USA : de l'état d'urgence à l'état d'exception permanent

(par Jean-Claude Paye)

29 mars 2008

Le 11 Septembre n'aura été qu'un prétexte pour suspendre temporairement, puis définitivement, de nombreuses libertés publiques et individuelles aux États-Unis. Le sociologue Jean-Claude Paye analyse le renouvellement du *Patriot Act*, les dispositions maintenues et celles qui ont été amendées. Il montre que les procédures dérogatoires adoptées dans la panique des attentats de New York et Washington sont devenues permanentes sans soulever d'amples contestations. Cette évolution ne prendra pas fin avec le mandat de George W. Bush, elle n'est d'ailleurs pas fondamentalement remise en cause par les candidats à sa succession.

Le renouvellement du *Patriot Act* a permis d'inscrire dans la durée des mesures qui, lors de leur première adoption en 2001, furent justifiées par une situation d'urgence. Les dispositions d'exception prises par le gouvernement états-unien, après les attentats du 11 septembre 2001, se fondent sur le vote du Congrès stipulant : « que le Président est autorisé à utiliser toutes les forces nécessaires et appropriées contre les nations, organisations ou personnes qui ont planifiés, autorisés, commis ou aidés les attaques terroristes survenues le 11 septembre 2001.... » [1]

C'est ainsi que le *Patriot Act* autorise l'incarcération, sans procès ni inculpation, pour une durée indéterminée d'étrangers soupçonnés de terrorisme, tout en installant une surveillance généralisée de la population. Certaines de ces mesures de contrôle sont permanentes, d'autres furent votées pour une période de quatre ans. Ces dernières, contenues dans 16 articles, venaient à expiration fin 2005 [2]. Pour pouvoir être prolongées, elles devaient faire l'objet d'un vote des deux Chambres autorisant leur réinstallation.

Le Patriot Act Reauthorization

Si le *Patriot Act* fût voté très rapidement, ce ne fût pas le cas de son renouvellement. Le président George Bush ne put signer « *The Patriot Act Improvement and Reauthorization Act* [3] que le 9 mars 2006. C'est au niveau du Sénat que la résistance s'est organisée, des sénateurs ayant même pratiqué la procédure du « flibustier », qui consiste à prendre et garder la parole pour empêcher tout vote. Pourtant, si ce processus interminable a permis, pour la première fois, une discussion parlementaire sur le contenu et les enjeux de la loi, le projet gouvernemental finira par être adopté. Les dispositions contenues dans le *Patriot Act* ont pour effet d'augmenter considérablement les pouvoirs de l'exécutif et principalement ceux du FBI. Les quelques aménagements apportés, à travers la procédure de renouvellement de la loi, sont loin de rétablir l'équilibre en faveur du pouvoir judiciaire. Les opposants au *Patriot Act* voulaient installer des mesures de contrôle garantissant les libertés individuelles, tandis que le gouvernement voulait profiter de ce vote pour augmenter les prérogatives du FBI. Les discussions se déroulèrent pendant une dizaine de mois, mais le gouvernement est parvenu à éviter que les dispositions permanentes soit réinstallées avec des contrôles judiciaires contraignants et a fait transformer 14 des mesures temporaires, adoptées en 2001 comme procédures d'urgence, en dispositions permanentes.

Est prolongé, l'article 213, une procédure permanente qui installe des techniques d'enquêtes très intrusives, dénommées « sneak and peek ». Il autorise le FBI à pénétrer dans un domicile ou un bureau en l'absence de l'occupant. Durant cette enquête secrète, les agents fédéraux sont autorisés à prendre des photos, à examiner le disque dur d'un ordinateur et à y insérer un dispositif digital d'espionnage, dénommé « lanterne magique ». Une fois installé, ce système enregistre toute activité informatique, sans que celle-ci soit transmise sur le Net. Cette possibilité existe déjà dans la procédure criminelle classique, mais elle est alors soumise à l'autorisation d'un tribunal et les agents doivent notifier immédiatement la procédure à la personne concernée. Avec le *Patriot Act*, la notification fut reportée à trois mois ou plus, si un tribunal l'autorise. De plus, le gouvernement avait la possibilité de reporter indéfiniment celle-ci pour des raisons de « sécurité nationale ». L'accord, pris lors de la procédure de renouvellement, fut de fixer impérativement ce délai à 30 jours [4].

