FUSION DU DROIT DE LA GUERRE ET DU DROIT PÉNAL : FRANCE, ÉTATS-UNIS

JEAN-CLAUDE PAYE *

En France, la dernière loi de programmation militaire déborde le champ de la guerre pour empiéter sur le domaine pénal, car elle a aussi pour objet « la prévention du crime ». Afin de réaliser cet objectif, elle installe une surveillance générale des citoyens. Cette fusion du droit pénal et du droit de la guerre crée un état martial numérique. La loi donne au pouvoir exécutif, en l'absence de tout contrôle* a priori *et* a posteriori, *des pouvoirs lui permettant une capture, en temps réel, non seulement des données de connexion téléphoniques ou informatiques, mais aussi du contenu des messages. Le pouvoir soumet ainsi les citoyens à des mesures qui autrefois relevaient de la surveillance d'agents d'un État ennemi.

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. Le plus souvent, il ne s'agit là que d'un premier pas conduisant à une fusion entre droit pénal et droit de la guerre. L'espionnage massif de ses citoyens par les services secrets d'un pays est aujourd'hui devenu la norme. Cependant, les révélations de Snowden en ce qui concerne les opérations de la NSA ne font que mettre en lumière une surveillance généralisée déjà légalisée.

Malgré l'indignation provoquée dans l'Hexagone par la mise en exergue des pratiques des agences de renseignement américaines, les chambres françaises viennent d'adopter, à travers leur vote de la dernière loi de programmation militaire, des dispositions permettant des pratiques similaires à celles de la NSA, à savoir l'espionnage massif par les agences de renseignement de leurs propres nationaux.

* SOCIOLOGUE
Auteur de *L'Emprise de l'image - De Guantanamo à Tarnac,* éditions Yves Michel, 2012.

L'anticipation étasunienne

Les États-Unis ont anticipé les législations européennes. Ainsi, la section 215 du Patriot Act[1], un texte voté le 26 octobre 2001 pour définir le cadre législatif de la guerre contre le terrorisme, a, pour une période limitée dans le temps, établi que la collecte et la surveillance des communications pouvaient se faire sans mandat ni ordonnance judiciaire. Ces dispositions ont été votées sous la forme d'un amendement à la loi FISA[2], initialement adoptée en 1978 pour fixer un cadre à l'espionnage des communications privées. Ici aussi, c'est sur la base d'une loi destinée à « *encadrer le renseignement* », que les procédures d'espionnage ont été étendues à l'ensemble des citoyens américains.

Le point de vue du gouvernement des États-Unis, considérant que les attentats du 11 septembre sont un acte de guerre et pas seulement un crime, s'appuie sur une résolution du Congrès du 18 septembre 2001, The Authorization for Use of Military Force, qui donne des pouvoirs spéciaux à l'exécutif. Le texte stipule « que le président est autorisé à utiliser tous les moyens nécessaires et appropriés contre les nations, organisations ou personnes qu'il désigne comme avoir planifié, autorisé, commis ou avoir aidé les attaques terroristes qui se sont déroulées le 11 septembre 2001 »[3].

La lecture que fait l'administration de cette résolution est celle d'un État qui est en guerre, non pas contre d'autres nations, mais contre des organisations non liées à un gouvernement étranger ou contre de simples individus. Cette interprétation redéfinit la notion de guerre. Elle lui donne un caractère asymétrique, celle d'une « *lutte à mort* » entre la super puissance mondiale et des personnes désignées comme ennemies des États-Unis. Ce nouveau concept s'affranchit de l'existence de toute menace réelle sur la nation américaine. Il est un pur produit de la subjectivité du pouvoir : l'état de guerre existe de par son énonciation.

---

[1] Texte de loi disponible sur <http://politechbot.com/docs/usa.act.final.102401.html>.

