

» USA Patriot Act

Dans le cadre du cours de Mme Preuss-Laussinotte

22 février 2005

ou l'avènement des prédictions d'Orwell...

LA loi symboliquement baptisée **USA Patriot Act** et adoptée le 25 octobre 2001 presque sans discussion au Congrès, illustre le débat récurrent entre sécurité et liberté.

Depuis le 11 septembre 2001, le pouvoir administratif a incontestablement empiété sur le judiciaire, car c'est dans véritable contexte de terreur politique et de guerre que l'administration Bush vient empiéter sur les libertés individuelles au travers de l'« *arme guidée de laser* » (John Ashcroft, Ministre de la Justice) qu'est le Patriot Act [1].

Là où Paul Auster voit une atteinte à la liberté d'expression, « *les moyens mis en oeuvre pour contrer la menace islamiste engendrent des situations sans précédent sur le plan du droit* » [2].

La version finale de la loi antiterroriste et dont les applications en matière de surveillance sur le Net sont inquiétantes a été adoptée par la Chambre des représentants, *The Uniting and Strengthening America By Providing Appropriate Tools Required To Intercept and Obstruct Terrorism* [3], cette loi a été votée à une écrasante majorité (seul Russ Feingold, Démocrate contre+ 1 abstention + 98 pour) à la suite des attentats du 11 septembre 2001.

La loi antiterroriste autorise notamment la mise sur écoute de tout appareil de communication utilisé par toute personne en rapport, de près ou de loin, avec un présumé terroriste. Elle prévoit également que toute intrusion non-autorisée dans un système informatique pourra être assimilé à un "acte terroriste" [4].

La loi confirme l'autorisation accordée au FBI d'installer un logiciel de surveillance, nommé **Carnivore** (DS 1000), chez les FAI, afin d'épier la circulation des messages électroniques et de conserver les traces de la navigation sur le Web de toute personne suspectée de contact avec une puissance étrangère.

Pour ce faire, seul l'aval d'une juridiction spéciale, dont les activités sont confidentielles, est nécessaire. Le texte de la loi allonge également la liste des informations que les enquêteurs peuvent exiger des FAI sans l'aval d'un juge.

Il autorise également ces derniers à remettre aux autorités, de leur propre initiative, des informations qui ne sont pas relatives au contenu, telle la navigation sur le Web.

Fin novembre 2003, le **Patriot Act II**, précédemment le *Domestic Security Enhancement Act*, le Congrès a encore accru les pouvoirs du FBI.

Un nouvel amendement facilite l'utilisation des *National Security Letters* (LSN), qui permettent à l'agence fédérale de requérir de FAI ou de sites Web des informations personnelles sur les internautes, sans aucun contrôle judiciaire.

Le nouveau texte supprime notamment l'obligation pour le FBI de soumettre chaque année au Congrès un rapport sur l'utilisation de ces NSL.

Les sénateurs, lors du vote de l'amendement ont souligné que l'extension du recours à ce type d'ordre administratif remet en question l'équilibre des pouvoirs au sein des institutions américaines.

Il peut aussi retirer aux américains leur citoyenneté s'ils participent à toute aide étendue à toute organisation qui a été étiquetée comme « terroriste » même sans leur connaissance [5] .

Janvier 2004 : Le Président Bush a demandé au Congrès de rendre permanent le Patriot Act (« vital »), alors que celui-ci devient caduc en 2005.

Les associations de défense de libertés individuelles ont immédiatement dénoncé cette démarche insistant sur les dérives auxquelles a déjà donné lieu cette loi provisoire (ACLU « *American Civil Liberties Union* » = le président « *joue sur les peurs des Américains pour justifier la prolongation de loi antiterroriste* » .

Le Ministre de la Justice, **John Ashcroft** (un des principaux défenseurs du Patriot Act) s'est lancé en août 2003 dans une tournée dans trois Etats afin de convaincre de la nécessité d'appliquer la loi antiterroriste afin de calmer les critiques de plus en plus virulentes.

En novembre 2003, il a annoncé la mise en place de nouvelles procédures incitant le FBI à appliquer de manière plus efficace le Patriot Act ; elles donnent notamment au FBI (agence gouvernementale) le pouvoir de récolter des informations sur des internautes hors de toute enquête officielle et de s'engager ainsi dans une surveillance a priori du réseau Internet.

Des sénateurs démocrates et républicains ont réagi face aux atteintes aux libertés individuelles. Le sénateur républicain Larry Craig a transmis au Congrès en octobre 2003, une proposition de loi, *The Security and Freedom Ensured Act (SAFE)* qui annule certaines mesures du Patriot Act.

Cet amendement revient à la situation antérieure à septembre 2001 concernant la saisie d'informations dans les bases de données des bibliothèques et des ordinateurs sur les lieux de travail, remettant en place les garde-fous nécessaires à la protection des données personnelles= l'administration Bush semble déterminée à s'opposer à l'adoption du SAFE Act (ministre Justice appelle au vote contre).

En septembre 2003, deux associations (lobby) américaines (ACLU et le CDT *Center for Democracy and Technology*) ont entamé une action contre l'application de cette loi.

