Les nouvelles menaces numériques : entre cyberterrorisme et secret d'état

publié le **22/08/2015**, vu **3379 fois**, Auteur : Vincent Julien

Les technologies du numérique, bien qu'elles constituent des vecteurs de progrès, constituent aussi des vecteurs de nouvelles menaces...

Nouvelles menaces pour la sécurité dans l'espace numérique, les atteintes informationnelles

Les atteintes informationnelles visent deux finalités, mais concernent un même objet : les informations sensibles. Elles consisteront donc soit à propager ou diffuser des informations sensibles visant à troubler l'ordre public au sein même du territoire, soit à recueillir ou soustraire des informations sensibles, dans le but cette fois d'impacter la sphère d'influence de l'Etat sur la scène internationale.

Atteintes visant à diffuser, propager des informations sensibles.

Les atteintes numériques visant à diffuser, propager des informations sensibles sont aujourd'hui plus que jamais d'actualité, comme en témoigne l'exemple du « cyber terrorisme » . Elles représentent non seulement une menace pour le principe de sécurité policière, à l'intérieur du territoire national, mais encore pour le principe de sécurité militaire, quand elles transcendent les frontières.

§.1/ Les atteintes visant à diffuser des informations sensibles : l'actualité du « cyber terrorisme ».

La banalisation de l'outil numérique, et l'augmentation exponentielle de son nombre d'utilisateurs a favorisé l'émergence d'infractions pénales dans l'environnement numérique : celles-ci concernent aujourd'hui principalement les faits d'association en relation avec une entreprise terroriste.

C'est qu'Internet est devenu non seulement un moyen de diffusion d'une idéologie terroriste, mais aussi un moyen de recruter de nouveaux combattants pour ces organisations : si hier encore, l'organisation terroriste « Al Qaeda» se servait d'Internet pour diffuser des scènes d'exécution, comme celle filmée en mai 2004 et reprise par tous les médias par la suite, il est aujourd'hui principalement question de l'Organisation de l'Etat Islamique (OEI ou « Daech ») :

L'organisation se démarque sur la scène médiatique en utilisant des outils de propagande très perfectionnés et dispose notamment d'une aile média, dénommée « Al-Hayat», qui a par exemple diffusé le film de propagande « Flames of War », traduit de l'arabe à l'anglais, dans lequel sont tournées des scènes de bataille en Syrie et en Irak, où sont promues les missions suicides, mises en avant les différentes origines géographiques des combattants, soulignant ainsi l'universalité du « djihad ».

Ce documentaire, dont on ne sait pas exactement s'il repose sur un ensemble de scènes réelles ou non, vise ainsi surtout à démontrer la capacité militaire de l'organisation ; cependant le but

subsidiaire de cette œuvre, par le biais notamment de la traduction de l'arabe vers l'anglais ou par la promotion des différentes ethnies s'alliant au « djihad », vise à recruter des combattants potentiels résidant pour une part en Europe

En dehors de toute activité terroriste, les atteintes de diffusion, propagation des informations recouvrent par ailleurs les individus ou groupes éditant des recettes d'explosifs ou d'engins incendiaires : il s'agit notamment du « Manuel du terroriste » en libre accès sur le web, qui « (…) décrit méthodiquement, de manière presque clinique, en dix-huit leçons comment se fondre dans le paysage d'un pays occidental, échapper aux poursuites, recruter, recueillir de l'information, fabriquer de faux papiers, détruire etc. (...) ». Aussi étonnant que cela puisse paraître, on peut trouver le synopsis de ce libre « fascinant » sur le site amazon.fr…

Ces menaces numériques ont nécessairement conduit le législateur à prendre de nouveaux moyens propres à prévenir ces atteintes informationnelles : désormais, on trouve dans le code pénal « l'infraction de diffusion du mode d'emploi et de fabrication d'armes et de moyens de destruction », dont la peine est aggravée lorsque cette infraction est commise par un réseau de télécommunications à destination d'un public non déterminé ou des infractions comme « les menaces de destruction, réelles ou supposées » :

La loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme est venue élargir le champ des infractions susceptibles d'être commises à des fins terroristes231, en renvoyant aux dispositions contenues aux articles 322-6-1232 et 322-13233 du code pénal : les peines encourues pour ces infractions sont parallèlement aggravées, selon la gradation prévue à l'article 421-3 du même code.

