Comité: Droits de l'Homme

Issue: Quelle sécurité dispensée pour protéger l'accès a l'information en ligne ?

Membre de l'état major: Nawrass Kamour

Position: Vice-présidente

Introduction :

Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes. En effet, l'article 12 de la déclaration universelle des droits de l'Homme consacre l'individu dans ses rapports avec les groupements qui l'entourent, et avec l'Etat dont il est citoyen. Ainsi, c'est bien l'individu que cet article protège en ses rapports avec les autres, tous les autres, qu'il s'agisse d'êtres humains ou d'institutions. De nos jours, internet fait partie de nos vies et représente pour l'humanité une opportunité de s'informer ainsi que de partager l'information. Et l'ONU indique que l'accès libre à Internet est quelque chose de primordial pour les droits de l'Homme. Il s'agit d'un article fondamental qui place l'individu sous une cloche protectrice. La protection de la vie privée de l'individu sera, par la suite, également consacrée par la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales, par le Pacte international relatif aux droits civils et politiques, par la Convention relative aux droits de l'enfant.Mais cette protection s'effrite sous les coups de buttoir de l'usage, de plus en plus intensif, de technologies nouvelles, que ce soit par des opérateurs économiques qui tendent à profiler les consommateurs par l'observation fine et approfondie de leurs modes de vie, que par les Etats qui cherchent à constituer des bases d'informations à fin de police, et à les enrichir sans cesse, afin de mieux connaître les citoyens, au détriment de la sphère de vie privée.
L'accès à l'information implique nécessairement l'accès à la formation et aux savoirs. Non seulement la pauvreté matérielle mais aussi la pauvreté intellectuelle contribuent à maintenir élevée la vulnérabilité d'une population, car elles creusent l'écart entre l'information à caractère scientifique et celle à caractère expérientiel, les deux étant essentielles à l'efficacité de tout plan de communication de crise.

A présent, il serait cruciale de se demander, quelles sécurités seraient les plus appropriées pour appréhender la notion d'accès a l'information en ligne. De cette manière, la notion de vie privée dans la déclaration universelle des droits de l'homme sera mise en évidence ainsi que le gouvernement face aux citoyens. De plus, l'étude de la protection de l'information parait être une évidence ainsi que le comite des droits de l'homme et le droit fondamental accorde par l'ONU. Pour finir, vous y trouverez en quoi la cybercriminalité adhère a la problématique et la position de certains pas ainsi que leurs actions et organisations face à la problématique.

Termes cles :

Vie privee : La vie privée est la capacité, pour une personne ou pour un groupe de personnes, de s'isoler afin de protéger ses intérêts. Les limites de la vie privée ainsi que ce qui est considéré comme privé diffèrent selon les groupes, les cultures et les individus, selon les coutumes et les traditions bien qu'il existe toujours un certain tronc commun.

Sécurité : Physiquement, la sécurité est l'état d'une situation présentant le minimum de risque. Psychiquement, la sécurité est l'état d'esprit d'une personne qui se sent tranquille et confiante. Pour l'individu ou un groupe, c'est le sentiment (bien ou mal fondé) d'être à l'abri de tout danger et risque.

Cybercriminalité : Un cybercrime est une « infraction pénale susceptible de se commettre sur ou au moyen d'un système informatique généralement connecté à un réseau ». Il s'agit donc d'une nouvelle forme de criminalité et de délinquance qui se distingue des formes traditionnelles en ce qu'elle se situe dans un espace virtuel, le « cyberespace ». Depuis quelques années la démocratisation de l'accès à l'informatique et la globalisation des réseaux ont été des facteurs de développement du cybercrime.

DUDH : La Déclaration universelle des droits de l'homme (DUDH) est adoptée par l'Assemblée générale des Nations unies le 10 décembre 1948 à Paris au palais de Chaillot. Elle précise les droits fondamentaux de l'Homme. Sans véritable portée juridique en tant que tel, ce texte n'a qu'une valeur d'une proclamation de droits.

Immixtion : Fait de s'immiscer, de s'ingérer indûment dans les affaires d'autrui.

Menace : Le fait qu'une personne ou une entité ait la possibilité ou bien l'intention (affichée ou non) d'infliger des blessures, la mort ou des dommages matériels à une autre personne ou groupe de personnes. Lorsque la cible subit des dommages qui n'est pas déterminée, on parle plutôt de danger

L'ONU déclarant l'accessibilité à internet comme droit fondamental :