Une autre procédure permanente est prorogée, celle installée par la clause 505, qui élargit les possibilités, accordées au FBI et à des administrations, d'obtenir des « lettres de sécurité nationale », une forme de citation administrative donnant accès à des données personnelles, médicales, financières, aux données des agences de voyage, de location de voitures et des casinos, ainsi qu'aux fichiers de bibliothèques [5]. Avant le *Patriot Act*, les « lettres de sécurité nationales » étaient limités aux cas de personnes « en liaison avec un pouvoir étranger ». La section 505 étend la capacité du FBI d'obtenir une telle autorisation en dehors de ce cadre. Le champs d'utilisation de cette procédure est ainsi largement étendu à toute activité criminelle. Lors des débats parlementaires, il est apparu que le gouvernement utilise 30 000 « lettres de sécurité nationale », chaque année depuis les attentats du 11 septembre. [6]

Un état d'urgence permanent

Les mesures contenues dans les articles 212 et 214 étaient temporaires et sont devenues permanentes. L'article 212 autorise les compagnies de téléphone et les fournisseurs d'accès Internet à divulguer, au gouvernement, le contenu et l'enregistrement des communications, si ces compagnies estiment qu'elles présentent un danger de mort ou qu'elles constituent une « injure grave. » Il n'y a pas de contrôle judiciaire, tel qu'un examen par un tribunal des résultats de la transmission d'informations par l'opérateur. Il n'y a pas non plus de notification de cette transmission à la personne concernée. Ces informations pourront être utilisées dans des enquêtes criminelles et pas seulement en matière de terrorisme.

La section 214 facilite l'obtention par le FBI, dans le cadre du *Foreign Intelligence and Security Act* de 1978, des données de connexions électroniques entrantes et sortantes. Cette saisie ne nécessite pas de mandat judiciaire. Avant le *Patriot Act*, le gouvernement devait prouver que la personne surveillée était un agent d'une puissance étrangère. Maintenant, il doit simplement signifier que l'information saisie est en « relation » avec une enquête relative au terrorisme. Le caractère vague de cette qualification permet de justifier n'importe quelle recherche.

L'article 209 est également devenu permanent. Il élargit la capacité de se saisir légalement de messages vocaux. Avant le *Patriot Act*, capturer de tels messages sur un répondeur installé dans un domicile nécessitait un mandat judiciaire. Les messages vocaux envoyés par un fournisseur de services nécessitait l'ordonnance d'un tribunal. De telles autorisations offrent plus de protections qu'un simple mandat de recherche qui est accordé sur sur la notification qu'« présomption raisonnable permet de penser qu'un délit va être commis ».

La section 209 amende la loi afin de traiter les messages vocaux comme de simples messages électroniques. Ainsi, la possibilité de saisie a été considérablement étendue. Tout procureur a la possibilité, a tout moment, d'accorder une telle autorisation. Si la saisie est effectuée sur des messages envoyés, et non sur un répondeur placé dans un domicile, elle peut être effectuée sans notification à la personne concernée.

L'article 218, devenu également permanent, autorise des recherches secrètes, sans notification, dans un domicile ou un bureau, si il y a une une « présomption raisonnable » de penser que le domicile ou le bureau contienne des informations relatives à l'activité d'un agent d'une puissance étrangère, sans qu'il y ait nécessairement la preuve ou l'indice d'un délit. Les agents obtiennent un mandat d'une cour secrète, mise en place par le FISA [7] Avant le *Patriot Act*, les agents fédéraux devaient certifier que l'objectif premier de la recherche portait sur l'obtention de renseignements en rapport avec l'étranger. L'article 218 abaisse ce standard, puisque les agents doivent seulement déclarer que la saisie d'informations en connexion avec l'étranger est un « objectif significatif » de la recherche. [8]