[2] Le Foreign Intelligence and Security Act de 1978 établit une cour spéciale chargée d'autoriser des opérations de surveillance « *d'agents d'un pouvoir étranger* ». Il s'agit d'une cour secrète composée de 11 magistrats désignés par le ministre de la Justice, *Electronic Privacy Information Center*, <http://www.epic.org/privacy/terrorism/fisa/>.

[3] US Congress' joint resolution of September 18, 2001 Authorization for Use of Military Force (« AUMF ») ; public law 107-40, 115 Stat. 224.

Temporaires, dans le Patriot Act voté au lendemain du 11 septembre 2001, ces mesures ont ouvert la voie à l'actuelle surveillance à grande échelle des communications mondiales par les États-Unis, dont celles internes au territoire américain. Elles sont devenues illimitées dans le temps, grâce à l'adoption du « Patriot Act Improvement and Reauthorization Act of 2005 »[4] qui a renouvelé l'ensemble des dispositions prises après les attentats et rendu permanentes celles qui avaient un caractère temporaire.

Un jugement comme déni de l'inconstitutionnalité

Ces mesures demeurent cependant en opposition avec le 4e amendement de la Constitution des États-Unis qui protège les citoyens américains des perquisitions et des saisies non motivées. Cette protection, pour être effective, requiert un mandat, ainsi qu'une justification pour toute capture de données[5]. C'est cette contradiction que dénie la décision, du 27 décembre 2013 rendue par le juge William H. Pauley de la Cour fédérale de New York, stipulant que la collecte massive de données téléphoniques par la NSA était légale[6]. Selon le juge, cette surveillance généralisée serait justifiée par la lutte contre Al Quaïda. S'appuyant inconditionnellement sur le témoignage de hauts fonctionnaires de l'administration Obama, il estime que si la NSA avait recouru à son actuel programme de surveillance électronique avant le 11 septembre 2001, les attentats n'auraient pas eu lieu.

Le juge Pauley cite, en l'approuvant, le témoignage du directeur adjoint du FBI, Sean Joyce, disant : « Notre mission est de mettre un terme au terrorisme, de le stopper. Pas après coup, mais de l'empêcher avant qu'il se produise aux États-Unis. Et je peux

[4] H.R. 3199, <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f :h3199enr.txt.pdf>.

[5] 4e amendement : « Le droit des citoyens d'être garantis dans leurs personne, domicile, papiers et effets, contre les perquisitions et saisies non motivées ne sera pas violé, et aucun mandat ne sera délivré, si ce n'est sur présomption sérieuse, corroborée par serment ou affirmation, ni sans qu'il décrive particulièrement le lieu à fouiller et les personnes ou les choses à saisir. »

[6] Sari Horwitz, « NSA collection of phone is lawful, federal judge rules », *The Washington Post,* le 27 décembre 2013, <http://www.washingtonpost.com/world/national-security/nsa-collection-of-phone-data-is-lawful-federal-judge-rules/2013/12/27/4b99d96a-6f19-11e3-a523-fe73f0ff6b8d_story.html>.

vous dire que tous les instruments sont essentiels et vitaux. Et les instruments tels que je vous les expose et l'utilisation qui en est faite actuellement ont été précieux pour déjouer certains de ces complots. Vous dites "comment peut-on déterminer la valeur d'une vie américaine ?" Et je peux vous répondre qu'elle n'a pas de prix. »[7]

Pour le juge, la collecte de données est légale grâce à l'article 215 du Patriot Act. Le rôle de la loi est alors renversé. Le Foreign Intelligence Surveillance Act (FISA) donnant une apparence de réglementation aux agences de renseignement, est transformé en un blanc-seing autorisant l'espionnage des populations étasuniennes. Cette lecture de l'article 215 opère d'abord un déplacement du rôle des agences de renseignement, de leur mission de contre-espionnage à la surveillance globale des citoyens américains, puis procède à un renversement de la fonction de la loi, de son rôle traditionnel de réglementation de l'action de l'exécutif, à celui de légitimation d'un pouvoir absolu.

