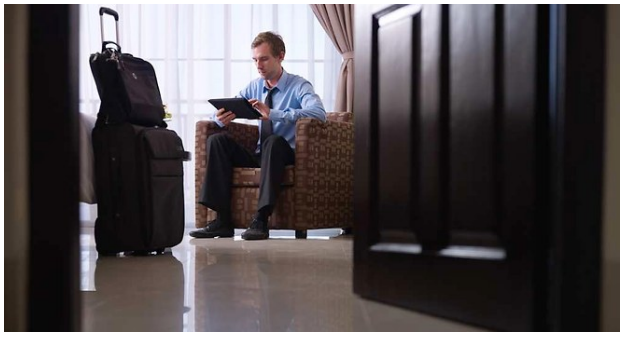
# Nouvelle vague d’attaques cybercriminelles : le « Dark hotel »



Nouvelle vague d’attaques cybercriminelles : le « Dark hotel »

**« Dark hotel » : ces hackers qui exploitent les réseaux Wi-fi des hôtels de luxe.**
**Des hackers ont pris pour cible des directeurs généraux et autres cadres dirigeants d’entreprises lorsqu’ils voyagent à l’étranger. Un phénomène qui durerait depuis quatre ans.**
Nom de code « Dark Hotel ». Ce nouvel acteur dans le monde du cyberespionnage sévit depuis au moins quatre ans, révèle la société de sécurité russe Kaspersky Lab. **Ses cibles appartiennent à l’élite économique internationale : directeurs généraux, vice-présidents, directeurs des ventes et marketing de grosses entreprises américaines et asiatiques**. Pour les piéger et leur dérober des données sensibles, ces hackers mettent à profit les réseaux Wi-fi des hôtels de luxe dans lesquels ils voyagent.

Ces hackers sans visage ont un mot d’ordre : ne jamais frapper deux fois la même cible. Leur mode opératoire ? Un faux logiciel, de type Adore Reader ou Google Toolbar, que le visiteur est invité à télécharger après s’être connecté au réseau Wi-fi de son hôtel. Un cheval de Troie permet ensuite au hacker de recueillir des données privées, y compris les mots de passe sur Firefox, Chrome, Internet Explorer ainsi que les identifiants sur Gmail, Yahoo,Facebook et Twitter.

Les victimes se font ainsi voler des données qui relèvent du domaine de la propriété intellectuelle des entreprises qui les emploient. Après l’opération, toute trace est effacée du réseau de l’hôtel, le hacker retournant dans l’ombre. Une « précision chirurgicale », souligne Kaspersky Lab.

Selon l’unité de recherche de la société russe, une empreinte laissée par les hackers suggère que les cybercriminels parlent coréen. Le plus haut volume d’activité a été détecté entre août 2010 et 2013. 90 % des cyberattaques étaient localisées au Japon, Taïwan, en Chine, en Russie et en Corée du Sud. Depuis 2008, elles se comptent par milliers. Kaspersky Lab n’est, pour l’heure, pas parvenu à tracer ces hackers.

A partager sans modération

**Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)**

**Source :**
http://www.lesechos.fr/tech-medias/hightech/0203938482430-dark-hotel-ces-hackers-qui-exploitent-les-reseaux-wi-fi-des-hotels-de-luxe-1064496.php
Aurélie Abadie

---

# CyberCercle du 8 octobre 2014 – Décryptage du rapport

# interministériel sur la lutte contre la cybercriminalité

## CyberCercle du 8 octobre 2014 – Décryptage du rapport interministériel sur la lutte contre la cybercriminalité

**Le 8 octobre dernier,  Denis JACOPINI s'est rendu au Décryptage du rapport interministériel sur la lutte contre la cybercriminalité organisé par le CyberCercle.**

Le CyberCercle a reçu mercredi 8 octobre 2014, Myriam QUEMENER, Magistrat, membre du groupe de travail auteur du rapport interministériel sur la lutte contre la cybercriminalité, membre de la Commission Numérique à l'Assemblée Nationale, et Maître Christiane FERAL-SCHUHL, avocat, ancien Bâtonnier du Barreau de Paris, co-présidente de la Commission Numérique à l'Assemblée Nationale, pour un petit-déjeuner-débat sur le thème :
« DECRYPTAGE DU RAPPORT INTERMINISTERIEL SUR LA LUTTE CONTRE LA CYBERCRIMINALITE »

