Ne soyons pas indignés mais réalistes sed quis custodiet ipsos custode ?

cahier de la pensée mili-Terre

le Chef de bataillon Jean-Jacques GRUND

publié le 10/06/2018

Autres thèmes

Il faut dépasser le stade de l'indignation provoquée par l'affaire Snowden et être réaliste en acceptant le fait que le monde numérique de l'Internet ne doit pas échapper à l'action de l'État car il est au cœur d'enjeux à la fois économiques et sécuritaires.

Les temps modernes se caractérisent par la place centrale qu'occupe la notion de liberté. Le séisme qu'a occasionné Edward Snowden lorsqu'il a révélé l'importance du contrôle exercé par l'agence de renseignement technique américaine, la NSA, sur une grande partie des échanges de données sur la «toile», a suscité l'indignation générale, et plus particulièrement celle des pays ou organisations supposées proches des États-Unis d'Amérique.

Pourtant, ce qui est apparu au grand jour n'est que la conséquence logique de la liberté offerte par la révolution numérique au travers de la démocratisation de l'Internet. Malgré une infrastructure coûteuse, la majorité des services communément utilisés sont gratuits. Il est donc naturel de se demander qui paye la note. L' «affaire Snowden» n'a fait que répondre à la question que personne ne veut poser. L'architecture d'Internet n'est viable gratuitement que si nous pouvons observer en échange de pouvoir être observés. L'analyste américain n'a donc fait que mettre en évidence une réalité: le monde de l'Internet tient plus du bazar que de l'agora.

Il convient donc dès à présent de dépasser le stade de l'indignation et d'être réalistes en acceptant le fait que le monde numérique de l'Internet ne doit pas échapper à l'action de l'État car il est au cœur d'enjeux à la fois économiques et sécuritaires.

Il doit donc rester sous la vigilance ou le contrôle étatique pour des enjeux relevant de l'intérêt national. La révolution numérique reste toutefois un facteur multiplicateur d'efficacité et de profit qu'il convient de savoir utiliser en toute connaissance de cause afin d'en conserver la maîtrise. Cela ne peut se faire que par l'éducation de tous les

utilisateurs.

Il est normal d'être mécontents par le fait que nous soyons l'objet de la surveillance de notre propre allié. C'est cette trahison supposée qui est remise en cause et non le fait que l'État puisse et doive exercer une certaine maîtrise sur le monde de l'Internet, au cœur d'un conflit entre liberté et contrôle. Le citoyen du monde peut en effet estimer que sa liberté a été bafouée et ses droits violés. Cependant, il n'a pas le droit d'en être indigné. En effet, Internet est un espace d'auto-exhibition, même pour les plus discrets. S'y connecter signifie de façon implicite se montrer au travers des données personnelles ou impersonnelles envoyées, y compris celles de géolocalisation. Qui n'a jamais envoyé de message électronique, partagé des photos ou fait des recherches sur la «toile»? En faisant cela, nous n'ignorions pas, mais occultions le fait que nous diffusions des informations qui échappaient à notre contrôle. Ces métadonnées, parfois partagées de façon inconsciente, sont quotidiennement récupérées par des sociétés commerciales. Elles nous proposent des services gratuits et vendent nos données à des sociétés tierces qui profilent nos habitudes de consommateurs afin de nous vendre des produits adaptés. Il s'agit des conséquences d'un contrat numérique implicite où se connecter à la toile pour récupérer des informations implique en même temps de donner des informations personnelles.

Au-delà de cette exploitation mercantile de la révolution numérique par des sociétés commerciales intrusives, l'Internet est au cœur d'enjeux qui relèvent de l'intérêt national des États. En effet, l'apparition d'outils numériques pour la plupart gratuits a conduit les sociétés criminelles ou terroristes à les utiliser afin de rendre anonymes leurs communications et les échanges financiers. En noyant leurs flux dans ceux de centaines de millions d'usagers, elles espèrent échapper au contrôle traditionnel des États. C'est pourquoi, il est crucial que ces derniers aient les outils techniques et législatifs pour pouvoir récupérer ces mêmes données involontairement offertes à la toile afin d'identifier et de traquer l'illicite, le criminel. Ils doivent donc se doter des capacités pour identifier et extraire les numéros de téléphones, les relations ou les localisations permettant de cibler ces entités terroristes ou criminelles. Ç'est globalement le cas pour l'ensemble des pays industrialisés et pas seulement les États-Unis. C'est la raison pour laquelle nous ne pouvons condamner ces derniers parce qu'ils possèdent ou utilisent ce genre d'outils, avec la démesure propre à ce pays, afin de mieux contrôler le cyberespace. Au contraire, ces mêmes pays collaborent pour lutter plus efficacement contre ces fléaux qui ont une empreinte mondiale.