Le jugement opère une fusion entre populations et pouvoir et enlève ainsi toute possibilité de conflit entre les droits des citoyens et les intérêts de l'État. Afin d'appuyer la thèse selon laquelle la défense des droits démocratiques peut être laissée aux mains de l'armée et des agences de renseignement, le magistrat cite le rapport de la commission d'enquête sur les attentats du 11 septembre : « Le choix entre la liberté et la sécurité est un faux choix, puisque rien n'est plus propre à mettre en péril les libertés civiles qu'un attentat terroriste sur le sol américain. » Le juge Pauley affirme aussi que, chaque fois qu'une personne utilise un téléphone, elle abandonne « *volontairement* » ses droits à la vie privée. Il intime alors de faire confiance au gouvernement sans questionner son action et affirme que si le gouvernement s'attaque aux libertés, il doit avoir de bonnes raisons pour le faire.

Insécurité juridique

En rapport avec les écoutes généralisées, les cours étasuniennes peuvent se prononcer en sens divers. Le jugement du tribunal fédéral de New York est une réaction au verdict rendu, le 16 décembre 2013, par le juge du district de Washington, Richard Leon[8].

---

[7] American Civil Liberties Union against James R. Clapper, United States District Court Southern District of New York, p. 49, <http://apps.washingtonpost.com/g/documents/world/us-district-judge-pauleys-ruling-in-aclu-vs-clapper/723/>.

[8] Ellen Nakashima and Ann E. Marimow, « Judge : NSA's collecting of phone records is probably unconstitutional », *The Washington Post,* le

Dans son prononcé, le juge Leon a qualifié de « presque orwelliennes » les opérations massives d'espionnage dans lesquelles l'Agence de sécurité nationale (NSA) collecte et emmagasine les données de pratiquement tous les appels téléphoniques aux États-Unis, locaux ou internationaux. Il affirme : « Je ne peux imaginer une invasion plus arbitraire que cette collecte hautement sophistiquée de données personnelles sur pratiquement tous les citoyens dans le but de les consulter et de les analyser sans mandat des tribunaux. »[9]

De manière encore plus significative, le juge a rejeté la justification de la guerre contre le terrorisme invoquée par les administrations Obama et Bush pour légitimer toutes les attaques contre les droits démocratiques. Le juge Leon a fait remarquer que le gouvernement n'a pas cité « un seul cas où l'analyse de toutes les métadonnées recueillies par la NSA aurait vraiment permis de contrecarrer une attaque terroriste imminente ».

Cependant, si le verdict stipule que les pratiques de la NSA violent avec une « quasi-certitude » les droits démocratiques fondamentaux garantis par le quatrième amendement de la Constitution des États-Unis, le magistrat n'a rien fait concrètement pour empêcher l'espionnage anticonstitutionnel de la NSA. Ainsi, malgré ses conclusions, le juge Leon, « étant donné les intérêts importants de sécurité nationale en jeu dans ce cas », a accepté de suspendre l'ordonnance d'injonction contre les opérations d'espionnage de la NSA, en attendant l'appel du gouvernement. Cette procédure pourrait prendre des années avant de se retrouver devant la cour suprême.

France : la loi de programmation militaire

La dernière loi française de programmation militaire, promulguée le 19 décembre 2013[10], s'inscrit dans la tendance initiée aux États-Unis. Elle illustre une évolution du droit occidental qui, tout en concentrant l'ensemble des pouvoirs aux mains de l'exécutif, pose l'anomie comme base de reconstruction d'un nouvel ordre juridique.

16 décembre 2013, <http://www.washingtonpost.com/national/judge-nsas-collecting-of-phone-records-is-likely-unconstitutional/2013/12/16/6e098eda-6688-11e3-a0b9-249bbb34602c_story.html>.

[9] *Ibidem.*

[10] <http://www.legifrance.gouv.fr/affichTexte.do ;jsessionid=?cidTexte=JORFTEXT000028338825&dateTexte=&oldAction=dernierJO&categorieLien=id>.