Cette conférence s'est déroulée dans les salons du Bateau MAXIM'S en présence d'une cinquantaine d'auditeurs, notamment des représentants de la magistrature, de la Gendarmerie nationale, de la D2IE, de l'ANSSI, du ministère de la Défense, et des entreprises partenaires des forces de sécurité dans la lutte contre la cybercriminalité.
Retrouvez Myriam QUEMENER par video sur notre chaîne YouTube : « Quels sont selon vous les points forts du rapport interministériel sur la lutte contre la cybercriminalité publié en juillet 2014 ? »

**Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)**

**Source :**
http://www.defense-et-strategie.fr/index.php?option=com_content&view=article&id=567:cybercercle-du-8-octobre-2014-decryptage-du-rapport-interministeriel-sur-la-lutte-contre-la-cybercriminalite

---

# Les cybercriminels utilisent aussi les Sous-domaines abandonnés


# Les cybercriminels utilisent aussi les Sous-domaines abandonnés

**Si la plupart des hackeurs tentent de contourner les mesures de sécurité mises en place sur les serveurs d'une entreprise, il est parfois plus simple de scruter l'architecture d'un site au global et les sous-domaines, notamment.**

Spécialisée dans la sécurité, la société Detectify, propose un outil de scan en mode SaaS et annonce avoir mené une enquête concernant la vulnérabilité des sous-domaines. Ces derniers seraient largement laissés à l'abandon et constitueraient un vecteur d'attaques.
Un prestataire de services proposant de créer des comptes utilisateur en leur attribuant un sous-domaine peut lui-même créer son propre sous-domaine pour lancer un service ou une campagne promotionnelle pendant quelques semaines, voire quelques années. Par la suite, à la fin de cette campagne ou à la fermeture du service en question, Detectify explique que le prestataire n'efface pas systématiquement la redirection du sous-domaine pointant vers le service ou la campagne. Or, un internaute peut donc se créer un compte chez ce prestataire de service puis obtenir ce même sous-domaine et orchestrer une attaque de phishing, par exemple.
Cette manipulation est possible lorsque la société en question ne procède pas à la validation du détenteur de chaque sous-domaine. Et il en existerait un certain nombre parmi lesquels nous retrouvons Heroku, Github, Bitbucket, Squarespace, Shopify, Desk, Teamwork, Unbounce, Helpjuice, HelpScout, Pingdom, Tictail, Campaign Monitor, CargoCollective, StatusPage.io ou encore Tumblr.
« Nous avons également identifié 200 organisations qui s'en trouvent affectées. Dans beaucoup de cas, nous parlons de société listées au NASDAQ ou figurant dans le top 100 d'Alexa », ajoute Detectify.
Pour vérifier si une personne est bien le propriétaire d'un domaine ou d'un sous-domaine, quelques sociétés, comme Google demandent de transférer un fichier HTML via FTP ou d'ajouter une CNAME particulière dans le panneau de contrôle du nom de domaine.

**Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)**

Source :
http://pro.clubic.com/it-business/securite-et-donnees/actualite-735061-domaine-abandonnes-vecteur-attaques-hackeurs.html?&xvc_mode=M&xvc_campaign=NL_ClubicPro_New_25/10/2014&partner=-&xvc_position=71726460?&xvc_misc=-&crmID=639453874_71726460?&estat_url=http%3A%2F%2Fpro.clubic.com%2Fit-business%2Fsecurite-et-donnees%2Factualite-735061-domaine-abandonnes-vecteur-attaques-hackeurs.html

---

# 500 000 PC infectés à cause d’une faille Windows XP


# 500 000 PC infectés à cause d’une faille Windows XP

**Selon les chercheurs en sécurité de Proofpoint, 52% des PC infectés par le botnet Qbot font tourner Windows XP. Exploitant une faille de Windows XP mais également de Seven et Vista, un groupe de cybercriminels russe a réussi à activer le botnet Qbot fort 500 000 PC zombies, essentiellement localisés aux Etats-Unis. Son objectif : Aspirer les identifiants bancaires des utilisateurs de ces PC corrompus.**