Dans l'attente de la décision, rendue le 28 septembre 2004 par le **Juge Marrero** du District de New York, le procureur général a accepté de suspendre l'envoi des ses ordres de blocage.

Le gouvernement américain en votant pour cette loi libéricide atteint aux libertés des américains mais vient semer le trouble car les Etats-Unis deviennent un modèle pour les états répressifs qui se targuent d'adopter des lois similaires.

Néanmoins, Washington se targue d'être le héraut de la liberté d'expression sur Internet, lançant de nouveaux programmes pour lutter contre la censure au niveau mondial (*Global Internet Freedom Act*, juin 2003 a pour objectif de lutter contre la censure de l'Internet mise en place par des régimes répressifs comme la Chine, elle prévoit la création d'un bureau de la liberté de l'Internet (*Office of Global Internet Freedom*)).

I- LES ATTEINTES AUX LIBERTES INDIVIDUELLES

« *La plupart des Américains sont prêts à restreindre leurs libertés si, en échange, le gouvernement leur assure de pouvoir rentrer chez eux sans risque chaque soir pour embrasser leurs enfants* » (banquier).

Depuis le 11 septembre, des bases de données contenant des informations et des dizaines de milliers de citoyens ordinaires ont été récupéré par des agents fédéraux

désireux de collecter le moindres informations susceptible de les aider dans la lutte contre le terrorisme (listes supermarché, listings de voyages, plongeurs sous-marins de San Francisco ville progressiste = siège de l'EFF *Electronic Frontier Foundation* qui a toujours protesté contre les abus du gouvernement) et même des informations issues de bases de données publiques !

Il semble qu'aucune activité ne soit exclue du champ d'investigation de l'Etat Américain dans une atmosphère où la sécurité est devenue prioritaire (sondages= beaucoup sont disposé à tolérer une surveillance accrue ou des contraintes plus élevées en matière de logiciel de chiffrement) [6].

Mais les défenseurs des libertés publiques et privées s'inquiètent de cet accroissement des pouvoirs d'investigation et de la bonne volonté montrée par les citoyens ; cela a réduit sans nécessité la liberté des personnes innocentes en menaçant les droits constitutionnels au respect de la vie privée et à la liberté d'expression.

Car même si aucune limitation n'est explicite, la peur des représailles aurait un effet inhibant sur les comportements publics (aucun soutien massif de la population) (choix entre terrorisme et l'abus des sources d'informations).

Le FBI a forcé l'ACLU à censurer un paragraphe sur son site qui indiquait quelles informations le FBI est autorisé à exiger sous le couvert du Patriot Act !!!

A- Comment le Patriot Act contourne le contrôle judiciaire et réduit les protections en matière criminelle

Droits susceptibles d'être violés :

1er amendement : liberté de religion, de parole, de réunion et e la presse.

4ème amendement : droit de ne pas subir des recherches et des saisies déraisonnables.

5ème amendement : nul individu ne peut être privé de sa vie, de sa liberté ou de ses biens sans un procès équitable.

6ème amendement : droit à un procès public rapide par un jury impartial, le droit d'être informé des éléments de l'accusation, le droit de confronter les témoins et d'assistance juridique.

8ème amendement : pas de détention arbitraire ou cruelle ni de condamnation exceptionnelle.

14ème amendement : tous les individus (citoyens américains ou non) résidant aux EU ont droit à un procès équitable et une égale protection par la loi.

Le critère de la « probable cause of crime » disparaît :

Le FBI disposait déjà d'un grand pouvoir en matière de surveillance des communications sur Internet et le téléphone : les écoutes peuvent être faites en cas de crimes impliqués dans une attaque terroriste : désormais, ces écoutes peuvent avoir lieu pour les autres crimes.

Le FBI a également l'autorisation d'intercepter des communications sans « cause sérieuse » de crime entrant dans le champ d'application du *Foreign Intelligence Surveillance Act* (FISA) de 1978.

Dans cette loi (FISA), une « *intelligence surveillance* » devait être préalablement autorisée par la Cour FISA dont les juges sont nommés par l'article 3 de la Constitution, désormais=champ libre ?

Définition : « *Foreign intelligence information* » = 2 aspects

a) toute information qui porte ou concerne un citoyen américain ou un résident permanent légal est nécessaire afin de protéger les Etats-Unis d'attaques hostiles ou de pouvoirs étrangers, de sabotage ou de terrorisme international, ou de renseignements secrets par ces derniers.

b) toute information portant sur des pouvoirs étrangers ou qui concerne un citoyen américain ou un résident permanent légal aux fins de la sécurité nationale ou la poursuite des affaires étrangères

Un citoyen américain n'est pas un « agent des pouvoirs étrangers » (*agent of a foreign power*) sauf si il ou elle s'engage volontairement dans des activités clandestines violant la loi, s'engage dans un sabotage ou dans le terrorisme international pour le compte d'un pays étranger, entre aux EU sous une fausse identité ou aide une autre personne à le faire.

Le **4ème amendement** de la constitution exige que le gouvernement prouve l'existence au juge d'une « *probable cause of crime* » avant de rechercher les éléments à charge.

Cette disposition venait assurer que les écoutes et les mandats de recherches sont strictement appliqués aux personnes « *likely to be involved in a criminal activity* » [7].

