LOPPSI 2 : le Patriot Act français

EN DROITE LIGNE DES USA, LA LOI LOPPSI 2 ACCENTUE LA SURVEILLANCE DU POUVOIR FRANÇAIS SUR SES CITOYENS AFIN QU'ILS S'ABANDONNENT À L'ÉTAT ET RENONCENT AU DROIT À LA VIE PRIVÉE.

/ **Jean-Claude Paye**
Sociologue, auteur de La Fin de l'État de droit. La Dispute.

La LOPPSI 2, loi d'orientation et de programmation pour la sécurité intérieure, adoptée par le Parlement français le 8 février a vu, ce 10 mars, treize de ses dispositions censurées par le Conseil constitutionnel. En dehors du cran d'arrêt mis à la privatisation de la sécurité, le refus du Conseil porte sur les mesures qui portent le plus atteinte à l'image démocratique de la France, telles celles ciblant les mineurs. Mais il a validé l'essentiel de la loi : la possibilité de filtrer progressivement la Toile et la légalisation de l'introduction de mouchards au sein des ordinateurs.

> **"LOPPSI 2, COMME LE PATRIOT ACT AMÉRICAIN, VISENT À RÉDUIRE LES LIBERTÉS FONDAMENTALES, ET CONTIENNENT DES RÉFORMES IMPORTANTES DESTINÉES À ASSURER UN CONTRÔLE DU NET."**

Cette loi présente de fortes similitudes avec le Patriot Act américain, voté immédiatement après les attentats du 11 septembre 2001. Ces deux législations se présentent comme un fourre-tout sécuritaire, une collection de mesures disparates, visant à réduire les libertés fondamentales, et contiennent des réformes importantes destinées à assurer un contrôle du Net.
Le USA Patriot Act anticipe les lois françaises. Il installe, dès 2001, tout un ensemble de dispositions qui mettront une décennie pour exister dans l'Hexagone, telles l'installation légale de chevaux de Troie dans les ordinateurs, l'incrimination de cybercriminalité ou l'infiltration policière dans les échanges électroniques.

LÉGALISATION DES CHEVAUX DE TROIE

Sous le couvert de la lutte contre la "criminalité organisée", la LOPPSI offre la possibilité, avec l'autorisation d'un juge d'instruction, d'installer, à l'insu de l'utilisateur, un dispositif technique enregistrant les frappes au clavier ou les captures d'écran, qui permettra de retenir toutes les infractions constatées, même si elles ne portent pas sur des faits relevant de la criminalité organisée.
Ces chevaux de Troie pourront être installés sur place ou en s'infiltrant à distance, durant une période renouvelable de huit mois. Afin de les mettre en place, les enquêteurs ont ainsi le droit de s'introduire dans le domicile de la personne concernée, si nécessaire de nuit.

LE FILTRAGE DE LA TOILE

La LOPPSI 2 prévoit également un système de filtrage des sites diffusant des images de mineurs, à caractère "manifestement pornographique". Sans intervention d'un juge, elle donne à une autorité administrative, l'Office central de lutte contre la criminalité, la possibilité de priver ces sites de l'accès à Internet. Cependant, l'administration peut saisir le juge pour les contenus "non manifestement pédopornographiques". Présentée comme une limitation des pouvoirs de l'exécutif, cette disposition a une conséquence perverse car elle permet d'étendre le filtrage à un contenu qui manifestement n'est pas pédophile. Tel est bien l'enjeu de cet article. Une fois le principe du blocage adopté, il suffit d'étendre progressivement le champ des sites filtrables, comme cela a été fait pour le fichier national des empreintes génétiques. La loi introduit ainsi une brèche annonçant d'autres motifs de blocage. Un simple amendement à la LOPPSI permettrait d'inclure les sites qui ne respectent pas le droit d'auteur.