Des pirates russes à l'origine du botnet Qbot ont construit une impressionnante armée de 500 000 PC zombies en exploitant des failles non corrigées dans des ordinateurs tournant sous Windows XP mais également Windows 7 et Vista. Des PC localisés principalement aux Etats-Unis, a fait savoir la société Proofpoint. Ces derniers temps, les hackers russes ont fait monter la pression avec des incursions sérieuses telle que l'attaque qui a visé la banque américaine JPMorgan Chase. Avec ce botnet, baptisé Qbot, les chercheurs de Proofpoint ont fait ressortir que le groupe qui est à l'origine de sa création l'a élaboré de façon méticuleuse à travers le temps, sans faire de vague, au point de rester sous les radars des sociétés de sécurité et donc de ne pas avoir attiré leur attention.

Selon Proofpoint, 75% des 500 000 PC infectés par le botnet Qbot sont situés aux Etats-Unis, sachant que parmi eux, 52% font tourner Windows XP, 39% Windows 7 et 7% Windows Vista. En Grande-Bretagne, la proportion de PC infectés est bien moindre, 15 000 postes environ. « Avec 500 000 clients infectés volant les identifiants des comptes bancaires en ligne des utilisateurs, le groupe de cybercriminels a le potentiel pour réaliser des bénéfices vertigineux », ont indiqué les chercheurs de la société de conseil en sécurité. Mais le botnet Qbot ne s'attaque pas seulement aux comptes bancaires, il compromet également les sites WordPress, soit en infectant le site lui-même ou bien en injectant des contenus corrompus dans leurs newsletters.
Article de Dominique Filippone

**Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)**

**Source :**
http://www.lemondeinformatique.fr/actualites/lire-500-000-pc-infectes-a-cause-d-une-faille-windows-xp-58878.html

---

# Loi sur le terrorisme : l'Assemblée nationale valide le blocage administratif des sites

## l'Assemblée nationale valide le blocage administratif des sites pour lutter contre le terrorisme

**Après trois jours de débat, l'Assemblée nationale a adopté le 18 septembre dernier, en première lecture le projet de loi visant à lutter contre le terrorisme. Parmi les différents articles, le polémique blocage administratif des sites faisant l'apologie du terrorisme a été voté par les députés.**

C'est un hémicycle bien vide qui s'est prononcé sur le projet de loi contre le terrorisme le 18 septembre dernier : au moment de l'adoption du texte dans son ensemble, une trentaine de députés seulement étaient présents pour voter. Ce texte, soutenu par le ministre de l'Intérieur Bernard Cazeneuve et par le rapporteur désigné, le député PS Sébastien Pietrasanta, a donc été adopté sans difficulté. Il doit encore obtenir l'approbation du Sénat avant de repasser au Palais Bourbon puis d'être ratifié par le président de la République.
Comme nous l'expliquions lundi, Bernard Cazeneuve appelait à un « consensus » autour de ce texte qui vise à lutter contre les nouvelles formes d'enrôlements et de propagandes terroristes, notamment via internet et dans les prisons françaises. Si l'objet du texte n'a en effet pas trop souffert de contradiction, on a pu voir une offensive de la droite qui juge le texte encore trop faible face à la menace qu'il entend combattre.

**Lutter contre le terrorisme et au passage, réguler Internet**
Si le texte a de lourde implication pour les droits fondamentaux des citoyens, celui-ci n'est pas pour autant sans conséquence pour internet. En effet l'article 4 du texte punit donc de 5 ans d'emprisonnement et d'une forte amende le fait d'utiliser Internet pour faire la promotion du terrorisme. La particularité de cet article est de considérer la diffusion via Internet comme une circonstance aggravante : lorsque l'incitation est faite sur un site web public, au vu et au su de tous, la condamnation pourra monter jusqu'à 7 ans et l'amende à 100.000 euros.
Conséquence logique, l'Assemblée a également entériné le blocage administratif (sans décision de justice donc), véritable serpent de mer des lois relatives à Internet. L'article 9, a fait l'objet de nombreuses critiques de la part de parlementaires de tout bord, notamment Laure de la Raudière et Lionel Tardy du coté de l'UMP ou encore Patrick Bloch et Corinne Erhel chez les socialistes.
Cette mesure « est une erreur et je vous invite, je nous invite, à ne pas la commettre », a lancé Christian Paul (SRC). « Faut-il faire reculer encore la liberté, contre le terrorisme ? » s'interroge de son côté Lionel Tardy, « la France s'engage à petits pas dans la direction de la NSA ».