Surtout, la loi est venue créer le « délit d'apologie et de provocation au terrorisme », lequel sanctionne dorénavant le fait de provoquer directement à des actes de terrorisme ou de faire publiquement l'apologie de ces actes :

Lorsqu'il s'agit d'apologie, la condition de publicité consistant à présenter ou commenter les actes de terrorisme en portant sur eux un élément moral favorable doit cependant être remplie, mais lorsqu'il est question de provocation, cette dernière condition n'est plus nécessaire à la consommation de l'infraction. La provocation devra cependant être une incitation directe, non seulement dans l'esprit mais également dans ses termes : elle doit persuader de commettre des faits matériellement déterminés.

Quand l'infraction est constituée sur le terrain numérique précisément, son auteur encourt la peine prévue pour le délit de provocation à la commission des infractions énumérées dans l'article 24 de la loi du 29 juillet 1881, pour laquelle joue le jeu des circonstances aggravantes : La peine de cinq ans d'emprisonnement et de 75 000euros d'amende initialement prévue, passe ainsi à sept ans et à 100 000euros d'amende lorsque la provocation est directe, ou lorsque l'apologie publique de ces actes est commise par le biais d'un service de communication au public en ligne.

§.2/ L'implication des atteintes visant à diffuser des informations sensibles sur le principe de sécurité policière politique :

Bien qu'aujourd'hui « (…)90% des individus qui basculent dans le terrorisme le font par Internet » selon le ministre de l'Intérieur, la menace terroriste reste quant à elle un phénomène ancien. Cependant, l'émergence des technologies lui permet non seulement d'être protéiforme, mais surtout persistante dans l'avenir :

Comme le rappelle le professeur Yves Mayaud, l'originalité de la menace terroriste se situe dans sa finalité : il s'agit en effet « (…) d'une criminalité très particulière, à base de conception,

d’organisation et de réalisation d’infractions dont l’effet doit dépasser les victimes directes, telle une réaction en chaîne, pour atteindre la collectivité dans son ensemble ». Il s’agit donc moins d’atteindre l’intégrité des personnes physiques, que la cohésion de la collectivité ; d’ébranler une conception individuelle, plutôt qu’un modèle d’Etat.

La propagation d’informations sensibles présente donc un danger pour la sécurité de l’Etat avant tout, car elle permet de persuader, sinon d’endoctriner des individus résident ou non à l’intérieur du territoire dans une lutte ou s’affrontent deux conceptions idéologiques, ou politiques différentes :

Concernant l’Etat de droit par exemple, il s’agira de confronter la vision que s’en fait l’Occident, reposant sur la Constitution et un ensemble de règles de droit, avec la vision que s’en fait cette fois l’Organisation de l’Etat Islamique (OEI) ou le fondement principal sera la « Charia ». Or, dans un cas comme dans l’autre, il s’agira bien d’un Etat de droit sans que ce dernier ne repose sur les mêmes fondements, ou conceptions. A cet égard, la France constitue une cible prioritaire d’ « Al Qaeda » depuis que la loi du 15 mars 2004 est notamment venue proscrire le port de signes religieux à l’école, ou depuis de son engagement au sein de la force internationale d’assistance et de sécurité en Afghanistan, sa position sur la question des relations libano-syriennes : il s’agit donc de critiquer, sinon de sanctionner la position défendue par l’Etat, sans considération particulière de celle adoptée par les individus.

