Projet de loi sur le renseignement : « dangereux », « liberticide », « stupide »

Alors que le projet de loi antiterroriste, concocté par le député PS Jean-Jacques Urvoas et dont les grandes lignes ont été dévoilées hier par le Figaro, est présenté ce matin en Conseil des ministres, les réactions commencent à fuser. Rappelons que ce projet de loi, qui sera défendu par le Premier ministre Manuel Valls (en photo ci-dessus), étend les capacités des services de renseignement au moins sur deux plans. D'un côté, ces derniers vont pouvoir avoir recours, **sur simple décision administrative, à des techniques spéciales d'écoute** ou de suivi (balises GPS, keyloggers enregistrant toutes les frappes des claviers, micros, introduction sur des systèmes tiers, utilisation de fausses bornes mobiles appelées IMSI Catcher). Autant de techniques déjà bien connues des services de renseignement, mais aujourd'hui limitées aux seules cas approuvés par un juge. Tout du moins en théorie. Notons que l'emploi de ces méthodes n'est pas limité à l'antiterrorisme mais couvre également « *la Défense Nationale, les intérêts de politiques étrangères, les intérêts économiques et scientifiques majeurs* ». Mais aussi une très vague formulation portant sur « *les violences collectives pouvant porter gravement atteinte à la paix publique* ».

L'autre volet du projet de loi porte sur la **collaboration des acteurs du Net** (FAI, hébergeurs, opérateurs, plates-formes de service), appelés à transmettre immédiatement les données de connexion des suspects, à remettre aux autorités les moyens permettant de déchiffrer les conversations cryptées et à détecter proactivement les comportements suspects (« *détecter, par un traitement automatique, une succession suspecte de données de connexion* »). Des relations qui seront couvertes par **le secret défense**. Selon NextInpact, la détection de ces comportements suspects reposerait sur des **boîtes noires, fournies aux opérateurs par les autorités**. Ces boîtiers, approuvés par une commission de contrôle, viseraient à détecter des comportements pouvant indiquer un lien avec le terrorisme, via l'analyse des métadonnées (et non des contenus des communications elles-mêmes). Bref, le gouvernement mise sur **le Big Data** pour éviter de s'engager dans une coûteuse solution 'à la NSA' consistant à stocker un maximum de données sur tous les utilisateurs pour ensuite disposer d'informations pertinentes sur des suspects.

En janvier dernier, dans un entretien chez nos confrères de l'Opinion, Jean-Jacques Urvoas expliquait : « *Par philosophie, mais aussi à cause de nos capacités juridiques ou financières limitées, nous allons créer un système aux antipodes de la surveillance de masse. Ce sera un harpon et pas un chalut !* ». Même si le harpon semble tout droit sorti de Minority Report, la nouvelle de Philip K . Dick, où des individus sont arrêtés pour les crimes qu'ils s'apprêtent à commettre.

Les grandes lignes du projet suscitent déjà de nombreuses réactions. Notons que le gouvernement a mis en place une concertation avec l'industrie. **Les associations représentatives seront ainsi reçues cette après-midi à Matignon**, tandis que l'Intérieur a engagé un dialogue direct avec les sociétés concernées. Un dialogue évidemment essentiel tant les modalités d'application de la loi peuvent en changer la nature. Mais d'ores et déjà, nombreuses sont les voix qui s'élèvent pour souligner les dérives que comporte ce texte.

Quadrature du Net : « une incroyable dérive »

La Quadrature du Net, association de défense des droits et libertés des citoyens sur Internet, a défouraillé la première. Dans un texte publié dès le 17 mars, l'association dénonce « *l'instrumentalisation sécuritaire des événements meurtriers de janvier* » (les attentats contre Charlie Hebdo et l'Hyper cacher) qui « *risque d'aboutir à une incroyable dérive du gouvernement en matière de surveillance des citoyens* ». La Quadrature pointe notamment la conservation des données de connexion recueillies par les services pendant 5 ans et la faiblesse du contrepouvoir imaginé par le texte : « *une commission consultative, aux pouvoirs limités, ne permettant des recours qu'a posteriori et sans garanties réelles pour les citoyens* ».

Syntec Numérique : « de plus en plus liberticide »

Dans un communiqué diffusé avant même la présentation officielle du texte en Conseil des ministres, Syntec Numérique exprime son « *inquiétude face à des mesures de plus en plus liberticides pour les citoyens et les entreprises* ». Et de mettre en exergue quatre d'entre elles : la fin du caractère exceptionnel des écoutes, l'absence de garde-fou sur la géolocalisation, l'obligation de déchiffrement pour les entreprises et l'absence de garanties pour les données exploitées et collectées. Syntec Numérique relève encore les nouvelles obligations qui pèseront sur les opérateurs et autres intermédiaires astreints à mettre en place ce que le syndicat professionnel voit comme de la « *surveillance prédictive* » et à « *apporter leur aide au déchiffrement des données* ».