L'article 218 amende le FISA afin que le FBI puisse secrètement conduire des recherches physiques ou sur écoutes afin de prouver l'existence d'un crime et ce même sans urgence : cette disposition s'applique même aux citoyens américains.

L'article 215 donne autorisation aux agents du FBI à obtenir à travers tout les pays un order de la cour FISA ou de tout juge fédéral, et permettant d'obtenir des informations en rapport avec la lutte contre le terrorisme ou contre les activités clandestines : informations très sensibles peuvent être collectées (dossier médical, santé mentale, docs financiers, vidéos louées, empreintes, échantillons ADN à partir de cheveux, contrats de travail, drogues, données d'immigration).

Cet article n'était pas nécessaire car d'une part, le FBI avait accès à la plupart de ces informations et d'autre part, il existait des lois et règlements en matière de vie privée, notamment le *Financial Privacy Act*, mais qui posaient des garde-fous pour certaines données sensibles en exigeant une notification (« *notice* ») aux personnes dont le domicile a été fouillé ou dont les communications ont été interceptées.

Le juge n'exerce aucun pouvoir discrétionnaire : il doit délivrer cet « *order* » sur présentation par le FBI d'une demande affirmant que ces enregistrements sont collectés dans un but d'enquête contre le terrorisme international (« *for a foreign intelligence investigation* »).

Or le critère (« *standard* ») pour obtenir une autorisation d'écoute sous le FISA est moins exigeant qu'en matière criminelle classique !!

Article 216= critères minimaux et inadaptés pour l'accès aux communications sur Internet= il change la loi en substance.

Loi ancienne : un agent mandaté peut recevoir un « *pen register or trap and trace order* » (commission rogatoire) pour obtenir de la compagnie de telephone les numéros appels entrants et sortants d'un poste désigné.

Pour l'obtenir (« *order* »)= l'agent doit simplement certifier que l'information à obtenir est « *pertinente dans la recherche d'un crime en cours d'exécution* » (très faible degré d'exigence « *level of proof* » = bien moins que le degré de « *probable cause* » qu'un crime a été, est commis ou est sur le point d'être commis).

Article 216= le juge doit délivrer l' « *order* » dès réception de l'attestation (« certification »), même s'il n'est pas d'accord et qu'il est certain que les agents ne trouveront pas d'informations pertinentes : il doit le délivrer= le juge n'est alors plus le protecteur de la vie privée.

Sous cet article, les autorisations de recherches portent désormais sur les « *dialing, routing and signaling* information » sans toutefois définir exactement les termes mais portent clairement sur les communications Internet qui sont bien plus intéressantes que de simples numéros d'appel !!! Cette définition vague devrait vraisemblablement s'appliquer aux sites visités.

Les contenus d'appels téléphoniques sont séparés des numéros d'appel entrant ou sortant d'un tel ; cependant il n'en est pas de même pour les adresses mails et leur contenu : cette information est communiquée par « *paquets* ». Afin d'exécuter l'autorisation de recherche sous l'article 216, il faudrait séparer les adresses mails de leurs contenus ; le FBI affirme qu'il n'aura pas accès au message en entier et qu'il faut lui faire confiance car il séparera les informations autorisées à être collectées et les autres.

« **Trust us, we are the government** » solution= ACLU = inconstitutionnelle.

Par ailleurs, relevons que le FBI utilise le système Carnivore de surveillance sur Internet afin de mettre en application cet article liberticide, qui lui donne accès non seulement à toutes les communications « visées » (« *target's communications* ») mais aussi à celles non visées mais qui utilisent les même FAI que la communication visée !!! Ainsi, l'article 216 permet au FBI d'obtenir des informations non-autorisées par l'autorité judiciaire.

Car normalement ces autorisations de surveillance ou de recherches doivent mentionner « *the place to be searched* », si une information n'est pas strictement visée, le FBI n'était pas en mesure de l'obtenir (« *new order warrant* ») ; de plus, la compétence du juge était territoriale afin d'éviter les « forum shopping » par les agents fédéraux.

Désormais, l'article 216 permet à un juge fédéral ou un magistrat d'une autre juridiction de délivrer un « *pen register or trap and trace order* » qui ne précise pas le n° IP en cause et il peut être délivré partout sur le territoire américain= affaiblissement des pouvoirs du juge et « chèque en blanc » pour les agents fédéraux (« *blank warrant* »). [8]

B- Vie privée et liberté d'expression (1er amendement)

Freedom of expression= freedom of speech, of the press, of assembly and petition.

Cour Suprême= « *cette liberté est la matrice, la condition indispensable de presque toutes les formes de libertés* » = position privilégiée (« *preferred position* ») dans la hiérarchie constitutionnelle [9].

Schenck v. US (1919) et Abrams v. US (1919)= la liberté d'expression peut uniquement être punie si elle représente un « danger actuel et clair » (« *a clear and present danger* ») imminent.

En 1969 dans Brandenburg v. Ohio, la Cour Supreme a établi un nouveau critère= la liberté d'expression ne peut être empêchée que si elle est intentionnellement et vraisemblablement source d'attaque imminente illégale à l'ordre social (« *likely to produce imminent lawless action* »).