Ces menaces sont notamment alimentées par la diffusion des technologies numériques qui, si elles touchent de plus en plus de personnes sur le globe et visent avant tout à faciliter la circulation d’informations, peuvent constituer des terrains propices à la critique des positions défendues par certains Etats. La propagande, si elle atteint aussi bien les personnes résident à l’intérieur du territoire national, que celles résidant à l’extérieur des frontières nationales présente donc un danger pour la « normalité », sinon plus encore la « loyauté » des citoyens envers la Nation ; quand le but sera moins de conserver les « biens personnels et l’intégrité de personnes en particulier », que de « préserver l’ordre public » dans sa globalité appelant comme réponse particulière non pas la « réglementation », mais plutôt l’ « état d’exception ». A cet égard, l’exemple du plan « vigipirate : alerte attentat » en témoigne : s’il est théoriquement un dispositif exceptionnel, il reste aujourd’hui permanent et fait craindre l’exercice d’une sécurité policière politique prolongé.

Atteintes visant à recueillir, soustraire des informations sensibles

Les atteintes à l’ordre public peuvent aussi porter sur l’espionnage et le trafic clandestin : dans un contexte de mondialisation, elles sont autant d’actualité que le phénomène terroriste, tandis que leur impact est non seulement économique, mais aussi militaire. Si elles concernent autant la sécurité policière que militaire, elles ont de commun leur nature essentiellement politique.

§.1/ Le recueillement d’informations sensibles, un vecteur d’espionnage contemporain.

Les atteintes visant à recueillir, soustraire des informations sensibles se distinguent de celles commises à des fins de diffusion d’informations, de propagande car elles visent cette fois principalement à récolter fraudu-leusement des informations confidentielles, à des fins concurrentielles notamment.

L’éditeur de logiciels de sécurité « McAfee » relevait déjà en 1994 que les ordinateurs du Département de la Défense Américaine auraient été visités plus de 300 000fois par des inconnus, avant que la section du dépar-tement américain du commerce ne soit piratée en 2006. En Europe, c’est la Grande Bretagne qui fût l’objet d’atteintes similaires, tandis que selon les estimations de l’éditeur de logiciels, 300 agences gouvernemen-tales et entreprises auraient été la cible d’attaques visant à accéder de manière frauduleuse à des informations confidentielles.

Face à ces menaces, le législateur national est donc intervenu : la loi du 26 juillet 1986 incrimine désor-mais le fait de communiquer à des autorités publiques étrangères, des renseignements d’ordre économique, commercial ou industriel, financier ou technique de nature à porter atteinte à la souveraineté ou aux intérêts économiques essentiels de la France. Ces actes sont notamment punis de six mois d’emprisonnement et 18 000euros d’amende.

Parallèlement, les articles 411-6 et suivants du code pénal sont venus incriminer le fait de livrer à une puis-sance les informations de nature à porter atteinte aux intérêts fondamentaux de la Nation, tandis que ces opé-rations d’espionnage peuvent être qualifiées au travers de plusieurs infractions :

Il peut s’agir de la violation de correspondance et de communication électronique, de la commercialisation illicite d’appareils conçus pour intercepter les communications électroniques ou conversations, et même de la publicité pour ces appareils. L’infraction classique d’accès frauduleux à un système informatique trouve là encore à s’épanouir d’ailleurs : la peine sanctionnant le recel de l’infraction est notamment aggravée lorsqu’il s’agit d’un accès, ou maintien frauduleux dans un système de traitement mis en œuvre par l’Etat depuis la loi du 27 mars 2012.

Enfin, concernant plus particulièrement le monde de l’entreprise, les attaques informationnelles commises à l’encontre des entreprises nationales peuvent aussi être constatées par le biais de la violation du secret pro-fessionnel avec divulgation, par l’une des parties, des informations concernant une autre partie ou un tiers dont elle n’a pu avoir connaissance qu’à la suite des communications ou consultations auxquelles il a été procédé dans le cadre des attributions de l’Autorité de la concurrence.