Le Conseil affirme que les mêmes droits dont les personnes disposent hors ligne doivent être aussi protégés en ligne, en particulier la liberté d'expression, qui est applicable indépendamment des frontières et quel que soit le média que l'on choisisse, conformément aux articles 19 de la Déclaration universelle des droits de l'homme et du Pacte international relatif aux droits civils et politiques. Il invite tous les États à aborder les préoccupations de sécurité sur Internet conformément à leurs obligations internationales relatives aux droits de l'homme afin de garantir la protection de la liberté d'expression, de la liberté d'association, du droit à la vie privée et d'autres droits de l'homme en ligne, d'une manière qui garantisse la liberté et la sécurité sur Internet afin que celui-ci puisse rester une force dynamique génératrice de développement économique, social et culturel. Estimant que «les mêmes droits dont les personnes disposent hors ligne doivent être aussi protégés en ligne, en particulier la liberté d'expression», le Conseil des droits de l'homme de l'ONU en a profité pour condamner «sans équivoque les mesures qui visent à empêcher ou à perturber délibérément l'accès à l'information ou la diffusion d'informations en ligne».

La résolution, adoptée par consensus, a tout de même soulevé de l'opposition chez certains pays membres du Conseil, dont la Russie et la Chine. Tous deux souhaitaient voir des amendements apportés à la décision, notamment en ce qui a trait au déploiement et à la facilitation de l'accessibilité à internet sur leurs territoires. Au total, outre la Russie et de la Chine, 15 pays ont manifesté des réserves sur la résolution: le Bangladesh, la Bolivie, le Burundi, Cuba, le Congo, l'Équateur, l'Inde, l'Indonésie, le Kenya, l'Afrique du Sud, le Qatar, l'Arabie saoudite, les Émirats arabes unis, le Venezuela et le Vietnam. Bien que cette résolution soit non contraignante d'un point de vue juridique, elle envoie tout de même un message clair à la communauté internationale, et sera prise en compte pour établir les bilans annuels des États en matière de respect des droits fondamentaux. À ce chapitre, la résolution a également profité de l'occasion pour condamner fermement la censure et la surveillance étatique en ligne. Ainsi, le Conseil «appelle tous les États à aborder les questions de sécurité sur internet conformément à leurs obligations internationales en matière de droits de l'homme, pour assurer la protection de la liberté d'expression, la liberté d'association, la vie privée et d'autres droits de l'homme en ligne».

Pour cette résolution, l'ONU s'oriente sur l'article 19 de la Déclaration universelle des droits de l'homme, qui encadre le droit à la liberté d'opinion et d'expression depuis 1948. L'article 19 stipule que «tout individu a droit à la liberté d'opinion et d'expression, ce qui implique le droit de ne pas être inquiété pour ses opinions et celui de chercher, de recevoir et de répandre, sans considération de frontières, les informations et les idées par quelque moyen d'expression que ce soit».

Notion de vie privee :

Le droit consacre également que dans un état démocratique le gouvernement consulte et le gouvernement rendait compte au citoyen alors que dans ce cas on découvre que les programmes de surveillance n'avais jamais fait l'objet d'aucune information officielle ou certainement de reddition de compte. Les révélations Snowden donc soulève trois grands enjeux: premièrement le rapport est un citoyen. Deuxièmement l'imputabilité de l'État face aux citoyens. Et troisièmement le respect de la souveraineté étatique. La question revenant a plusieurs reprises et qui est aujourd'hui inevitables est : " je ne suis coupable de rien donc je n'ai rien a cacher ". Simplement le fait de poser la question c'est confondre culpabilité et intimité, l'intimité amoureuse de deux personnes n'a rien de coupable mais pourtant c'est privé! Les portes opaques, les rideaux, les vêtements, ne cachent rien de coupable mais préservent l'intimité, ils préservent cet espace vital dont on a besoin pour être soi-même pour être libre. On n'en vient à l'évidence que l'intimité préserve la liberté, et la liberté définit la démocratie. Ceci est l'enjeu ultime, c'est la démocratie. Ce qui nous ramène au premier enjeu soulevé par les révélations de Snowden qui sont le rapport État-citoyen. Parfois pour banaliser l'espionnage, la surveillance on dit avec humour que c'est la deuxième plus vieille profession du monde. Or l'État ne peut d'emblée aborder le citoyen comme un ennemi, c'est incompatible avec son devoir de protection du citoyen.

Il y a bien des circonstances où c'est justifié d'exercer une certaine surveillance en prenant un exemple de ses détestable mesures de sécurité aux aéroports. Même les experts en sécurité aérienne disent que c'est d'absurde nous traiter tous en suspects, ils n'ont simplement rien trouvé de mieux. En plus de cela il faudrait bien admettre que ces mesures de sécurité ont tout de même passé un certain test de légitimité. Un test s'articulant autour de quatre grands critères: Le premier critère et la nécessité, toute intrusion, toute atteinte à la vie privée ne peut être légitime que s'il est démontré qu'elle est nécessaire dans l'intérêt public. Deuxièmement elle est légitime que si elle est proportionnelle à cette nécessité, c'est-à-dire qu'elle ne va pas plus loin que ce qui est nécessaire dans l'intérêt public. Troisièmement il faut qu'il soit démontré qu'elle est efficace face a l'intérêt public poursuivi, et finalement il faut démontrer qu'il n'y a pas d'option moins envahissantes. Par exemple, toujours autour de la sécurité aérienne on a obtenu au Canada que les scanners corporels ne projettent plus l'image du passager. Il y a une image fixe tout ce qui est projeté c'est ce que le passager porte sur lui. On a donc trouvé une façon moi envahissante pour assurer la sécurité. On a donc trouvé tant bien que mal, un équilibre nécessité qui entraîne une certaine légitimité. Mais cette légitimité est mise à l'épreuve elle est mise à l'épreuve par de nouvelles techniques de surveillance.