Le gouvernement peut réduire certains « *protected speech* » en imposant des restrictions temporelles, de lieu et de manières (« *time, place and manner restrictions* »), la plupart du temps en exigeant des demandes d'autorisations préalables.

Si la Cour Suprême a reconnu le droit du gouvernement à ne pas révéler certaines informations (ex déploiements de troupes en temps de guerre), cependant elle n'a jamais confirmé une injonction du gouvernement fondée sur des questions de sécurité nationale.

Les bibliothécaires (ALA *American Library Association*) s'inquiètent du Patriot Act notamment car la mesure facilite l'obtention des registres des abonnés : les agents fédéraux n'ont plus besoin d'une commission rogatoire (« *trap or trace order* ») pour obtenir immédiatement les fichiers, au lieu de devoir prouver l'existence d'une piste sérieuse (« *probable cause* »). Qui plus est, la procédure est désormais secrète.

Le tribunal qui autorise les recherches délibère à huis-clos et les bibliothécaires encourent des poursuites s'ils rendent publiques des informations sur l'enquête, de quelque nature que ce soit.(augmentation des pouvoirs d'investigations sur une catégorie des simples citoyens ; livres=fiché) : FBI a déjà approché 85 des 1500 bibliothèques en 2002 selon l'ACLU [10]

Le Républicain **Bernie Sanders** a proposé un amendement à l'article 215 aux fins de voir rétablir le standard de la « *probable cause* » (affaires criminelles) aux commission rogatoires délivrées aux bibliothèques, relevant que la plus grande inquiétude réside dans le secret [11].

Lors du vote de l'amendement celui-ci avait gagné la majorité des votes à l'expiration des votes ; mais les leaders Républicains on laissé les votes ouverts durant deux fois plus de temps que le délai imparti (20 mins) et ont « persuadé » les républicains de changer leurs votes. « *Je trouve ironique qu'un amendement désigné pour protéger la démocratie américaine et nos droits constitutionnels, les leaders républicains ont du détourner les votes et le processus démocratique pour gagner. C'est un jour très triste pour la démocratie* » .

Affaire= Mohamed Amry dénoncé par un compatriote de sa connaissance après 20 ans aux Etats-Unis, 2 mois de détention préventive+ 8 mois de liberté surveillée avec bracelet électronique après versement d'une caution de 200.000=extradition= accusation a toujours refusé de dévoiler toutes les informations supposées à charge [12].

Les personnes non citoyens américains peuvent être détenus sans accusation sous ordre de l'attorney général sans qu'il ne soit nécessaire de démontrer à la cour qu'elle est dangereuse ou sur le point de quitter le pays.

Actions politiques : le FBI a proposé l'allègement des mesures (1970') qui leur interdit d'espionner les gens en raison de leurs activités politiques.

Selon les nouvelles dispositions, les agents auraient le droit d'accéder aux bases de données publiques même s'ils ne mènent pas une enquête spécifique= pêche à l'information du numérique.

But ? on ne sait pas avec exactitude quelles bases de données sont visées, mais des éléments sont apparus au grand jour (sondage informel Privy Council chargé de la protection des données personnelles 64% sociétés de voyage et de transport, seules 14% en ont informé les intéressés chaîne de supermarché= fichier de ses cartes d'achat, Lexis/Nexis= énorme base de données avec des articles de journaux, dossiers légaux et fichiers publics affirme travailler étroitement avec les services gouvernementaux y compris sur l'authentification de l'identité des personnes !)

Les avocats des droits civils= autorités fédérales ne donnent que peu d'indications (aucune) sur la manière dont ces nouveaux outils légaux étaient exploités pour mener des enquêtes.

Patriot Act II [13]=affaiblit les contre-pouvoirs (checks and balances), les amendements 1 et ` posent d'importantes limites à la possibilité pour le gouvernement de faire des recherches ou des enregistrements, notamment en matière de religion et d'activité politique. Désormais le gouvernement a libre accès

aux informations concernant les citoyens ordinaires.

Les communautés religieuses qui prendraient des positions opposées à celles du gouvernement pourraient se voir d'infiltrations et de surveillance (section 312) à l'instar des bibliothèques (sections 128 & 129).

« Il y a six mois, note David Cole, le pourcentage d'Américains préoccupés par la restriction des libertés individuelles était de 7 %. Aujourd'hui, selon CBS, il est de 52 %. « Tous les candidats démocrates ont remis en cause l'USA Patriot Act, demandant son annulation ou son amendement. « Il y a eu un grand débat sur la nécessité de sacrifier les droits des libertés à la sécurité. En pratique, cependant, le gouvernement avait surtout sacrifié les libertés des étrangers. Mais comme les affaires Hamdi et Padilla (voir Dans le trou noir de Guantanamo)Je démontrent, ce que nous faisons à des étrangers naturalisés ouvre peut-être la voie à ce que l'on fera à des citoyens américains demain. «

Moyens d'expression : ACLU= les pouvoirs définis par la loi sont extrêmement larges et s'attaquent en profondeur aux libertés individuelles ; nombreux éditeurs dans les grands quotidiens américains ont classé la loi comme réactionnaire.

