Date de dépôt : 12 septembre 2013

Réponse du Conseil d'Etat

à la question écrite urgente de M. Michel Forni : Le loup n'est plus dans la bergerie

Mesdames et
Messieurs les députés,

En date du 28 juin 2013, le Grand Conseil a renvoyé au Conseil d'Etat une question écrite urgente qui a la teneur suivante :

Les faits se passent de commentaires.

Genève est éclaboussée par l'affaire Snowden qui rebondit des Etats-Unis en passant par la Chine, la Russie et l'Equateur, suite aux révélations de cet informaticien, ex-employé de la CIA.

Les fuites sur les méthodes de surveillance généralisée des communications par l'Agence de sécurité américaine (NSA), hors USA, mettent au grand jour ce dispositif d'espionnage qui permet d'écouter et d'intercepter les communications et les données « sensibles ».

Les révélations confiées au Guardian laissent à penser que l'équivalent britannique de la NSA a pu également intercepter de nombreuses communications sur le réseau de fibres optiques ainsi que dans les e-mails, en collaboration avec le Service de Renseignement américain.

Certes, comme l'a rappelé le patron de la NSA, le général Keith Alexander : les communications concernant les citoyens américains sont spécialement protégées en vertu de leur constitution.

Genève semble être une plateforme pour l'espionnage, et pour la récupération de données, phénomène pouvant également créer de l'intoxication, de la délinquance économique et financière.

Il ne s'agit plus d'agiter l'épouvantail de la sécurisation excessive mais de bien mettre à l'abri notre cyberdémocratie qui accompagne la civilisation du numérique dans ses potentialités et également dans le zapping des idées.

Il n'y a pas de place pour l'abattement ni pour un sentiment d'impunité, même si les armes dissuasives sont difficiles à trouver dans une Suisse coincée entre l'arsenal sécuritaire américain et les zones de libre-échange européen.

Il n'est jamais bon de légiférer sous le coup de l'émotion ni à la recherche de plans de moralisation, notamment ceux développés par nos voisins contre la fraude fiscale ou dans le sens d'une prévention de la corruption avec un arsenal répressif qui englobe des techniques spéciales d'enquête (surveillance, infiltration, captation de données informatiques ou même vol de ces dernières, ...) en y associant souvent des moyens exorbitants.

Hors de Genève, « l'accessibilité » à des données gérées par les géants de l'internet au profit des services de renseignements des Etats-Unis et le scandale qui en résulte, permettent d'observer les premiers coups de semonce d'une riposte proportionnée. Les autorités européennes souhaitent frapper fort.

Certains pays sont en mesure de confirmer les infractions constatées en matière de protection de données et confirment qu'il y a bien violation du droit européen.

Certes, le régulateur britannique a enjoint Google à supprimer les données récupérées lors d'opérations de photographie de rue, sous peine de sanctions, et, dans le même temps, le scandale Prism a éclaté confirmant l'écoute et l'interception de communications sur des réseaux téléphoniques et des réseaux sociaux (internet).

Le groupe californien s'autorise à analyser les informations (contenu des e-mails, site web) dans une soixantaine de services (dont les moteurs de recherche Gmail, You tube, Google Rive) ce qui lui permet de dresser le profil précis des utilisateurs et également des données qui y sont associées.

Les commissions nationales de l'informatique et de liberté (CNIL) ont engagé des procédures de sanction qui donnent trois mois à Google, en particulier, pour se mettre en conformité avec le droit européen.

Genève est touchée et un certain brouillard plane sur notre cité car les dispositifs énumérés par l'ex espion Snowdon, laissent à penser que nos hôtes les organisations internationales, nos forteresses bancaires, nos centres de recherche, sont bel et bien espionnés par un système sophistiqué.

Au vu de ce qui précède, mes questions sont les suivantes :

- ***Quels sont les dispositifs cantonaux ou fédéraux qui doivent être engagés par analogie au CNIL européen ?***
- ***Que fait Genève pour faire respecter l'article 271 du Code pénal suisse face à ce type de cyber espionnage made in USA ?***

RÉPONSE DU CONSEIL D'ÉTAT

Le Conseil d'Etat est en mesure de répondre aux deux principales questions du député M. Michel Forni de la manière suivante :

Quels sont les dispositifs cantonaux ou fédéraux qui doivent être engagés par analogie au CNIL européen ?