Renaissance numérique : « CNCIS essentielle… donc remplacée »

Le think tank Renaissance Numérique, qui avait publié en janvier une lettre ouverte à Jean-Jacques Urvoas, appelant l'Etat à plus de dialogue sur les questions relatives à la surveillance d'Internet, regrette que ses demandes de rencontre avec le Président de la Commission des lois de l'Assemblée nationale soient restées lettre morte. Dans un mail à la rédaction, Guillaume Buffet, le président de Renaissance Numérique, se refuse à anticiper sur des mesures qui restent à détailler. Mais s'étonne de la manière dont la CNCIS (Commission nationale de contrôle des interceptions de sécurité) est supplantée par une nouvelle autorité administrative, la Commission nationale de contrôle des techniques de renseignement (CNCTR), présentée par le gouvernement comme plus étoffée et dotée de compétences techniques approfondies. « *Seul espace de contre-pouvoir actuel, il mériterait au moins d'être repensé avec l'avis et/ou la participation des associations citoyennes et non pas à l'initiative de ceux qui doivent être contrôlés*, commente Guillaume Buffet. *Il est d'autre part… étonnant de noter que cet organe qui nous a été présenté depuis l'origine comme le parfait rempart et la démonstration de l'inutilité de nos requêtes soit finalement potentiellement réinventé*. » Joint au téléphone ce matin, Guillaume Buffet estime avoir besoin d'un éclairage plus précis sur cette prochaine autorité : « *on entend dire que la nouvelle commission serait fondée à mener des perquisitions chez les opérateurs et FAI. Dans ces conditions, on voit mal en quoi elle pourrait être un quelconque contrepouvoir.* »

Tristan Nitot : « le recours à l'algorithmique »

S'il ne nie pas l'utilité du travail des services de renseignement, Tristan Nitot, qui a quitté la fondation Mozilla pour rejoindre la start-up Cozy Cloud, qualifie de « *catastrophe* » le texte de loi. « *L'implication envisagée des grands opérateurs de service et des FAI pour détecter les comportements suspects est extrêmement préoccupant. Cette idée d'algorithmique (embarquée dans les fameuses boîtes noires, NDLR) me met très mal à l'aise. On s'éloigne encore plus de la logique judiciaire. Comme si la voie administrative elle-même n'était plus assez rapide.* » Le défenseur du logiciel libre y voit le plus gros point noir du projet de loi : « *certes, contrairement à ce que fait la NSA, on ne va pas capturer toutes les données, mais on va bien tout surveiller ! De fait, cela signe la mise en place de la surveillance de masse* ». L'autre motif d'inquiétude de Tristan Nitot réside dans l'introduction de backdoors dans les systèmes de cryptographie : « *C'est stupide et je pèse mes mots. Car tous les pays vont demander la même chose, ce qui va poser de gros problèmes en matière de renseignement économique. Même si je ne vois pas pour l'instant les grands acteurs d'Internet céder sur ce point au gouvernement français* ».

Tristan Nitot relève tout de même deux points positifs dans le texte : la constitution d'une commission de contrôle « *plus musclée* » – « *et c'était nécessaire car la CNCIS était désemparée face au volume d'activités, mais la CNCTR aura-t-elle les moyens d'être indépendante ?* » – et le début d'un encadrement des IMSI Catcher, ces fausses bornes GSM servant aux interceptions. « *Peut-être y aura-t-il un peu moins d'hypocrisie sur le sujet* », espère l'ex-Mozilla qui écrit en ce moment un livre sur la vie privée et la surveillance de masse.

In fine, Tristan Nitot se demande si la crise de confiance qu'amènent les techniques de surveillance – crise filmée à hauteur d'homme dans le documentaire Citizenfour de Laura Poitras – ne sera bénéfique pas à long terme. « *Peut-être faut-il passer par cette défiance cathartique pour revenir à un système où les utilisateurs reprennent le contrôle de leurs données. Il ne faut pas oublier que le Cloud signifie avant tout l'utilisation de l'ordinateur de quelqu'un d'autre*. »

CNIL : « garanties insuffisantes »

Selon un document de travail que s'est procuré Le Monde, et qui serait quasi-définitif selon nos confrères, la Commission nationale de l'informatique et des libertés, saisie du projet de loi comme pour chaque texte relatif aux données personnelles et à la vie privée, émet plusieurs réserves. La Commission s'émeut notamment des volets concernant la collaboration active réclamée aux opérateurs et FAI : la collecte de métadonnées en temps réel sur les réseaux de communication et l'installation de systèmes de détection de comportements suspects. La CNIL estime que « *les garanties prévues pour préserver les droits et libertés ne sont pas suffisantes pour justifier une telle ingérence* ».

Même défiance affichée vis-à-vis des conditions d'utilisation des fausses bornes GSM (ou IMSI Catcher). Certaines de ces bornes ne se contentent pas de récupérer quelques données techniques de téléphones ciblés (une description aimable qui figurait dans la presse en début de semaine), mais détournent des communications dans une zone de couverture complète (dégradant au passage leur sécurité, via le passage de la 3G ou de la 4G à des communications 2G facilement déchiffrables). Or la CNIL remarque que ces équipements sont soumis à un système de contrôle plus lâche que les autres moyens d'espionnage. *« Un tel dispositif permettra de collecter de manière systématique et automatique des données relatives à des personnes pouvant n'avoir aucun lien ou un lien purement géographique avec l'individu effectivement surveillé »*, pointe fort justement la Commission.

A lire aussi :

La France bricole un Patriot Act du pauvre

Après les attentats : l'Intérieur bricole un plan d'action, pas un Patriot Act

Loi anti-terroriste : un arsenal tout juste renforcé et bientôt chamboulé ?

Accès administratifs aux données de connexion : pareil qu'aujourd'hui… mais en pire

Crédit photo : © gouvernement.fr