En France, 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 qui étend les pouvoirs de surveillance des autorités administratives françaises à « la prévention de la criminalité. » Ainsi, en généralisant la tendance déjà imprimée par la lutte « antiterroriste, » cet article fusionne droit de la guerre et droit pénal. En visant génériquement la « *prévention de la criminalité* », cette procédure ne s'appliquera pas seulement au terrorisme, mais 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. L'engagement de la France en Libye procède 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 « protéger les populations d'un tyran. » Il en est de même en ce qui concerne la Syrie. Suite au massacre chimique de Damas, attribué aux troupes loyalistes, l'entourage du président Hollande, envisageant une intervention limitée, avait fait état de « la grande détermination de la France à réagir et à ne pas laisser ces crimes impunis »[11].

Une fusion du militaire et du pénal

Afin de procéder à la 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, la Commission nationale de contrôle des interceptions de sécurité (CNCIS) 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 contacts de correspondants téléphoniques, ainsi que sur les données de géolocalisation en temps réel. Seulement

[11] Réforme pénale, Syrie, pression fiscale… Hollande s'explique dans *Le Monde*, *Le Monde.fr* | 30.08.2013, <http://www.lemonde.fr/politique/article/2013/08/30/hollande-au-monde-le-massacre-de-damas-ne-peut-ni-ne-doit-rester-impuni_3468851_823448.html>.

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 des informations sur les utilisateurs de réseaux de communication, sans recours à un juge et sans autorisation préalable de l'organe administratif de contrôle. 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 tous 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 ».

Saisie des données en temps réel

L'article 20, qui entrera en vigueur en janvier 2015, permet la capture en temps réel sur simple demande administrative, par « *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 américain, on doit alors faire référence au Patriot Act Improvement and Reauthorisation Act de 2006 qui rend permanentes les mesures temporaires prises immédiatement après les attentats du 11 septembre 2001.

En opérant un déni de l'extension, à la fois dans l'espace et le temps, des procédures utilisées, les défenseurs de la loi soutiennent que la nouvelle législation ne fait qu'inscrire et rationaliser des

dispositifs déjà existants, notamment ceux de la loi du 23 janvier 2006 relative à la lutte contre le terrorisme qui, dans un cadre plus limité, permet également des interceptions de données. De manière générale, la concentration des pouvoirs aux mains de l'exécutif et la neutralisation du pouvoir judiciaire sont justifiées au nom d'une interprétation pervertie de la loi qui identifie la collecte d'informations, par la police et par des agences de renseignement, avec la phase d'enquête d'une procédure judiciaire. Autrefois, l'instruction relevait de l'initiative et du contrôle du troisième pouvoir, avant que la notion « d'enquête préliminaire » écorne déjà ce principe, en donnant des pouvoirs accrus à la police et au procureur de la République, un magistrat relié directement au pouvoir exécutif.

Capture des données de connexion et des contenus

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 Commission nationale informatique et libertés (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 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 semblent permettre aux services de renseignement d'avoir accès aux données de contenu, et non pas seulement aux données de connexion. »[12]

Ce n'est pas uniquement l'article 20 qui pose problème, mais aussi le 21 qui est entré en vigueur dès janvier 2014. Il 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'Autorité nationale de sécurité des systèmes d'information (ANSSI). 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. Ainsi, l'article 21 de la loi stipule que : « Pour répondre à une attaque informatique qui vise les systèmes d'information affectant le potentiel de guerre

[12] <http://www.01net.com/editorial/610724/loi-de-programmation-militaire-la-cnil-deplore-lacces-possible-aux-contenus/>.

ou économique, la sécurité ou la capacité de survie de la Nation, les services de l'État peuvent, dans les conditions fixées par le Premier ministre, procéder aux opérations techniques nécessaires à la caractérisation de l'attaque et à la neutralisation de ses effets en accédant aux systèmes d'information qui sont à l'origine de l'attaque ».