L'article 207 porte de 30 jours à 6 mois, avec des possibilités de renouvellement pouvant aller jusque un an, le temps pendant lequel des connections, en matière de renseignement en liaison avec l'étranger, peuvent être utilisées, avant qu'une autorisation doive être demandée à un tribunal. Cette disposition est aussi devenue permanente, tout comme celle contenue dans l'article 216, qui permet, à un juge fédéral ou à un magistrat d'une autre juridiction, de délivrer un mandat permettant d'enregistrer les données, entrantes et sortantes, d'une connection électronique, mandat qui ne précise pas le n° IP concerné et qui peut être délivré partout sur le territoire états-unien.

Il s'agit d'un véritable un chèque en blanc donné aux agents fédéraux. Pour obtenir l'autorisation, l'agent doit simplement certifier que l'information recherchée est « pertinente dans la recherche d'un crime en exécution ». Le juge doit délivrer l'autorisation, dès réception de l'attestation, même si il n'est pas d'accord avec la procédure engagée.

Identité entre travail de renseignement et enquête criminelle

La procédure de renouvellement du *Patriot Act* a aussi permis de prolonger pour quatre ans la section 6001 de l'*Intelligence Reform and Terrorism Prevention Act* of 2004, qui autorise une surveillance de personnes isolées, soupçonnées d'être des terroristes [9] Ces individus sont désignés comme « loups solitaires ». Ils feraient partie du terrorisme international, mais agiraient seuls. Cet article redéfinit la notion « d'agent d'un pouvoir étranger » en incluant, dans celle-ci, les personnes engagées dans « le terrorisme international » ou dans des « activités terroristes en préparation ». Ainsi, pour être considéré comme un agent d'une puissance étrangère, il n'est plus nécessaire d'être en liaison avec un tel pouvoir. Cette disposition s'applique aux personnes ne disposant pas de la nationalité américaine.

Sont prolongées pour une nouvelle période de quatre ans, les mesures contenues dans les articles 215 et 206 du *Patriot Act*. La section 215 permet, moyennant une autorisation secrète d'un tribunal, au FBI d'avoir accès aux données médicales, aux comptes bancaires, aux données d'emprunt des bibliothèques ou de « toute chose tangible », sans qu'il soit nécessaire, pour les enquêteurs, de montrer que cette recherche porte sur des faits en connexion avec le terrorisme ou avec une puissance extérieure. Si le FBI doit préciser que l'ordonnance est demandée pour une enquête en matière de renseignement extérieur ou de terrorisme, il ne doit pas établir une qu'il existe une « présomption raisonnable » de l'existence d'un rapport entre les enregistrements demandés et une puissance étrangère.

Les personnes concernées ne pouvaient parler à personne à propos de cette action. L'accord intervenu leur permet de mettre en question cette procédure après un délai d'un an. Il y est ainsi introduit un processus formel de contestation qui n'existait pas auparavant. Cependant, le gouvernement a la possibilité d'empêcher cette procédure pour des raisons de sécurité nationale [10]

Quant à l'article 206, il autorise l'utilisation de connexions « nomades ». Les agents du FBI n'ont pas besoin d'identifier le suspect pour obtenir l'autorisation d'installer leur dispositif de surveillance des communications. Est installée une connexion « sous couverture » à l'ensemble des téléphones installés dans le voisinage de la personne ciblée ou à ceux de ses relations, sans qu'il soit nécessaire de montrer que l'individu surveillé utilise ces appareils. Cela explique pourquoi, un tel dispositif est appelé connexion « John Doe ». Ne devant pas nommer la personne devant être surveillée, le gouvernement peut légalement surveiller le téléphone de n'importe quel individu, sans avoir à montrer que ce dernier est en relation, d'une manière ou d'une autre, avec une puissance étrangère, avec le terrorisme ou même en rapport avec une quelconque activité criminelle.