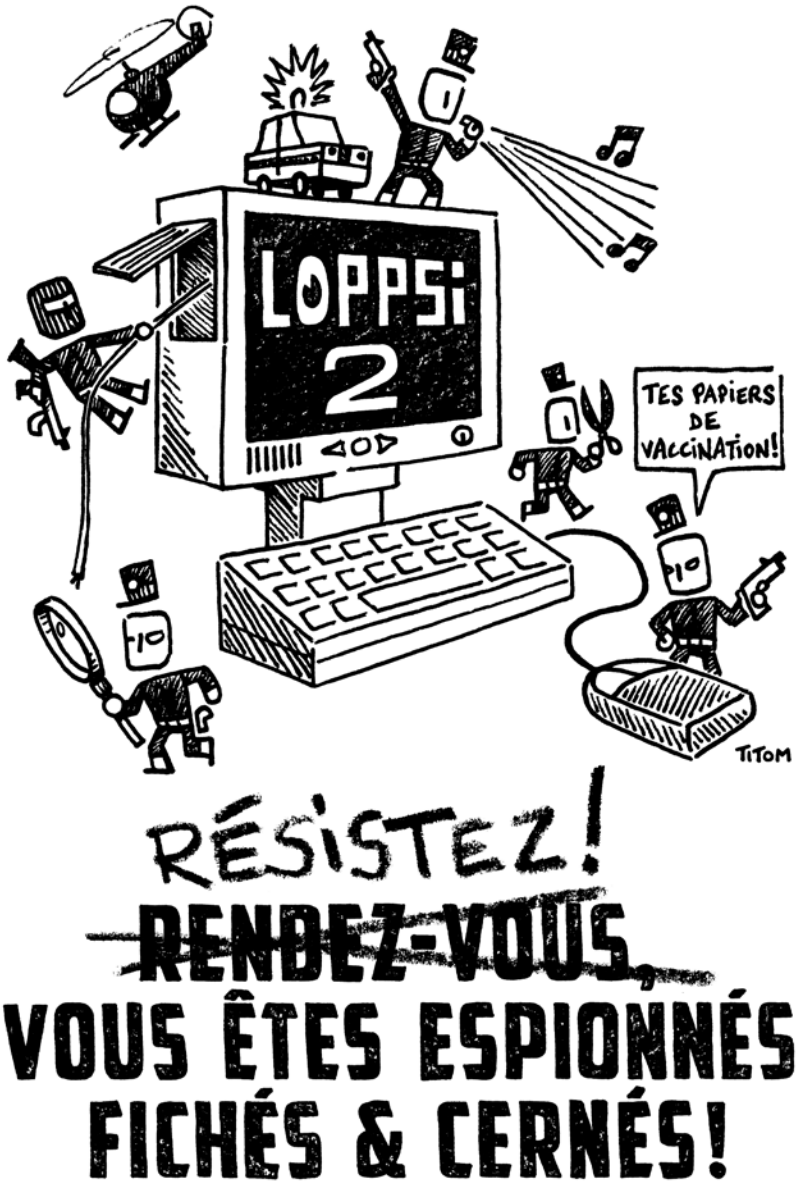
DÉVELOPPEMENT ET CROISEMENT DES FICHIERS

Cette loi coordonne les fichiers, tels le STIC et le JUDEX, qui contiennent des "données à caractère personnel" concernant les personnes suspectées d'avoir participé à un crime, un délit ou à une contravention de 5e classe. Le texte prévoit que les décisions d'acquittement ou de relaxe conduisent à un effacement des données, sauf si le procureur de la République en prescrit le maintien. Il lui donne aussi le pouvoir d'effacer les informations personnelles ou de les maintenir dans le fichier, en cas de non-lieu ou de classement sans suite.
La loi permet aussi d'utiliser des systèmes de recoupement automatique qui croisent des données publiques, disponibles sur Internet, avec des données privées : IP et numéro de téléphone. Il s'agit d'informations nominatives sur les personnes suspectées d'être auteurs ou complices de crimes ou de délits, mais aussi sur les victimes ou simplement sur des personnes susceptibles de fournir des renseignements. Quant aux fichiers dits "de rapprochement", ils vont permettre de croiser les informations nominatives, recueillies

dans des enquêtes et cela sans aucune limite en termes de gravité des infractions concernées.