Les FAI répugnent à discuter les détails de cette surveillance se retranchant derrière la sécurité nationale mais reconnaissent que les demandes de surveillance ont augmenté depuis 2001 dans des proportions difficiles à évaluer (davantage due à la vigilance des services gouvernementaux qu'aux pouvoirs définis par le Patriot Act lui-même, psdt Time Warner).

Dérives de la censure [14] : l'état de Pennsylvanie avait adopté en 2002, une loi permettant au Ministre de la Justice et aux procureurs du District de requérir par l'intermédiaire du juge le blocage de sites Web à caractère pédophile.

Outrepassant ses prérogatives, le procureur général a demandé directement aux FAI le blocage de certains contenus sur le Net.

Or l'application d'une censure sélective sur le Net est techniquement impossible, le filtrage d'une seule page entraîne souvent l'inaccessibilité de nombreux sites portant parfaitement légaux.

Près de 500 ordres de blocage= centaines de disparitions de publications en ligne sans contenu pédophiles.

ACLU= CDT ont entamé une procédure en justice contre l'application de cette loi (pas décision), important car loi d'un Etat (même si pas fédérale)= jurisprudence.

Liberté d'expression

Liberté de la presse [15] : le 30 mai 2002= plan de réforme de la police fédérale (FBI) selon lequel le FBI recentre ses activités sur la lutte antiterroriste et non sur la lutte contre la criminalité.

RSF a adressé une lettre au Ministre de la Justice afin que M.Aschcroft réaffirme le principe du secret des sources et de la confidentialité des informations en soumettant tout acte de surveillance à l'autorisation préalable d'un magistrat.= rappelle les heures sombres du maccarthysme.

Par ailleurs, des dérapages récents viennent étayer ces peurs, ainsi l'organisation non-gouvernementale américaine EPIC (*Electronic Privacy Information Center*) s'est procuré des documents officiels du FBI qui prouvent des défaillances de son logiciel d'interception des mails « carnivore » .

Le collectif FEN [16](Free expression Network), organisation onusienne qui regroupe une douzaine d'organisations anglo-saxonnes dont les mandats portent sur la liberté d'expression, la cyberliberté et la liberté de la presse ; estime que la situation s'est détériorée depuis 2001. Le ministre de la Justice et les services fédéraux ont restreint

deteriorée depuis 2001, le ministre de la justice et les agences fédérales ont restreint l'accès des journalistes à certains documents, de même que de très nombreux documents ont été purement et simplement retirés des sites ou des bibliothèques.

Depuis le 11 septembre 2001, des musulmans originaires de pays arabes et de l'Asie du sud-est sont les premières victimes des mesures liberticides prises par l'administration Bush : + 1 millier arrêtés en raison de leur religion ou de leur origine ethnique aucun d'eux n'a été inculpé, après plusieurs semaines ou mois de détention, de crime terroriste.

Au nom de la lutte contre le terrorisme, l'administration peut désormais conduire ses opérations en secret, réprimer des délits d'opinion, placer sous surveillance des citoyens même lorsqu'il n'y a pas d'éléments permettant de soupçonner une activité criminelle, recueillir des informations sensibles sur la vie privée des citoyens et des étrangers résidant aux Etats-Unis [17].

La loi sur la Sécurité Intérieure (*Domestic Security Enhancement Act*) donne à l'Etat « le droit de retirer la nationalité à une personne qui serait en rapport avec une organisation figurant dans la liste noire du ministère de la justice, même si cette personne n'est pas au courant de cela ». En somme, écrit Noam Chomsky (4), « donnez quelques dollars à une organisation de charité islamique qu'Ashcroft a classée comme terroriste, et vous pouvez vous trouver dans le premier avion quittant ce pays. Sans possibilité de recours ».

« Les Etats-Unis, la Grande-Bretagne, la France, l'Allemagne, l'Espagne, l'Italie, le Danemark, le Parlement européen, le Conseil de l'Europe ou le G8 s'en sont pris, au fil des mois, aux libertés numériques », déplore le secrétaire général de Reporters sans frontières. « Ces pays et ces institutions ont pourtant une culture démocratique profondément ancrée. Leurs citoyens ont gagné de haute lutte le droit à la liberté d'expression, à la protection de la confidentialité de leurs courriers et au secret des sources des journalistes ».

II- CYBERSURVEILLANCE : LE TOUT SECURITAIRE DE BIG BROTHER

A- Cyberliberté et terrorisme

Les Etats-Unis, acteur dominant de l'Internet mondial, se veulent porte-parole de la liberté d'expression sur le Net. Pourtant le 11/9 2001, leur législation antiterroriste empiète de plus en plus sur les libertés individuelles des internautes.

Depuis le milieu des années 90, un certain nombre d'Etats et d'institutions ont cherché à contrôler Internet au travers des lois ou textes de régulation : la croisade antiterroriste et les dérapages sécuritaires qu'elle engendre ont précipité cette tendance.

Le rapport de RSF évalue les « dommages collatéraux » de l'atteinte aux libertés fondamentales numériques [18] : « la situation est inquiétante parce que, outre les pays ennemis de la liberté d'expression, Internet doit désormais faire face à une nouvelle menace en provenance des démocraties occidentales ».