Avant le *Patriot Act*, les connexions « nomades » étaient utilisables uniquement dans des investigations criminelles, y compris en matière de terrorisme, mais n'étaient pas permises dans des investigations en matière de renseignement. L'enquête criminelle comprend une série de mesures de sauvegarde en matière de protection de la vie privée. Une telle connexion doit spécifier l'identité de la personne surveillée ou le téléphone posé sous surveillance. Pour passer d'un appareil à un autre, le gouvernement doit s'assurer que l'objectif identifié par le mandat utilise actuellement cet appareil. Avec le *Patriot Act*, les connexions nomades, qui passent d'un appareil à un autre, sont autorisées en matière de renseignement, comme enquêtes sous FISA, sans inclure ces mesures de protection.

Le *Patriot Act*, notamment à travers les articles 206 et 215, généralise, à l'ensemble des matières criminelles, des dispositions établies, en matière d'espionnage, par le *Foreing Intelligence Surveillance Act* de 1978. Cette dernière loi, donne dans ces matières des pouvoirs exceptionnels à l'administration, en soustrayant ses actes à un véritable contrôle judiciaire, autre que l'autorisation, préalable et sans suivi, de tribunaux d'exception, souvent secrets.

Le *Patriot Act* estompe la différence entre enquête criminelle et travail de renseignement en permettant au FBI de conduire des recherches sous le Titre III (matière criminelle) et d'obtenir les autorisations nécessaires sous les procédures et avec les garanties réduites du FISA. Il a aussi créé des autorisations permanentes pour l'échange d'informations entre agences de renseignement et services de police, permettant de dépasser les barrières administratives empêchant de telles connexions. L'article 905 autorise le ministre de la Justice (Attorney Général) à saisir le directeur du National Intelligence afin de fournir des preuves obtenues par des procédures de renseignement, telles les recherches sous couverture, à une procédure judiciaire. L'article 504 autorise le transfert de renseignements FISA vers les divisions criminelles. [11] Le département de la Justice a admis avoir envoyé environ 4 500 dossiers FISA vers la division criminelle. Le nombre de poursuites engagées est inconnu [12].

Le renouvellement du *Patriot Act* permet d'inscrire dans la durée des mesures qui, lors de leur première adoption en 2001, furent justifiées par une situation d'urgence. En devenant permanentes, ces mesures de surveillance intrusives deviennent la base d'un nouvel ordre politique qui donne à l'administration des prérogatives revenant au pouvoir judiciaire. Cependant, contrairement à la première version, votée par la Chambre en juin 2005, la forme juridique adoptée reste celle de l'état d'exception permanent et non directement celle de la dictature. La résistance du Sénat a permis de garder et d'introduire quelques possibilités formelles de contrôle et de recours judiciaires, sans que celles-ci entament réellement les prérogatives du FBI et du gouvernement.

Jean-Claude Paye

Jean-Claude Paye est sociologue. Derniers ouvrages publiés : La Fin de l'État de droit, La Dispute 2004 ; Global War on Liberty, Telos Press 2007.

---

[1] Authorization for Use of Military force, Pub. L. 107-40, &&1-2, 115 Stat. 224.

[2] « USA Patriot Act Sunset », Electronic Privacy Information Center.

[3] H.R. 3199, version finale.

[4] Sen.John E. Senunu, « Patriot Act deal balances liberty, security, Washington Memo, February, 12, 2006.

[5] « National Security Letters and your Privacy », ACLU.

[6] Idem.

[7] 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'un Cour secrète composée de 11 magistrats désignés par le ministre de la Justice. Source : Electronic Privacy Information Center.

[8] « Memo to interested Persons Outlining What Congress Should Do About the Patriot Act Sunsets », ACLU, March, 28, 2005.

[9] Intelligence Reform and Terrorism Prevention Act of 2004 ; « Lone Wolf » Amendement to the Foreign Intelligence Surveillance Act.

[10] « Conyers calls Patriot Act reauthorization 'dangerous' », February, 28, 2006,

[11] Kate Martin, « Why Section 203 and 905 Should be Modified », American Bar Association's Patriot Debates,

[12] Oversight answers, submitted by Jamie E. Brown, Acting Assistant Attorney General, May 13, 2003, on file with the House Judiciary Committee.