérieure, fait suite à « LOPSI 1 » que Nicolas Sarkozy avait fait adopter en 2002 lorsqu'il était ministre de l'Intérieur. Cf. *Journal officiel de la République française* n°0062 du 15 mars 2011, page 4582.

Source : « L'État français est-il en guerre contre les Français ? », par Jean-Claude Paye, *Réseau Voltaire*, 26 mars 2014, www.voltairenet.org/article182979.html