Le rapport cite, entre autre, la Résolution 1373 relative au combat contre le terrorisme votée par le Conseil de sécurité de l'ONU le 28 septembre 2001 ; l'USA Patriot Act adopté aux Etats-Unis le 24 octobre 2001 et les décrets présidentiels de George W. Bush ; la révision de la Directive européenne sur la protection des données de télécommunications votée le 30 mai 2002 ; le vote de lois par les Parlements nationaux un peu partout dans le monde ; les recommandations du G8 ou d'Europol (police européenne), etc.

La loi des droits civiques (Bill of Rights) en est la dernière victime : Le vice-président Richard Cheney a annoncé la couleur, en déclarant peu après le 11 septembre 2001 : « Beaucoup de mesures que nous avons été obligés de prendre deviendront

permanentes dans la vie américaine, elle feront partie d'une nouvelle "normalité".
 « Une perspective effrayante, selon l'avocate Deborah Pearlstein, pour qui cette « normalité » se traduit en réalité par « un éloignement de l'Etat de droit.

Les Etats-Unis ne se considèrent plus liés aux principes qui ont longtemps constitué leurs fondements « *Les entorses aux droits constitutionnels n'ont pas commencé avec M. Bush. Dans le sillage du premier attentat contre le World Trade Center, en 1993, et de celui qui a détruit le bureau fédéral d'Oklahoma City en 1995, le Congrès a passé l'Anti-Terrorism Act, « un des pires assauts à la Constitution depuis des décennies [19] » .*

Cette loi a ressuscité le délit d'association et elle a créé une cour spéciale ayant accès à des informations classifiées (secret défense) pour déporter des étrangers suspectés de terrorisme. Et surtout elle a supprimé la loi - qui n'avait que quelques années de vie - interdisant au FBI d'enquêter sur les activités concernant le premier amendement (liberté d'expression, association politique, religieuse et de presse).

Alors que les sénateurs américains lancent un programme pour lutter contre la censure d'Internet dans le monde, ils se refusent à contrôler l'activité de leurs entreprises, dont certaines aident pourtant les dictatures à s'équiper en matériel de surveillance et de filtrage de la Toile.

Electronic Privacy Information Center, un groupe qui a contribué à rendre publics les détails sur Carnivore = alerte les citoyens.

ACLU=21 août 2002 a fait une demande officielle pour savoir comment les pouvoirs détenus du Patriot Act étaient écoulés, pas de réponse.

On ne sait pas non plus quel comportement on-line est considéré suspect.

Certains pensent que les FAI et autres sociétés de même type pourraient prendre des mesures excessives de leur propre initiative=gestionnaires de réseaux trop zélés pourraient prendre des mesures restreignant arbitrairement des communications électroniques ou l'accès à certains sites Internet (déjà le cas pour les sites pornographiques ou les courriers contenant des obscénités).

Les FAI et les opérateurs de téléphonie devront produire toutes les informations requises (dates de connexion, destinataires d'appels...) sur leurs clients suspectés par le FBI lorsque les « enregistrements exigés relèvent d'une enquête autorisée dans le cadre de la protection contre le terrorisme international » .

Los Angeles : cas d'un homme qui a posté un message évoquant des problèmes de sécurité dans certains logiciels de courrier électronique et proposait d'y remédier, il a été inculpé pour s'être introduit dans un ordinateur fédéral.

La définition juridique du « terrorisme » est étendue à certains crimes informatiques et un nouveau crime de « *cyberterrorisme* » est prévu.

Il comprend les actes de piratage causant plus de 5000 dollars de dommages dans l'année, et est puni de 5 à 20 ans de prison. Un nouveau laboratoire d'expertise et de formation sera créé à l'usage des autorités fédérales.

Les mesures de surveillance étendue des communications téléphoniques et électroniques doivent expirer en décembre 2005 en l'absence d'une action du législateur [20].

B- L'espoir du contrôle judiciaire : la décision du 28 septembre 2004

« *La démocratie déteste les secrets injustifiés* » (Juge Marrero).

Le 28 septembre 2004, le Juge Marrero, juge du District de NY, vient censurer une partie essentielle de la loi et la déclare inconstitutionnelle en ce qu'elle autorise le FBI

à demander des informations au FAI sans contrôle judiciaire (*such letters « effectively bars or substantially deters any judicial challenge »*) et viole la liberté d'expression en imposant un silence permanent sur les sociétés recevant ces lettres. Cette décision pourra avoir un impact direct sur les méthodes de surveillances gouvernementales.

« Under the mantle of secrecy, the self-preservation that ordinarily impels our government to censorship and secrecy pay potentially be turned on ourselves as a weapon of self-destruction » .

Dans un procès intenté au nom d'un FAI non cité, l'ACLU mettait en cause cette loi estimant qu'elle restreint la liberté d'expression et les libertés individuelles= quiconque recevant la fameuse lettre (NSL) a l'interdiction d'en faire part « à qui que ce soit » , ordre qui va à l'encontre de la constitution.

« Tous les destinataires, excepté les plus impétueux et ceux qui ne se laissent pas démonter, penseraient qu'ils n'ont pas le droit de consulter un avocat ou demander conseil (...) ils se résigneraient au silence absolu concernant l'existence de la NSL, pour le destinataire raisonnable, au vu du ton péremptoire de la lettre et de la conduite du FBI associée à la NSL, la rébellion n'est pas une option viable » , précise le juge Marrero.