La question que soulève un programme tel que PRISM cumule deux problématiques : celle portant sur l'espionnage électronique par une entité étatique étrangère et celle relative à la protection des données à caractère personnel.

Concernant l'aspect de l'espionnage, on notera à titre liminaire que le groupe européen des autorités de protection (ci-après : « CNIL Europe ») ne semble *a priori* pas particulièrement armé pour protéger la population européenne contre les programmes massifs d'espionnage du type ECHELON (téléphonie), UPSTREAM (câbles optiques) ou PRISM (serveurs des entreprises majeures de l'internet, dès 2007). C'est ainsi que par une note du 14 juin 2013, la CNIL française a annoncé la « *création d'un groupe de travail sur l'accès des autorités publiques étrangères à des données personnelles de citoyens français* »[1].

La loi cantonale sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD – A 2 08) et la loi fédérale sur la protection des données (LPD – RS 235.1) indiquent que la responsabilité de la confidentialité des données personnelles incombe au responsable du traitement des données LIPAD (appelé « maître du fichier » par la LPD); dans ce cadre, un programme d'espionnage mené par une entité étrangère ne correspond pas aux types d'accès indus de tiers pour lequel ces lois envisagent de prime abord d'engager la responsabilité des personnes en charge du traitement des données.

[1] http://www.cnil.fr/linstitution/actualite/article/article/creation-dun-groupe-de-travail-sur-lacces-des-autorites-publiques-etrangeres-a-des-donnees/,

En outre, un programme comme PRISM permet au gouvernement américain d'obtenir *a priori* légalement des informations de la part non pas des « maîtres de fichier », mais des fournisseurs de service à qui ces données sont confiées, que ce soit de manière récurrente ou momentanée. Tout au plus peut-on en conclure que les Etats-Unis ne font désormais plus partie des Etats assurant par leurs lois une protection similaire à celle offerte par la LPD aux données personnelles. Encore faudra-t-il prouver que la notion de prévention contre le terrorisme, officiellement mise en avant pour justifier la mise en œuvre de ce type de programme, a été interprétée par le gouvernement étasunien de manière non proportionnelle.

La lutte contre l'espionnage électronique émanant d'autorités étrangères n'est enfin pas du ressort des autorités cantonales genevoises en charge de la protection des données. Ceci dit, la LIPAD fait déjà obligation à un maître de fichiers d'annoncer tout hébergement ou transmission volontaire de données personnelles à l'étranger.

Concernant l'aspect protection des données, l'équivalent suisse du contrôleur européen à la protection des données (CEPD) n'est autre que le préposé fédéral à la protection des données (PFPD). À l'échelle cantonale, il s'agit des préposé(e)s cantonaux à la protection des données et à la transparence (PPDT). M. Jean-Philippe Walter, préposé fédéral adjoint à la protection des données, a confirmé ces points, tout en reconnaissant avoir peu de moyens pour lutter contre ce type d'atteintes :

« *Le PFPDT a pris connaissance des révélations relatives au programme PRISM. Il s'agit d'activités de renseignement menées par un Etat étranger pour lequel le PFPDT n'a pas ou peu de moyens d'intervention. Le PFPDT n'intervient que dans la mesure où des traitements de données personnelles interviennent en Suisse et sont le fait d'organes fédéraux ou de personnes privées. Dans le cas qui vous occupe, une intervention de notre part pourrait concerner des organes fédéraux ou des personnes privées qui livreraient des données aux autorités américaines. Cette communication de données ne pourrait intervenir que pour autant que le droit suisse le permette et que les dispositions de loi fédérale sur la protection des données soient respectées. […] D'autre part, les responsables de traitement doivent veiller à la sécurité des données qu'ils détiennent et prendre toutes les mesures qui s'imposent pour éviter qu'un tiers puisse y avoir accès sans droit.* »

Il convient d'ajouter que la responsabilité des maîtres de fichiers ne peut sérieusement pas être invoquée s'agissant de courriels envoyés de Suisse à Suisse, et qui, en application des règles d'aiguillage de l'information instaurées sur l'internet, viendraient à passer par le territoire des Etats-Unis, ou pour des intrusions sur des machines bénéficiant d'éventuelles « portes arrière » (« *back doors* ») engrammées dans les processeurs de production américaine à l'attention des agences de leur gouvernement. Les mesures de sécurité attendues des maîtres de fichiers ne sauraient en effet excéder les règles correspondant à la bonne pratique du moment.