La sécurité a l’information :

Les chercheurs en sécurité mettent en garde: «La sécurité des informations continue d'être ignorée par les meilleurs gestionnaires, cadres intermédiaires et employés .Le résultat de cette négligence est que les systèmes organisationnels sont beaucoup moins sûr qu'ils pourraient être autrement et que les failles de sécurité sont plus fréquentes que nécessaire ". Afin de renforcer le niveau de protection de l'information dans l'organisation, le responsable de cette information doit commencer par comprendre les menaces qui pèsent sur l'information, puis examiner les vulnérabilités inhérentes aux systèmes qui stockent, traitent et transmettent les informations Les informations éventuellement soumises à ces menaces. La première partie de cette stratégie est l'identification des menaces dominantes face à la sécurité de l'information organisationnelle et le classement de ces menaces afin de permettre aux organisations de diriger les priorités en conséquence.

L'essor des réseaux numériques donne lieu à des interprétations divergentes. Les unes soulignent l'emprise d'un individualisme croissant, désagrégeant les anciennes cohésions politiques. Les autres y oient le ecteur d'une sociabilité renouvelée. Les deux lectures se retrouvent cependant sur un point : dans le développement des systèmes de communication, la question de l'identité numérique représente désormais un enjeu central, sur les plans techniques, économiques et juridiques aussi bien que sociétaux. Cette convergence témoigne de l'importance prise par les procédures de traçabilité dans l'ensemble des transactions - commerciales, administratives ou relationnelles. Après avoir été pensée comme une cible, qui venait après une information déjà constituée, la personne est devenue une ressource, un agent de pertinence et un opérateur de liens entre les informations.Cette évolution coïncide avec l'émergence de nouveaux comportements, eux-mêmes portés par des dispositifs inédits, qui modifient les périmètres de l'identité. Décomposée en traces, exposée, indexée, recyclée, la présence numérique fait l'objet de traitements qui désagrègent la personne et mobilisent du même coup des aspirations à maîtriser son identité.

Après avoir été appréhendée sous le seul angle de la protection, la gestion des données personnelles se pose donc de plus en plus en termes de réappropriation. Par un mouvement de balancier qu'on a déjà pu observer dans d'autres médias, l'acculturation progressive aux dispositifs techniques déporte ainsi les questions ers des problématiques d'ordre politique.

La cybercriminalité :

La cybercriminalité est clairement la nouvelle menace du xxie siècle. Elle force les polices à repenser leurs moyens d'action, à se mettre au niveau techniquement et à développer des outils transnationaux, car l'échelle devient mondiale. Le cybercrime est d'autant plus difficile à appréhender qu'il prend des formes diverses et n'a, par définition, pas de frontières.

Il peut s'agir d'apologie du terrorisme, de réseaux de pédopornographie ou de proxénétisme, ou encore d'attaques contre des systèmes de données, comme celle qu'a connue récemment TV5 Monde. Internet donne aussi aux malfaiteurs un nouveau terrain de jeu pour mettre en place des escroqueries comme la fraude à l'e-paiement, le blanchiment d'argent ou le trafic de stupéfiants. Le cyberespace permet l'expression de menaces inédites par l'utilisation des nouvelles technologies, mais il étend aussi le périmètre des crimes « classiques ». Avec la démocratisation de l'accès à Internet et l'innovation constante autour des nouvelles technologies, la cybercriminalité devient un enjeu de société, à la fois pour les gouvernements, les entreprises et les citoyens. Et ce n'est que le début : toutes les études tablent sur une augmentation significative du nombre de crimes liés à Internet dans les années et décennies à venir. Il s'agit d'un vrai défi pour les États et les polices du monde entier.