L'envoi de ces lettres n'est pas nouveau, avant le Patriot Act, elles étaient utilisées lors d'enquêtes concernant des espions ou terroristes présumés après autorisation du juge. Précaution juridique qui a sauté avec le vote de la loi.

Le verdict du juge ne prendra effet que dans 90 jours, de quoi laisser au gouvernement le temps de faire appel (à l'étude pour le Ministre de la Justice).

D'autres raisons motivent l'arrêt des lettres NSL pour le juge = effrayante perspective de les voir détournées de leur usage d'origine : *« ainsi, le FBI pourrait théoriquement envoyer une lettre à l'administrateur d'un système informatique utilisé pendant une campagne électorale, afin d'obtenir le nom des personnes qui ont une adresse e-mail ; le FBI pourrait en théorie également envoyer une lettre NSL pour connaître l'identité d'une personne dont le « web log » critique le gouvernement »* .

Ensuite, les FAI disposent dans leurs fichiers de beaucoup plus d'informations sur un individu qu'à l'époque analogique, *« les données Internet obtenues via une NSL pourrait être largement différentes de celles dont disposent les banques et compagnies de téléphone. Elles seraient susceptibles de livrer de paquets d'adresses e-mails avec lesquelles un abonné a correspondu, ainsi que les pages qu'il a visitées »* .

Trois propositions de lois sont actuellement à l'examen au Congrès (2 à la Chambre, 1 au Sénat), elles vient à éclaircir les zones d'ombres entourant les NSL, en clarifiant les procédures qui peuvent être utilisées, tout en imposant des sanctions pour les personnes qui ont révélé l'existence de la lettre [21].

L'impact définitif de cette décision est difficilement mesurable. En sus de pouvoir faire appel, le gouvernement estime que cette décision n'a d'effet que dans le district sud de manhattan. Par ailleurs, il a peu de chance d'être appliqué avant une décision d'appel.

Encore aujourd'hui, les plaignants ont interdiction de révéler le nom de la compagnie qui a engagé l'action. Enfin, Le champ d'application est encore plus restreint car la décision ne s'applique qu'aux NSL visant les FAI ; ce sont d'autres dispositions qui encadrent les NSL et les établissements financiers et de crédits [22].

C- Les dispositions du CSEA

[23] Le 15 juillet 2002, la Chambre des représentants a adopté le *Cyber Security enhancement Act* dont le texte avait été rédigé avant le 11 septembre mais adopté dans le prolongement du Patriot Act.

Le texte a été intégré à la nouvelle loi sur la sécurité intérieure (*Homeland Security Act*) adoptée le 19 novembre 2002 et accompagnée de nombreux décrets et mesures anti-terroristes décidés par l'administration Bush afin de s'attribuer des pouvoirs que le Congrès leur avait refusés.

Toute personne qualifiée de « *hacker* » (pirate informatique) qui met en danger sciemment ou « *par imprudence* », la vie d'autres personnes par l'usage d'un ordinateur peut être emprisonnée à vie = concerne le hacking de systèmes informatiques « sécurisés des centrales nucléaires, des centres de gestion du trafic aérien ou des serveurs de l'armée.

Avant le CSEA, les FAI supportaient la responsabilité civile et pénale à l'égard de leurs abonnés en cas de divulgation de leurs informations sauf en cas d'indices patents de dysfonctionnements du système dû à un internaute déterminé, de mandat du juge ou de constat d'infraction ou de crime en cours de commission.

Le CSEA permettra quant à lui la surveillance « *limitée* » lorsqu'une attaque survient sur un ordinateur protégé et connecté ou que des « *intérêts ayant trait à la sécurité nationale* » .

Les informations collectées seront- officiellement- : numéro de tel du suspect, son adresse IP, la destination et la provenance de ses communications, son URL et les informations contenues dans le titre des mails qu'il reçoit ou envoie.

Toutefois, les FAI sont autorisés à transmettre le contenu des mails ainsi que toute information électronique dans les cas de « *crimes sérieux* » .

Les FAI qui assumaient auparavant une position inconfortable, ont été libérés de tout scrupule et affranchis de toute barrière en deux temps.

D'abord par le "Patriot Act" qui lui a permis d'ouvrir son réseau aux multiples techniques de renseignement portant sur des informations couvertes par le droit à la vie privée de ses utilisateurs dès lors qu'il a des motifs « *raisonnables* » de penser qu'il y a abus (une once d'objectivité subsistait malgré le maigre critère) ; le CSEA a encore allégé le critère en conditionnant sa coopération avec l'autorité à « *sa croyance de bonne foi* » qu'il y ait abus.

« *Une question subsiste : peut-on ne pas être de bonne foi devant un agent du gouvernement qui demande l'accès aux données informatiques ?* »

L'incitation à préserver la vie privée des utilisateurs ne pourra contrebalancer la tentation de collaborer et de se conformer à la loi dont se prévalent les autorités présentes.

Enfin, les agents autorisés à requérir les FAI ne sont plus les autorités judiciaires ou leurs mandataires mais toute l'autorité fédérale d'Etat ou locale (vaste liste !).

Aucune permission ou mandat préalable du juge ne sont nécessaires pour procéder aux investigations électroniques.