Cybermenace et guerre virtuelle

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 permettrait de s'attaquer, par exemple, à une manifestation organisée et diffusée à travers les réseaux sociaux.

La politique des États-Unis est éclairante en ce qui concerne les possibilités offertes par l'utilisation de telles notions. Les termes de cyberguerre et de cyberterrorisme sont centraux dans le discours du gouvernement américain. Le déclenchement de la guerre en Irak avait déjà permis une inflation de déclarations alarmistes. Tom Ridge, secrétaire à la Sécurité intérieure, avait annoncé que son département allait « surveiller Internet pour déceler tout signe éventuel d'attaque terroriste, de cyberterrorisme, de piratage et de guerre de l'information opérée entre les États »[13]. Pour lui, les cyberterroristes sont aussi dangereux que les terroristes : « Nous n'opérerons aucune distinction entre virtuel et physique au sein de ce département », a-t-il affirmé.

L'article 21 de la loi de programmation militaire autorise une telle indifférenciation entre le réel et le virtuel. La menace existe car, simplement, elle est nommée comme telle et permet alors de mettre en place une batterie de mesures limitant les libertés collectives et individuelles, comme les collectes d'information ou le piratage de systèmes informatiques privés.

Un État martial numérique

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

[13] Declan McCullagh, "Perspective : Cyberterror and Professional Paranoiacs", CNET *News.com*, March 21, 2003. <http://news.com.com/Cyberterror+and+professional+paranoiacs/2010-1071_3-993594.html>.

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.

Se posant comme une loi martiale numérique, devant faire face à un état de guerre permanente, l'article 22 permet au Premier ministre de faire couper un serveur, de dérouter des données vers des routes spécifiques, ou même de faire participer les opérateurs à des contre-attaques. Cependant, seules les mesures liées spécifiquement à la sécurité des systèmes d'information pourront être ordonnées sans contrôle judiciaire.

Quant à l'article 23 bis de la loi, il dispose que « les agents de l'autorité nationale de sécurité des systèmes d'information, habilités par le Premier ministre et assermentés dans des conditions fixées par décret en Conseil d'État, peuvent obtenir des opérateurs de communications électroniques, en application du III de l'article L. 34-1 du Code des postes et des communications électroniques, l'identité, l'adresse postale et l'adresse électronique d'utilisateurs ou de détenteurs de systèmes d'information vulnérables, menacés ou attaqués ».

Ainsi, la loi donne à l'Autorité nationale de sécurité des systèmes d'information accès aux fichiers d'abonnés. L'agence pourra obtenir les coordonnées de tout hébergeur, éditeur ou abonné de site Internet « pour les besoins de la prévention des atteintes aux systèmes de traitement automatisé. » En théorie, l'ANSSI pourrait, par exemple, se faire communiquer les identités de tous les internautes dont les ordinateurs sont vulnérables et identifier des cibles afin d'exploiter ces failles pour les besoins de la défense nationale.

La France en guerre contre ses citoyens ?

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 adoptées le 29 août 2002 [14]. Cette législation permet déjà l'accès à distance de la police aux données conservées par les

[14] Loi n° 2002-1094 du 29 août 2002 d'orientation et de programmation pour la sécurité intérieure, <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000780288>.

opérateurs et les fournisseurs d'accès Internet. Par rapport à la Loi sur la sécurité quotidienne de 2001 [15], elle permet de dépasser le passage obligé par une réquisition adressée à un opérateur de télécommunications. Formellement, cette étape impose une vérification par le pouvoir judiciaire de la légalité de la requête adressée à un opérateur. Cet impératif, qui nécessite une commission rogatoire, impose le respect de la procédure d'instruction et permet d'éventuels recours contre la mesure ordonnée. En abandonnant la nécessité de recourir à une demande du pouvoir judiciaire, la loi de 2002 constituait un pas important dans l'orientation de l'enquête policière vers le travail de renseignement. Quant à la LOPPSI 2 [16], définitivement adoptée le 8 février 2011, elle permet de filtrer progressivement le Net et légalise l'introduction de mouchards (chevaux de Troie) au sein des ordinateurs privés.