**Pas une volte face ?**
Face à ces critiques, le rapporteur Pietrasanta a fait valoir plusieurs gardes fous mis en place pour éviter les dérives : il faudra d'abord passer par l'éditeur et l'hébergeur afin de faire retirer les contenus problématiques, et le blocage ne sera mis en place que dans les cas ou les premiers recours n'auront rien donné. De plus, une personnalité qualifiée sera nommée pour jauger de la conformité de ces blocages. Reste le risque de surblocage, évoquée par la députée EELV Isabelle Attard qui cite en exemple le récent cas australien de blocage hasardeux de 250.000 sites.

Bernard Cazeneuve est donc revenu sur la méthode de blocage, expliquant que le blocage par DNS, jugé plus précis, serait privilégié mais que la méthode ne serait pas inscrite dans la loi, préférant attendre de fixer cet aspect là par décret.
La volte face du PS sur la question de blocage administratif, qu'il a largement combattu lorsque la droite était au pouvoir, est revenu à intervalle régulier dans les débats, mais la majorité a assuré que son texte disposait de suffisamment de garanties permettant d'assurer la protection des libertés fondamentales. Il faut donc la croire sur parole.

**Prochaine étape : le Sénat**
Autres articles adoptés qui pourraient bien changer la donne : les articles 10 et 11, qui simplifient les procédures de perquisition policières dans le Cloud et faciliter le déchiffrement de données récupérées au cours d'une perquisition. Le texte a donc été adopté sans changement majeurs, la droite n'ayant pas réellement réussi à durcir les mesures proposées par le PS et les mesures majeures prévues par le texte sont globalement restées intactes.
Le projet de loi doit maintenant obtenir l'approbation du sénat. Pour plus de détails, le site NextInpact a couvert de très près les débats et un compte rendu des échanges est en ligne sur leur site. Armez vous néanmoins de patience, l'article dépasse allégrement les 60 000 signes, soit un texte environ 15 fois plus long que celui que vous venez de lire. Mais cette loi n'aura plus aucun secrets pour vous.

**Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)**

**Source :**
http://www.zdnet.fr/actualites/loi-sur-le-terrorisme-l-assemblee-nationale-valide-le-blocage-administratif-des-sites-39806557.htm
Par Louis Adam

---

# Google et Dropbox tentent eux

# aussi de simplifier la cybersecurité

## Google et Dropbox tentent eux aussi de simplifier la cybersecurité

**Les deux entreprises ont initié une alliance dédiée à la cybersecurité, nommée Simply Secure. Google et Dropbox entendent s'atteler au défi séculaire du monde de la cybersecurité : la simplicité d'accès et d'usage de ces outils.**

Si l'on devait compter le nombre de start-ups et de projets qui promettent d'offrir un service garantissant à la fois la plus haute confidentialité des données et une simplicité d'utilisation inégalée, on pourrait probablement passer un moment à établir la liste.
En effet, les récentes révélations Snowden et autres fuites multiples de photos de stars dénudées n'ont fait que rappeler à la communauté des chercheurs en cybersecurité le douloureux problème qui frappe le secteur : les solutions existent, simplement personne ne sait vraiment les utiliser. Mais quand deux géants tels que Google et Dropbox s'allient autour du développement de solutions simples et faciles d'accès pour protéger la vie privée des utilisateurs, l'initiative mérite d'être notée. C'est l'objet de Simply Secure, le consortium dévoilé par les deux entreprises la semaine dernière.

**Beaucoup de bruit pour rien ?**
Si pour l'instant, Simply Secure n'a pas grand-chose à offrir, il promet beaucoup. Simply Secure l'explique ainsi sur son site « nous voulons aider la communauté de cybersecurité open source à faire mieux. Nous ne voulons pas racheter, nous ne voulons pas inventer » mais simplement apporter un soutien dans le domaine de la recherche. Leur cible : le taux d'adoption des outils déjà existant, qui reste particulièrement bas, comme le rapporte le Guardian.