Si une requête en vue de l'utilisation de tous les moyens d'espionnage électronique disponibles est adressée au juge, ces outils pourront dans tous les autres cas être utilisés pendant 48h (« *pen register* » et « *tap & track devices* »).

A posteriori, aucune disposition ne prévoit de procéder d'information d'une institution publique, du pouvoir judiciaire ou bien évidemment de l'intéressé ... : seule obligation pour l'autorité qui a procédé aux écoutes = informer le Ministère de la Justice après 3 mois.

De plus, paradoxalement, **l'urgence** ne doit plus être « *imminente* » , une menace indéterminée risquant de se concrétiser un jour suffit.

En outre, rien ne prohibe explicitement le recours à ces techniques si l'ordinateur n'est plus le vecteur de la menace mais un moyen d'intercepter de l'information pour prévenir la concrétisation d'un risque n'ayant aucun rapport avec l'informatique.

Quatre propositions amendements écartés dont la centralisation des informations relevées en vertu du CSEA par le Gouvernement afin de renforcer l'efficacité des collectes et de les rendre transparentes et vérifiable la mise en oeuvre du CSEA (opacité totale)

-restituer la compétence exclusive d'autorisation des écoutes et enregistrements secrets au pouvoir judiciaire ce qui revenait à vider le CSEA d'une majeure partie de son sens.

-formaliser l'existence et le rôle du *National Infrastructure Protection Center* dans une loi afin de démocratiser cette institution (qui coordonne les actions préventives et réactives à tout type d'attaque réelle ou virtuelle sans toutefois être responsable de la centralisation des informations collectées en vertu du CSEA, centre créé par le gouvernement sans recours à un texte fondateur !)

-prévoir une information minimale du pouvoir judiciaire lorsque des actions sont menées sur la base du CSEA.

Il semble que le CSEA n'ait pas été adopté pour traquer les surdoués du hacking, ses applications potentielles sont effrayantes, pourvu que l'utilisation d'un ordinateur connecté intervienne.

Par Maya GHOZALI

Maya Ghozali

[1] D'autres pays ont suivi l'exemple des Etats-Unis, ex. la Loi sur la Sécurité Quotidienne en France.

[2] La sécurité, guerre à la terreur, Eric Pelletier, L'express, 27/09/2004.

[3] H.R. 3162.

[4] Bush tient sa loi USA Act, Estelle Dumout, 26/10/2001, ZDNet France.

[5] Big Brother : un juge fédéral américain abolit une partie du Patriot Act, Associated Press, novembre 2004.

[6] Après le 11 septembre : l'informatique au centre du « New Deal » sécuritaire aux Etats-Unis, John Borland et Lisa Bowman, CENT News.com, 6/9/2002.

[7] How the antiterrorism Bill enables law enforcement to use Intelligence authorities to circumvent the privacy protections afforded in criminal cases, ACLU, 23 octobre 2001.

[8] How the antiterrorism bill limits judicial oversight of téléphone and Internet surveillance, ACLU, 23 octobre 2001.

[9] Freedom of expression, ACLU, 1er mars 2002.

[10] What is section 215 ?, ACLU, 24 octobre 2002.

[11] Sun should set on part of Patriot Act, Seattle Times, 15/7/2004 ; www.bernie.house.gov.

- [12] Je ne suis pas un terroriste, mohamed Amry, Ed. Balland, Paris 2004.
- [13] Justice department contemplates seeking : more powers bill would further erode limits on antiterror powers, ACLU, fact sheet on Patriot Act II, 28 mars 2003.
- [14] Reporters sans frontières, Etats-Unis, www.rsf.org, 22/06/2004.
- [15] La réforme du FBI menace la confidentialité du travail des journalistes, Reporters sans frontières, 3/6/2002.
- [16] www.enduring-freedoms.org
- [17] Des lois « patriotiques », Augusta Conchiglia, Le Monde Diplomatique, janvier 2004.
- [18] Internet en liberté surveillée : la croisade antiterroriste menace la cyberlité dans le monde, 11 septembre 201-11 septembre 2001, 5/09/2002.
- [19] « Terrorism and Constitution », The New Press, New York, 2002.
- [20] Etats-Unis : la loi facilite la surveillance électronique, Forum des droits de l'Internet, 29/10/2001.
- [21] Surveillance : la justice américaine égratigne le Patriot Act, Declan McCullagh, CENT News.com, 4/10/2004.
- [22] Key part of Patriot Act ruled Unconstitutional, Dan Eggen, www.bernie.house.gov.
- [23] Le CSEA : droits, libertés et répression des cybercrimes aux Etats-Unis d'Amérique, Donatien Cassiers, Droit et Nouvelles Technologies, 23/12/2002.

© 2002-2006. Les contributions publiées sur le site demeurent la propriété exclusive de leurs auteurs respectifs. Tous droits réservés. Les différents squelettes sont sous licence **Creative Commons**.



Ce site est développé sous **SPIP**, hébergé chez **OVH**, et déclaré à la **CNIL**, n°1147436. Pour faire usage de votre droit de consultation ou de modification sur les données stockées vous concernant, merci d'envoyer un mail aux **webmasters**. Directeur de publication : Thibault Grouas.