Si le principe est compris par la plupart des citoyens, c'est donc bien l'objet du contrôle qui a pu les indigner. En effet, c'est le fait que leur propre gouvernement ait pu être ciblé, ou que leurs données personnelles aient pu être collectées qui a suscité cette vague de protestation. Dans le cadre de cette dialectique entre liberté et contrôle, les restrictions apportées à l'accès de ces données virtuelles ne sont pas techniques mais politiques. Seule la législation peut empêcher les entreprises de monnayer les informations récoltées sur Internet, mais alors se pose la question de l'équilibre financier sur lequel repose l'existence de la «toile». Seule la volonté politique peut contrôler et orienter les recherches des services de renseignements techniques, et alors se pose la question des raisons ayant poussé la NSA à espionner certaines ambassades ou dirigeants alliés.

Il s'agit donc de ne pas se laisser embarquer dans la spirale d'une polémique injustifiée autour de l'article 20 de la loi de programmation militaire (ex art. 13) sous prétexte des errements de la NSA dans l'affaire PRISM[1]. En effet, cette dernière jouit d'un régime d'exception dans le cadre du Patriot Act, qui lui permet de faire peu de cas des libertés individuelles. Il convient au contraire de réaliser une analyse dépassionnée permettant d'évaluer les enjeux: il faut rendre plus efficace et mieux encadrer législativement l'action des services étatiques dans leur lutte contre l'illicite tout en protégeant les citoyens des intrusions non justifiées dans leur vie privée.

Le texte adopté par le Parlement ne fait que donner des capacités juridiques plus étendues à nos services spécialisés tout en les encadrant plus strictement. Il ne remet pas en question le secret de correspondance, sanctuarisé par l'article L 241-1 du code de la sécurité intérieure. Les services ne pourront toujours pas accéder sans autorisation au contenu des correspondances électroniques ou aux données stockées dans des bases sans autorisation du juge. Le texte facilite uniquement l'accès aux données techniques de connexion, qui seront fournies sur demande par les opérateurs. Par analogie avec le courrier postal, cela revient à lire l'adresse de l'expéditeur et du destinataire. Ainsi, le citoyen n'a pas à craindre d'intrusions injustifiées dans sa vie privée. Au contraire, il dispose du droit de saisine au titre de l'article 243-9 de la commission nationale de contrôle des interceptions de sécurité (CNCIS), autorité administrative indépendante dont les services de sécurité connaissent l'intransigeance et dont l'importance a été soulignée par le Conseil constitutionnel. Les seuls qui pourraient légitimement se plaindre seraient les criminels et les terroristes, détectés plus aisément grâce aux facilités permises par la nouvelle loi et dont la correspondance pourra être lue après accord préalable du juge.

Il s'agit donc d'être réalistes et de ne pas limiter légalement la capacité d'action de nos services. Le nouveau texte répond à leurs besoins en unifiant et clarifiant le droit, en créant un seul et même régime là où auparavant existaient deux dispositifs, le premier découlant de l'interprétation de la loi de 1991 relative aux interceptions de sécurité tandis que le second avait été introduit par la loi relative à la lutte antiterroriste de 2006 et pour ce seul domaine. En créant un cadre juridique unique, l'action des services spécialisés est rendue plus efficace et clarifiée tout en facilitant le contrôle démocratique et citoyen de leur activité. Nous citions Juve nal en épigraphe: «Qui gardera les gardiens eux-mêmes?». Cette question a survécu pendant près de deux millénaires parce qu'elle est toujours demeurée pertinente. Là se situe en effet le cœur des enjeux du monde numérique. Il s'agit de la problématique du contrôle des activités étatiques et non étatiques autour de l'utilisation des données déposées sur la «toile» par les citoyens. Paradoxalement, c'est bien l'action des services de sécurité qui est la plus contrôlée. Il serait naïf de croire que l'action de la NSA ne fut pas autorisée au plus haut niveau politique et qu'elle échappa à tout contrôle. Les révélations de «l'affaire Snowden» n'ont donc de sens qu'en étant justifiées par la théorie de la raison d'État, dans un cadre de forte compétition économique et diplomatique au niveau mondial. Elles n'ont été permises que par notre extrême dépendance vis-à-vis des entreprises américaines dans le domaine des technologies de l'information. Ces dernières peuvent être contrôlées par le gouvernement américain, pour leur intérêt, tout en échappant facilement au nôtre. Ce qui s'est passé est de notre responsabilité car nous n'avons pas pu suivre la révolution numérique. Utilisons donc notre indignation pour rattraper notre retard.