Les Nations Unies :

L'article 12 de la DUDH consacre l'individu dans ses rapports avec les groupements qui l'entourent, et avec l'Etat dont il est citoyen. Ainsi, c'est bien l'individu que cet article protège en ses rapports avec les autres – tous les autres – qu'il s'agisse d'êtres humains ou d'institutions. L'article 12 sanctuarise la vie privée de l'Homme, c'est-à-dire la part de vie qu'il est et doit demeurer le seul à connaître, et ses prolongements naturels : la famille, le domicile, la correspondance. L'article 12 protège également l'Homme contre les atteintes à son honneur et à sa réputation. L'honneur, c'est l'idée que l'on se fait de soi-même. La réputation c'est l'idée que les autres se font de vous.La vie privée, la famille, le domicile, la correspondance sont ainsi éligibles à la protection de la loi tant ces domaines sont importants pour l'Homme.

Il s'agit d'un article fondamental qui place l'individu sous une cloche protectrice. La protection de la vie privée de l'individu sera, par la suite, également consacrée par la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales, par le Pacte international relatif aux droits civils et politiques, par la Convention relative aux droits de l'enfant. Mais cette protection s'effrite sous les coups de buttoir de l'usage, de plus en plus intensif, de technologies nouvelles, que ce soit par des opérateurs économiques qui tendent à profiler les consommateurs par l'observation fine et approfondie de leurs modes de vie, que par les Etats qui cherchent à constituer des bases d'informations à fin de police, et à les enrichir sans cesse, afin de mieux connaître les citoyens, au détriment de la sphère de vie privée.

Quelques pays :

CANADA :

La Loi sur l'accès à l'information accorde aux citoyens canadiens, aux résidents permanents et à toute personne ou société présente au Canada un droit d'accès aux documents des institutions fédérales assujetties à la Loi. La Loi complète d'autres politiques et procédures visant à rendre les renseignements du gouvernement accessibles au public, comme les initiatives sur le gouvernement ouvert et la divulgation proactive des frais de voyage et d'accueil, des contrats et autres renseignements fréquemment demandés. Cette page offre des liens vers la Loi, ainsi que vers des instruments de politique et des outils qui appuient son application.

TUNISIE :

Le Décret-loi N° 2011-41 relatif à l'accès aux documents administratifs des organismes publics (Loi sur l'accès à l'information) adopté par le gouvernement tunisien, est entré en vigueur le 26 mai 2011. Il impose d'importantes nouvelles obligations de transparence aux organismes publics en Tunisie, en vue de créer un mode de gouvernance plus ouvert et d'améliorer les relations entre les citoyens tunisiens et leur gouvernement. En particulier, il donne aux citoyens un droit d'accès à l'information détenue par les organismes publics, soumis seulement à un léger régime d'exceptions, et décrit les modalités d'exercice de ce droit.

Sous l'effet de cette loi, les organismes publics sont appelés à opérer des changements importants sur la façon dont ils gèrent et partagent les informations avec les citoyens. Le droit d'accès à l'information des citoyens a un effet immédiat, depuis l'entrée en vigueur de la loi En même temps, la loi donne deux ans aux organismes publics pour se conformer entièrement à ses dispositions, notamment pour adopter les structures et les mesures institutionnelles nécessaires.

BIBLIOGRAPHIE :

http://www.ohchr.org/FR/NewsEvents/Pages/DisplayNews.aspx?NewsID=20223&LangID=F

http://branchez-vous.com/2016/07/04/pour-lonu-nuire-lacces-internet-violation-des-droits-de-lhomme/

http://www.infopresse.com/article/2016/7/5/l-onu-declare-l-accessibilite-a-internet-comme-droit-fondamental

http://www.journaldugeek.com/2016/07/04/pour-lonu-couper-internet-est-une-violation-des-droits-de-lhomme/

http://www.thierryvallatavocat.com/2016/07/onu-les-restrictions-de-l-acces-a-l-information-sur-internet-sont-contraires-aux-droits-de-l-homme.html

http://www.un.org/fr/universal-declaration-human-rights/

http://www.persee.fr/doc/afdi_0066-3085_1980_num_26_1_2418

https://communication.revues.org/850

https://fr.wikipedia.org/wiki/S%C3%A9curit%C3%A9_internet

https://scholar.google.fr/scholar?hl=fr&q=What+security+is+provided+to+protect+access+to+online+information%3F&btnG=&lr=

https://pdfs.semanticscholar.org/80bf/49b08a0debff7dd2ad5dec8d98cc4ba714cc.pdf

http://www.journaldugeek.com/2016/07/04/pour-lonu-couper-internet-est-une-violation-des-droits-de-lhomme/

http://www.thierryvallatavocat.com/2016/07/onu-les-restrictions-de-l-acces-a-l-information-sur-internet-sont-contraires-aux-droits-de-l-homme.html

http://www.infopresse.com/article/2016/7/5/l-onu-declare-l-accessibilite-a-internet-comme-droit-fondamental

http://branchez-vous.com/2016/07/04/pour-lonu-nuire-lacces-internet-violation-des-droits-de-lhomme/

http://www.ohchr.org/FR/NewsEvents/Pages/DisplayNews.aspx?NewsID=20223&LangID=F