§.2/ Le recueillement frauduleux d’informations sensibles, un impact économique significatif sur le principe de sécurité militaire :

L’actualité des menaces d’espionnage concerne aujourd’hui moins la pérennité des entreprises, que la survie de l’Etat dans un contexte mondialisé :

Les révélations sur les programmes d’espionnage menés par la NSA ont entraîné des « (…) changements fondamentaux et irréversibles dans beaucoup de pays et quantité de domaines » selon le journaliste du Guardian qui a rendu publiques les informations confidentielles recueillies par M. Edward Snowden. C’est que depuis 1950, les Etats-Unis disposent d’un réseau de surveillance globale qui, au gré des changements géopolitiques, a changé de fonction :

S’il était classiquement question « d’équilibre les menaces », dans le but de privilégier « le principe d’indiscutable » d’une position sur l’autre dans un contexte de guerre froide, afin de « dissuader » l’adversaire, de disposer d’hégémonie dans une « sphère d’influence » toujours plus étendue , d’assurer in fine la sécurité militaire, cette surveillance va progressivement changer de fonction :

Aujourd’hui, elle visera toujours à « combattre les menaces, actuelles ou futures (…) pesant sur

une économie mondiale construite autour des intérêt américains (…)» mais va se diversifier : elle [concernera désormais] les acteurs non étatiques, les pays moins développées bien déterminés à se faire une meilleure place dans l'économie mondiale ou, au contraire, les pays désireux de s'engager sur d'autres voies de

développement, et […] d'autre pays capitalistes développés ». Pour remplir ces nouveaux objectifs, l'industrie de la cyber guerre va se développer et donner lieu à des privatisations massives : ce qui était de longue date une fonction régalienne, dans un contexte de sécurité militaire, va se transformer en entreprise menée par l'Etat et les milieux d'affaires, visant moins à assurer une sécurité, qu'à réellement asservir les autres acteurs économiques étatiques ou non, alliés ou ennemis selon les circonstances et les changements de politique globale.

A ce titre, les acteurs de la sécurité sont aujourd'hui moins les gouvernements, que les multinationales disposant de technologies numériques de pointe : la sécurité constitue moins le préalable classique nécessaire au développement de l'économie, que la résultante d'accords économiques internationaux permettant aux gouvernements qui en usent, d'asseoir leur position stratégique sur un marché. Dès lors, les fruits de l'obtention d'un marché leur permettront non seulement de développer leur influence sur le terrain géopolitique, mais encore de nourrir leur influence militaire sur les autres acteurs de la scène internationale.

Risques liés aux atteintes informationnelles

Les deux types d'atteintes, selon qu'elles visent à diffuser ou à recueillir des informations sensibles suscitent des réponses adaptées des pouvoirs publics, qu'elles visent à assurer la sécurité politique à l'intérieur du territoire, ou militaire visant l'extérieur des frontières cette fois : cependant, elles ont de commun leur faculté de tempérer le principe de liberté de l'Internet, leur impact privilégiant la souveraineté d'Etat, sur celle de l'individu.

§.1/ Risques pour le principe de liberté d'Internet

« Internet donne à chacun d'entre nous la possibilité de s'exprimer, de créer, d'apprendre et de partager». A ce titre, si l'Internet apporte une énorme contribution au développement, l'exercice de la liberté d'expression doit être sauvegardé et promu non seulement aux médias traditionnels, mais encore à « (…) tous les types de plates-formes médiatiques émergentes contribuant au développement, à la démocratie et au dialogue » selon le rapport de l'UNESCO, « Freedom of Connection – Freedom of Expression ».

Cependant, on recense encore aujourd'hui plus de la moitié des pays privilégiant la censure des contenus sur Internet : dans certaines régions du globe marqués par l'instabilité politique, l'un des moyens les plus efficaces de contenir les insurrections populaires consiste en effet à couper les connexions Internet, ou le réseau de téléphones mobiles afin de cloisonner les frontières, et d'empêcher une circulation non seulement libre, mais encore neutre, pouvant constituer une critique des autorités publiques en place. Cette neutralisation du réseau Internet, garantie d'une liberté d'expression et de l'information, est d'ailleurs privilégiée de longue date par certains régimes politiques qualifiés d'autoritaires, comme celui de la Corée du Nord : le système repose sur une forme d'intranet ouvert permettant d'accéder à des sites d'information coréens, à la télévision éducative et à des formes rudimentaires de boite e-mail, quand ces outils sont utilisés majoritairement par les habitants de la capitale. Par ailleurs, la possession d'un ordinateur doit nécessiter une autorisation officielle, tandis que les Nord-Coréens pouvant accéder au réseau intranet, ne pourront téléphoner qu'à l'intérieur des frontières du pays, à la condition qu'ils reçoivent quotidiennement des messages de propagande à la gloire du régime.