Le programme de l'alliance Simply Secure est donc de s'ouvrir aux acteurs déjà existant et de mettre en place plusieurs partenariats. Pas vraiment de concret à l'horizon donc, et l'alliance s'attaque à un problème pour le moins épineux que beaucoup auparavant ont tenté d'aborder, sans réel succès.
Mais la question de la cybersecurité n'a jamais été aussi significative aux yeux du grand public, et cette initiative de la part de Google et Dropbox vient réaffirmer leur engagement en faveur d'un internet plus sécurisé. Pas sur que cela soit un réel souci pour la NSA, mais c'est l'intention qui compte.

**Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)**

**Source :**
http://www.zdnet.fr/actualites/google-et-dropbox-tentent-eux-aussi-de-simplifier-la-cybersecurite-39806679.htm
Par Louis Adam | Lundi 22 Septembre 2014

# Rapport 2013 DU GIABA : trafic de drogue, fraude fiscale, cybercriminalité constituent les infractions les plus fréquentes au Sénégal

Rapport 2013 DU GIABA : trafic de drogue, fraude fiscale, cybercriminalité constituent les infractions les plus fréquentes au Sénégal

**Le Groupe intergouvernemental d'action contre le blanchiment d'argent en Afrique de l'Ouest (Giaba) vient de publier son rapport annuel pour l'année 2013, dans lequel, il souligne que le trafic de drogue, la fraude fiscale, les autres investissements et la cybercriminalité ont été les infractions sous-jacentes les plus fréquentes en 2013.**

Le rapport annuel 2013 du Groupe intergouvernemental d'action contre le blanchiment d'argent en Afrique de l'Ouest (Giaba) vient d'être publié. En ce qui concerne notre pays, le Giaba a signalé que «le rapport national du Sénégal répertorie le trafic de drogue, la fraude fiscale, les autres investissements et la cybercriminalité comme infraction sous-jacentes les plus fréquentes en 2013». Il a aussi rappelé que «le rapport de l'Organe international de contrôle des stupéfiants (Incsr) 2013 du développement d'Etat américain étend la liste pour y inclure les fraudes bancaires et de dépôt, la falsification de documents, la revente de voitures volées et les combines de la Ponzi. Un taux de corruption élevé a également été signalé dans le pays, un phénomène qui frappe tous les niveaux de gouvernance et le commerce, selon le rapport ».
Le Giaba a souligné que «le Sénégal a de plus en plus démontré son engagement à lutter contre les crimes financiers, y compris le Bc/Ft» surtout en prenant des mesures pour renforcer son dispositif de lutte contre le blanchiment des capitaux et de lutte contre le financement du terrorisme (Lbc/Ft). Cependant, «Un projet de stratégie national de Lbc/Ft est actuellement en attente d'approbation par les autorités, conformément à la loi de Lbc/Ft».
Le rapport annuel renseigne aussi que, chez nous, «plusieurs décisions de justice ont été rendues, y compris des peines d'emprisonnement, des amendes et confiscations, suite à des accusations de blanchiment de capitaux». Et en 2013, la Cellule de renseignement financier a reçu 109 déclarations d'opérations suspectes liées au blanchiment, 14 des cas analysés ont été envoyés aux autorités d'exécution, aux fins d'enquête et de poursuite et 3 condamnations ont été prononcées. Il faut dire que dans les premières lignes de la partie du rapport consacré à notre pays, la traduction en justice, pour enrichissement illicite de Karim Wade, a été rappelée : «En 2013, la répression de la corruption a conduit à la mise en accusation devant les tribunaux de plusieurs ministres dans le gouvernement du Président Wade, dont son fils, Karim Wade, pour corruption» y lit-on.
Même si le Sénégal a fait des progrès d'envergure dans le renforcement de son système de Lbc/Ft, les lacunes suivantes demeurent, selon le Giaba «l'adoption d'un cadre approprié de l'approche fondée sur les risques, la mise en oeuvre de mesures de vigilance pour la surveillance continue des relations et transaction avec les clients, la conduite de l'application de mesures renforcées de vigilance pour les clients à risques élevés».
Egalement, «le renforcement de l'obligation de déclarer les tentatives d'opération et un mécanismes pour la mise en oeuvre des résolutions 1267 et 1373 du conseil de sécurité de l'Onu et les résolutions qui les ont suivies».

**Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)**

**Source :**
http://www.dakaractu.com/Rapport-2013-DU-GIABA-trafic-de-drogue-fraude-fiscale-cybercriminalite-constituent-les-infractions-les-plus-frequentes_a73269.html

# Chine : première hausse des infections aux virus informatiques en cinq ans

## Chine : première hausse des infections aux virus informatiques en cinq ans

**Plus de la moitié des ordinateurs en Chine sont infectés par des virus, indique une récente enquête, précisant que ce nombre est en hausse pour la première fois en cinq ans.**

Ce taux a augmenté de 9,8% en glissement annuel en 2013, mettant fin à une baisse successive de cinq ans, a annoncé mardi le Centre national des mesures d'urgence face aux virus informatiques.
D'après une enquête menée par le centre, 54,9% des ordinateurs examinés étaient touchés par des virus.
Les sites bancaires et les méthodes de paiement en ligne restent les principales cibles des virus, et les pirates tentent de dérober à la fois des fonds et des informations privées. Les utilisateurs de Weibo sont aussi vulnérables aux attaques de virus, selon le centre.
Chen Jiamin, directeur adjoint du centre, a affirmé que les failles de sécurité mettaient en lumière les manques en matière d'administration des sites Internet et de technologies de sécurité des réseaux dans plusieurs organisations.

**Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)**

**Source :**
http://french.people.com.cn/n/2014/0917/c31357-8783700.html

# Home Depot : finalement 56 millions de cartes bancaires piratées

Home Depot : finalement 56 millions de cartes bancaires piratées

**Début septembre, l'enseignement américaine Home Depot révélait avoir observé une activité inhabituelle concernant les données de paiement de ses clients avant de reconnaître une intrusion informatique.**

Home Depot expliquait ainsi que tout client ayant utilisé, depuis le mois d'avril, une carte bancaire pour régler un achat dans l'un de ses magasins aux Etats-Unis et au Canada est potentiellement concerné par le vol de ces données de paiement.
Le groupe ne chiffrait pas le nombre de clients affectés ni le détail exact des données personnelles compromises. Le New York Times évoquait  le nombre de 60 millions de cartes de paiement compromises.

**EMV**
Bingo, Home Depot indique aujourd'hui que ce sont 56 millions de cartes bancaires ont été « mises en péril ». De quoi constituer un nouveau triste record en la matière, jusqu'ici détenu par Target (40 millions de cartes de paiement compromises).
D'ailleurs, comme pour Target, il semble que les pirates aient exploité une variante du programme malveillant BlackPOS installé dans le système de paiement de l'entreprise.
Seule bonne nouvelle, Home Depot estime qu'à ce stade de l'enquête aucune preuve ne permet d'établir que les codes PIN des cartes bancaires compromises figurent également parmi les données dérobées. Mais cette protection est assez peu utilisée aux Etats-Unis…
A la suite de cette intrusion informatique, dont l'ampleur doit encore être précisée, Home Depot a fait savoir qu'il déploierait sur l'ensemble de ses magasins, d'ici à octobre 2015, la technologie EMV de paiement pour cartes à puce. Ce standard international, en vigueur notamment en France, apporte en principe une sécurité accrue des transactions et contribue donc à réduire la fraude.

**Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)**

**Source :**
http://www.zdnet.fr/actualites/home-depot-finalement-56-millions-de-cartes-bancaires-piratees-39806615.htm

# Loi sur le terrorisme : l’Assemblée nationale valide le blocage administratif des sites

| | |
|---|---|
|  | Loi sur le terrorisme : l’Assemblée nationale valide le blocage administratif des sites |

**Après trois jours de débat, l'Assemblée nationale a adopté en première lecture le projet de loi visant à lutter contre le terrorisme. Parmi les différents articles, le polémique blocage administratif des sites faisant l'apologie du terrorisme a été voté par les députés.**

C'est un hémicycle bien vide qui s'est prononcé sur le projet de loi contre le terrorisme aujourd'hui : au moment de l'adoption du texte dans son ensemble, une trentaine de députés seulement étaient présents pour voter. Ce texte, soutenu par le ministre de l'Intérieur Bernard Cazeneuve et par le rapporteur désigné, le député PS Sébastien Pietrasanta, a donc été adopté sans difficulté. Il doit encore obtenir l'approbation du Sénat avant de repasser au Palais Bourbon puis d'être ratifié par le président de la République.
Comme nous l'expliquions lundi, Bernard Cazeneuve appelait à un « consensus » autour de ce texte qui vise à lutter contre les nouvelles formes d'enrôlements et de propagandes terroristes, notamment via internet et dans les prisons françaises. Si l'objet du texte n'a en effet pas trop souffert de contradiction, on a pu voir une offensive de la droite qui juge le texte encore trop faible face à la menace qu'il entend combattre.