Les actions envisageables vont donc d'une injonction au préposé fédéral à la protection des données et à la transparence (PFPDT) et à la préposée cantonale (PPDT) afin d'envisager les mesures qu'il serait possible de renforcer pour tenir compte de tels programmes d'espionnage (par exemple quant au statut à accorder pour les garanties étasuniennes légales en matière de réciprocité LPD), à la sensibilisation du public concerné. Il semble toutefois que le PFPDT n'y réagira pas dans le sens attendu par le député auteur de la présente question, puisqu'il a jugé utile de ne pas refuser le « *Safe Harbour* » aux États-Unis après la révélation du programme PRISM; le PFPDT semble donc estimer que les Etats-Unis offrent toujours sur leur territoire une garantie similaire à celle de la Suisse en matière de protection des données personnelles.

Il convient enfin de remarquer que plusieurs des sociétés étasuniennes soupçonnées d'avoir coopéré avec leur gouvernement dans le cadre du programme PRISM, soit Microsoft (dès 2007), Yahoo! (2008), Google (2009), Facebook (2009), Paltalk (2009), YouTube (2010), Skype (2011), AOL (2011) et Apple (2012), affirment n'avoir collaboré et transmis d'informations que de manière ponctuelle et non pas massive comme les documents transmis par Edward Snowden semblent le suggérer[2]. Les doutes qui peuvent raisonnablement planer sur de telles récusations ne semblent pas pouvoir pour autant être juridiquement prouvés à ce stade.

[2] Source : Edward Snowden, répercuté par l'article Wikipedia sur PRISM (http://fr.wikipedia.org/ wiki/PRISM(programme_de_surveillance).

Que fait Genève pour faire respecter l'article 271 du code pénal suisse face à ce type de cyber espionnage made in USA ?

Pour mémoire, l'article 271 du code pénal suisse (CPS) stipule :

Actes exécutés sans droit pour un Etat étranger

1. *Celui qui, sans y être autorisé, aura procédé sur le territoire suisse pour un Etat étranger à des actes qui relèvent des pouvoirs publics,*

   celui qui aura procédé à de tels actes pour un parti étranger ou une autre organisation de l'étranger,

   celui qui aura favorisé de tels actes,

   sera puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire et, dans les cas graves, d'une peine privative de liberté d'un an au moins.
2. *Celui qui, en usant de violence, ruse ou menace, aura entraîné une personne à l'étranger pour la livrer à une autorité, à un parti ou à une autre organisation de l'étranger, ou pour mettre sa vie ou son intégrité corporelle en danger, sera puni d'une peine privative de liberté d'un an au moins.*
3. *Celui qui aura préparé un tel enlèvement sera puni d'une peine privative de liberté ou d'une peine pécuniaire.*

L'article 271 CPS (dont à l'évidence seul l'alinéa 1 pourrait être topique) ne semble pas adapté pour régler la question de l'espionnage économique et l'espionnage des données à caractère personnel tels que pratiqués par le programme PRISM. Il n'est tout d'abord pas certain que le législateur, par l'action de « *procéder à des actes relevant des pouvoirs publics* », ait visé la surveillance électronique, ne fût-ce qu'en raison de l'existence de l'article 272 CPS (voir ci-après). En outre, l'infraction doit avoir eu lieu « *sur le territoire suisse* » (al. 1), alors qu'un programme comme PRISM opère essentiellement à travers le « *cloud computing* »[3]. Il faut en effet rappeler que