La France a déjà débuté la réflexion et a conçu un plan numérique France 2020 afin de combler ses lacunes. Ce plan a identifié cinq défis dont la protection des données personnelles et de la vie privée, le cloud computing, la neutralité d'Internet ainsi que «l'amélioration de notre écosystème numérique pour stimuler les initiatives et soutenir les innovations». Nous voyons donc que l'enjeu va au-delà de la protection de la vie privée: il est économique. Dans le contexte de crise que nous connaissons depuis l'été 2008, l'économie numérique sera l'un des principaux supports qui nous permettra de retrouver la croissance. Elle représentait déjà un quart de la croissance de l'économie française en 2010[2] 700.000 emplois ont été créés en 15 ans. 450.000 de plus devraient être créés d'ici à 2015 . De plus, les investissements dans le numérique accroissent aussi la compétitivité de l'ensemble des autres secteurs de l'économie, notamment par l'utilisation des nouveaux services offerts comme le cloud computing et l'échange rapide d'information. Les entreprises présentes sur Internet croissent deux fois plus vite que les autres et exportent deux fois plus. L'économie numérique, c'est aussi de nouveaux services qui deviennent vite indispensables pour la vie quotidienne de nos concitoyens. Il s'agit donc que des entreprises françaises ou européennes puissent aussi rivaliser avec Yahoo ou Google, permettant ainsi une application des lois plus aisée car dans notre champ d'action. L'État doit avoir un rôle à jouer en soutenant le développement d'entreprises, actuellement en difficulté, qui ont en leur temps été à la pointe comme Alcatel-Lucent. Il doit aussi être réaliste et prendre en compte le fait que nous sommes au sein d'une guerre économique qui n'a jamais été aussi dure, surtout en période de crise, et que dans ce domaine il n'y a pas d'alliés. Le monde virtuel est le nouveau champ de bataille du XXI^{ème} siècle. L'État doit donc éduquer et préparer nos citoyens à affronter cette révolution numérique et les facilités qu'elle offre, qui sont à la fois une opportunité mais aussi une menace qui pourrait être exploitée par d'autres.

Nous sommes probablement entrés dans une seconde ère de l'Internet qui voit notre naïveté disparaître face aux risques qui se dévoilent au grand jour. Les équilibres entre liberté et contrôle, gouvernements et citoyens, fournisseurs de service et usagers, transparence et protection des données seront difficiles à obtenir. De nouveaux droits apparaîtront comme celui du «droit à l'oubli» et qu'il faudra garantir. De nouveaux procédés de protection et chiffrement, mais aussi juridiques, comme de nouvelles formes de coopération et de diplomatie devront être trouvés afin de prendre en compte la virtualité du monde numérique où la conflictualité n'en n'est pas moins âpre. Le grand défi du futur sera celui de la confiance. Le sociologue Niklas Luhmann a dit[3] que la confiance est une donnée élémentaire de la vie en société et qu'elle réduit la complexité de la vie sociale. Il s'agit donc d'obtenir cette même confiance dans le monde numérique afin d'y atténuer la suspicion.

[1] programme secret de surveillance conçu par la NSA pour intercepter les communications d'internautes étrangers.

[2] Rapport France numérique 2010-2020

[3] Niklas Luhmann, «La confiance, un mécanisme de réduction de la complexité sociale», Paris, Économica, 2006.

Ayant effectué une première partie de carrière dans le domaine de la guerre électronique et titulaire du brevet de l'enseignement militaire supérieur, le Chef de bataillon GRUND effectue actuellement une formation en mastère spécialisé à Telecom Paristech.

Titre :	le Chef de bataillon Jean-Jacques GRUND
Auteur(s) :	le Chef de bataillon Jean-Jacques GRUND
Date de parution	01/06/2018