La dernière loi française de programmation militaire s'inscrit dans cette tendance qui confond intérieur et extérieur de la nation. En fusionnant défense nationale et « *prévention de la criminalité* », elle installe des mesures de surveillance générale appliquant aux citoyens des procédures qui relevaient auparavant du seul contre-espionnage. Il s'agit d'imposer aux populations des procédures qui, autrefois, étaient uniquement utilisées vis-à-vis d'agents d'une puissance ennemie et d'inscrire ces mesures dans le droit, c'est à dire d'obtenir le consentement des citoyens. Le rôle de la loi est alors renversé. Au lieu de délimiter l'action de la puissance publique, elle enregistre simplement l'absence de limites à l'exercice du pouvoir exécutif.

Le citoyen ennemi de l'État : base d'un nouvel ordre de droit

En France, la notion d'ennemi n'est pas encore, comme aux États-Unis, explicitement introduite dans le droit pénal. Cependant, elle fonctionne déjà à l'état pratique à travers des législations comme la LOPSI 1 et 2 et la loi de programmation militaire.

---

[15] Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne, <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000222052>.

[16] La loi dite LOPSI 2 », Loi d'Orientation et de Programmation pour la performance de la Sécurité Intérieure, fait suite à « LOPSI 1 » que Sarkozy avait fait adopter en 2002 lorsqu'il était ministre de l'Intérieur, <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023707312&categorieLien=id>.

Aux États-Unis, de nombreuses dispositions de surveillance installées par le Patriot Act ont d'abord pris une forme provisoire. Justifiées au nom de l'existence d'un état de guerre, elles furent votées afin d'être appliquées pendant une période limitée. C'est seulement dans un deuxième temps, lors de leur renouvellement, qu'elles furent adoptées comme des mesures n'ayant plus de limite temporelle.

En France, les dispositions adoptées prennent immédiatement un caractère permanent. Elles ne se réfèrent plus à un état d'urgence, mais directement à un état de guerre permanente, bien que, contrairement aux États-Unis, la notion d'hostilité ne fasse pas encore formellement partie du droit pénal.

Aux États-Unis, l'insertion de l'hostilité dans l'ordre juridique intérieur étasunien s'est d'abord effectuée par des actes administratifs justifiés au nom de l'état d'urgence. Cependant, dès 2006, le Military Commissions Act of 2006[17] inscrit la notion de guerre dans la loi pénale et dans la permanence. Il transforme ainsi cette notion en permettant au président des États-Unis de désigner comme ennemis ses propres nationaux, ainsi que tout ressortissant d'un pays avec lequel les États-Unis ne sont pas en guerre. Cette loi crée un droit purement subjectif et donne au pouvoir exécutif des prérogatives de magistrat. L'administration peut désigner toute personne comme « *ennemi combattant* », nommer les juges militaires et déterminer le niveau de coercition des interrogatoires.

Le 28 octobre 2009, le président Obama a signé le Military Commissions Act of 2009[18]. La nouvelle loi ne parle plus « *d'ennemi combattant illégal »,* mais bien d'« ennemi belligérant non protégé ». Ce qui élargit le champ de l'incrimination, car elle ne porte plus uniquement sur des combattants, mais sur « *des personnes qui sont engagées dans un conflit contre les États-Unis* ». La nouvelle définition permet de s'attaquer directement non seulement à des personnes capturées en rapport à un engagement armé, mais à des individus qui posent des actes ou émettent des paroles de solidarité vis-à-vis de ceux qui s'opposent à l'armée étasunienne ou simplement à la politique guerrière du gouvernement.

[17] <http://www.govtrack.us/data/us/bills.text/109/s/s3930.pdf>.

[18] Il s'agit du Titre XVIII du « National Defense Authorization Act for Fiscal Year 2010 », <http://www.defense.gov/news/commissionsacts.html>.