DANS LE "REGARD" DU POUVOIR

La loi apparaît comme une collection de mesures disparates, allant de la constitution de fichiers sur la population, de la légalisation des mouchards électroniques, à la criminalisation des squatters ou à la possibilité d'installer un couvre-feu pour les enfants de moins de 13 ans. Il a cependant une forte cohérence, non pas au niveau des différents objets, mais dans l'intentionnalité du pouvoir. Ces délits n'ont d'ailleurs pas d'autres finalités que d'être des supports de l'image de l'insécurité et de son alter ego, la sécurité.
La criminalisation des squatters, des gens du voyage, des étrangers en situation irrégulière ou simplement des jeunes, sous-entend que toute forme d'existence, qui n'est pas étroitement contrôlée, est dangereuse. Il est ainsi induit que la sécurité réside dans un abandon complet aux initiatives du gouvernement, à ses différents fichiers et à ses perquisitions informatiques.
Ce n'est pas pour rien que la loi opère un déplacement sémantique en remplaçant "vidéosurveillance" par "vidéoprotection". Cette mutation n'est pas destinée à nous tromper. Elle s'inscrit au contraire dans la transparence, celle de l'intention du gouvernement, de Big Mother et de sa gouvernance fusionnelle. Ainsi, la sécurité, la protection octroyée, consiste aussi bien à être dans l'œil des caméras de surveillance généralisées par la LOPPSI 2 qu'à être repris et conservé dans les fichiers de police, même si on a été acquitté par la justice. Le but n'est pas d'établir une surveillance. Une enquête de la CNIL nous avait déjà appris que, en 2008, les fichiers policiers comprenaient 83 % d'erreurs.
L'objectif est tout autre, il s'agit de nous intimer que notre protection consiste à nous abandonner à l'État et à renoncer au droit à une vie privée. ■



L'antécédent du Patriot Act

La plupart des mesures établies par la LOPPSI 2, l'installation de chevaux de Troie dans un ordinateur, la constitution de fichiers de croisement de données personnelles, la création de l'incrimination de cybercriminalité, alias cyberterrorisme, font déjà partie du Patriot Act étasunien, voté immédiatement après les attentats contre les tours du World Trade Center. Développé par le FBI, le système Carnivore, rebaptisé depuis DCS 1000, permet, entre autres, de récupérer le contenu des courriers électroniques, ainsi que les données de connexion. Avant les attentats, ce système ne pouvait être utilisé qu'avec l'accord préalable d'un juge. Le Combating Terrorist Act, voté de toute urgence, le 13 septembre 2001 par le Sénat, a exempté les services de sécurité de cette autorisation.
Ainsi, la surveillance de la Toile a été définitivement légalisée par le Patriot Act. Cette loi a autorisé le FBI à brancher le système Carnivore sur le réseau d'un fournisseur d'accès afin de surveiller la circulation des courriers électroniques et de conserver les traces de navigation d'une personne suspectée de contact avec une puissance étrangère. L'aval d'une juridiction spéciale suffit pour un branchement.
Carnivore fonctionne par mots-clefs. Il passe au peigne fin l'ensemble des courriels entrant ou sortant des serveurs des fournisseurs d'accès étasuniens afin de chercher des adresses déterminées. Ce système est capable de copier les données transmises par les internautes, adresses visitées et contenus des courriels, sans passer par l'intermédiaire de boîtes noires. Il utilise des filtres en fonction de la nature de l'écoute.
Pour le FBI, la collaboration des fournisseurs d'accès est indispensable afin de pouvoir utiliser cette procédure. En effet, ce sont eux qui stockent les courriers électroniques et qui en assurent le relais à travers Internet. Carnivore serait capable de reconstruire chaque page Web visionnée par un internaute.