[3] « Le *cloud computing* est une nouvelle manière de fournir et d'utiliser les aptitudes des systèmes informatiques, qui est basée sur les *nuages* (*cloud* en anglais) : un parc de machines, d'équipement de réseau et de logiciels maintenu par un fournisseur, que les consommateurs peuvent utiliser en libre-service via l'internet. Les caractéristiques techniques du nuage ne sont pas connues du consommateur et les services sont payés à l'usage. » (Wikipedia, l'encyclopédie libre, citant Rajkumar BUYYA, James BROBERG, Andrzej M. GOSCINSKI, *Cloud Computing: Principles and Paradigms*, John Wiley & Sons, 2010 ; Lee GILLAM, *Cloud computing*, Springer –

l'internet a été conçu pour résister à une attaque nucléaire et les chemins sur ce réseau n'obéissent donc pas nécessairement à une logique de proximité géographique, mais de moindre coût en fonction de la bande passante. Cela explique que la plupart des messages mondiaux soient susceptibles de passer par les Etats-Unis, étant précisé qu'il n'est jamais possible de prédire le chemin concret d'un message; c'est à cette occasion qu'ils sont interceptés par les autorités étasuniennes[4]. L'article 271 CPS n'est alors à l'évidence pas applicable.

L'article 272 CPS (« Espionnage ») semble à première vue plus adéquat pour gérer la situation soulevée dans la présente question. Pour mémoire, cet article stipule :

> ***Espionnage***
>
> *Service de renseignements politiques*
>
> 1. *Celui qui, dans l'intérêt d'un Etat étranger, ou d'un parti étranger ou d'une autre organisation de l'étranger, et au préjudice de la Suisse ou de ses ressortissants, habitants ou organismes, aura pratiqué un service de renseignements politiques, ou aura organisé un tel service,*
>
> *celui qui aura engagé autrui pour un tel service ou favorisé de tels agissements,*
>
> *sera puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.*
>
> 2. *Dans les cas graves, le juge prononcera une peine privative de liberté d'un an au moins. Sera en particulier considéré comme grave le fait d'avoir incité à des actes propres à compromettre la sûreté intérieure ou extérieure de la Confédération ou d'avoir donné de fausses informations de cette nature.*

Il n'est toutefois pas certain qu'une activité d'espionnage politique au sens strict puisse être soulevée ici, puisque celle-ci est officiellement justifiée par la lutte contre le terrorisme. A titre d'exemple, il est utile de rappeler que pour se prémunir contre l'« espionnage économique », la France a dû se doter le

---

2010 ; Judith HURWITZ - Robin BLOOR - Marcia KAUFMAN - Fern Halper, *Cloud Computing for Dummies*, John Wiley & Sons – 2009.

[4] http://commons.wikimedia.org/wiki/File:Prism_slide_2.jpg

24 janvier 2012 d'un délit de violation du « secret des affaires »[5]. Encore faut-il que l'espionnage électronique porte sur des données de caractère économique (données financières, commerciales, scientifiques ou techniques relevant du secret des affaires), ce qui n'est pas le cas s'agissant de données à caractère personnel. En outre, le maintien du « *Safe Harbour* » par le PFPDT renforce cette position.

La solution semble donc pour la Suisse d'adopter une disposition pénale *ad hoc*. Enfin, un projet de modification de la loi fédérale sur le renseignement civil (LFRC – RS 121), dont le Conseil fédéral vient d'approuver, le 13 août 2013, le message[6] et le projet de modification à l'attention du Parlement[7], pourrait permettre au Service de renseignement civil suisse (SRC) de mieux assurer la sécurité des données face aux Etats étrangers, par la collaboration plus étroite qu'elle assure entre la Confédération et les cantons. Ce projet introduit toutefois un droit d'accès direct (droit d'être informé) en faveur du Service de renseignement civil suisse (SRC) en vertu des dispositions des articles 8 et 9 de la loi fédérale sur la protection des données (LPD).

Au bénéfice de ces explications, le Conseil d'Etat vous invite, Mesdames et Messieurs les Députés, à prendre acte de la présente réponse.

AU NOM DU CONSEIL D'ÉTAT

La chancelière :	Le président :
Anja WYDEN GUELPA	Charles BEER

[5] Projet de loi : http://www.scribd.com/doc/79216284/Loi-violation-du-secret-des-affaires

[6] http://www.news.admin.ch/NSBSubscriber/message/attachments/31524.pdf.

[7] http://www.vbs.admin.ch/internet/vbs/fr/home/documentation/news/news_detail.49856.nsb.html.