**Lutter contre le terrorisme et au passage, réguler Internet**
Si le texte a de lourde implication pour les droits fondamentaux des citoyens, celui-ci n'est pas pour autant sans conséquence pour internet. En effet l'article 4 du texte punit donc de 5 ans d'emprisonnement et d'une forte amende le fait d'utiliser Internet pour faire la promotion du terrorisme. La particularité de cet article est de considérer la diffusion via Internet comme une circonstance aggravante : lorsque l'incitation est faite sur un site web public, au vu et au su de tous, la condamnation pourra monter jusqu'à 7 ans et l'amende à 100.000 euros.

Conséquence logique, l'Assemblée a également entériné le blocage administratif (sans décision de justice donc), véritable serpent de mer des lois relatives à Internet. L'article 9, voté jeudi 18 septembre, a fait l'objet de nombreuses critiques de la part de parlementaires de tout bord, notamment Laure de la Raudière et Lionel Tardy du coté de l'UMP ou encore Patrick Bloch et Corinne Erhel chez les socialistes.
Cette mesure « est une erreur et je vous invite, je nous invite, à ne pas la commettre », a lancé Christian Paul (SRC). « Faut-il faire reculer encore la liberté, contre le terrorisme ? » s'interroge de son côté Lionel Tardy, « la France s'engage à petits pas dans la direction de la NSA ».

**Pas une volte face ?**
Face à ces critiques, le rapporteur Pietrasanta a fait valoir plusieurs gardes fous mis en place pour éviter les dérives : il faudra d'abord passer par l'éditeur et l'hébergeur afin de faire retirer les contenus problématiques, et le blocage ne sera mis en place que dans les cas ou les premiers recours n'auront rien donné. De plus, une personnalité qualifiée sera nommée pour jauger de la conformité de ces blocages. Reste le risque de surblocage, évoquée par la députée EELV Isabelle Attard qui cite en exemple le récent cas australien de blocage hasardeux de 250.000 sites.
Bernard Cazeneuve est donc revenu sur la méthode de blocage, expliquant que le blocage par DNS, jugé plus précis, serait privilégié mais que la méthode ne serait pas inscrite dans la loi, préférant attendre de fixer cet aspect là par décret.
La volte face du PS sur la question de blocage administratif, qu'il a largement combattu lorsque la droite était au pouvoir, est revenu à intervalle régulier dans les débats, mais la majorité a assuré que son texte disposait de suffisamment de garanties permettant d'assurer la protection des libertés fondamentales. Il faut donc la croire sur parole.

**Prochaine étape : le Sénat**
Autres articles adoptés qui pourraient bien changer la donne : les articles 10 et 11, qui simplifient les procédures de perquisition policières dans le Cloud et faciliter le déchiffrement de données récupérées au cours d'une perquisition. Le texte a donc été adopté sans changement majeurs, la droite n'ayant pas réellement réussi à durcir les mesures proposées par le PS et les mesures majeures prévues par le texte sont globalement restées intactes.
Le projet de loi doit maintenant obtenir l'approbation du sénat. Pour plus de détails, le site NextInpact a couvert de très près les débats et un compte rendu des échanges est en ligne sur leur site. Armez vous néanmoins de patience, l'article dépasse allégrement les 60 000 signes, soit un texte environ 15 fois plus long que celui que vous venez de lire. Mais cette loi n'aura plus aucun secrets pour vous.

**Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)**

**Source :**
http://www.zdnet.fr/actualites/loi-sur-le-terrorisme-l-assemblee-nationale-valide-le-blocage-administratif-des-sites-39806557.htm
Par Louis Adam | Jeudi 18 Septembre 2014