Le principe de liberté d'Internet peut donc constituer une menace pour la sécurité policière

politique, car s'il permet d'ouvrir une fenêtre sur le monde, il implique nécessairement que le monde puisse voir au travers de cette fenêtre : à ce titre, il peut menacer la « préservation de l'ordre public », tel qu'entendu par le régime politique en place, qu'il consiste à asseoir une légitimité ou à préserver une idéologie et justifie le maintien de l'ordre. Or, si l'ordre peut être assuré par la force, il découle nécessairement d'une « domestication » des comportements déviants, lesquels trouvent particulièrement matière à s'épanouir sur le terrain de l'Internet, dès lors qu'ils pourront « contaminer » d'autres souches de la population, ce qui présente un risque pour l'intégrité d'un régime politique en place. La censure permettra donc d'asseoir une « loyauté » sur l'ensemble, permettant d'éradiquer la déviance menaçant le régime, et de promouvoir la « dénonciation » de ces comportements, afin de contenir les risques de contamination, donc de propagation de la critique à l'encontre du régime.

§.2/ Risques pour le principe de « sécurité humaine ».

« La sécurité humaine pourrait offrir une nouvelle approche de la sécurité et du développement : elle concerne la sécurité des individus et des communautés plus que celle des Etats » :

Comme le rappelle le Programme des Nations Unies pour le Développement (PNUD) de 1994, « le concept de sécurité (…) s'applique davantage aux Etats-Nations qu'aux personnes », le principe de sécurité humaine visera dès lors moins à insister sur la sécurité de l'Etat, que sur celle de l'individu, privilégiant la sécurité sur la violence politique. L'assise du principe contemporain de sécurité humaine serait plus que jamais nécessaire aujourd'hui, tandis que le développement des technologies de l'information et de la communication conduit l'ensemble de la population du globe à prendre connaissance des souffrances endurées par certains peuples, dans certaines régions ; par ailleurs, tandis qu'au lendemain de la Seconde Guerre Mondiale, les Etats en adhéré à une série de conventions, traités et déclarations, l'abolition des frontières traditionnelles conduirait plus encore les Etats à respecter leurs obligations.

Cependant, les atteintes informationnelles peuvent porter un coup d'arrêt à l'exercice de ce nouveau principe de sécurité humaine : c'est que les atteintes visant à diffuser, propager des informations sensibles, conduisent de plus en plus les Etats à recourir à une violence politique, plutôt qu'à assurer la sécurité. A cet égard, tandis que le terrorisme constitue une notion protéiforme et évolutive, il vise avant tout à promouvoir une idéologie politique aux antipodes de celle défendue par l'Etat : il s'agit par exemple de la politique indépendantiste promue par le Groupe Islamiste Armé (GIA) qui s'insurge contre le pouvoir algérien dans le but d'établir un gouvernement islamiste, ou d' « Al Qaeda » ou « Daech » qui poursuivent une même logique, opposée aux conceptions occidentales de l'Etat de droit.

On retrouve par ailleurs une illustration de cette violence politique avec le nouveau délit d'apologie du terrorisme, lequel peut moins constituer une apologie de la violence à proprement parler, que la défense d'une position idéologie opposée à celle promu par le gouvernement français. Il s'agit dès lors moins de promouvoir la sécurité juridique de l'individu que celle policière de l'Etat, impliquant la défense du gouvernement. La radicalisation de certains occidentaux traduit d'ailleurs cette logique de « souveraineté de l'Etat» : bien que ces derniers soient nés, et aient grandi à sur le territoire national, ils peuvent marquer leur rejet des positions prises par l'Etat sur la scène internationale en critiquant la prévalence des intérêts du gouvernements sur ceux des populations opprimées : il s'agira alors moins pour l'Etat de sauvegarder une certaine liberté d'expression, que de s'assurer de la loyauté de ces derniers au gouvernement, de conforter une sécurité juridique plutôt que de promouvoir une police politique.