

Contribution du gouvernement du Québec aux thèmes qui seront discutés à la réunion inaugurale du FGI à Athènes

INTRODUCTION

Tel qu'il est affirmé dans la « Politique québécoise de l'autoroute de l'information », le gouvernement du Québec croit fermement à l'importance des technologies de l'information et des communications (TIC) pour développer la société de l'information, moteur essentiel à la croissance socio-économique. Le gouvernement du Québec porte d'ailleurs une grande attention aux règles qui régissent l'évolution de l'Internet. C'est pour cette raison qu'il appuie, depuis le début, l'ensemble des démarches entourant le Sommet mondial sur la société de l'information (SMSI).

La création du Forum sur la gouvernance de l'Internet (FGI) est une solution intermédiaire pour favoriser et institutionnaliser le dialogue et la coopération entre toutes les parties prenantes et pour corriger les lacunes actuelles de coordination et de collaboration, tout en facilitant la participation. La tenue du FGI exige des parties prenantes de revoir leurs façons d'interagir et de collaborer. Ce dialogue permettra, sans aucun doute, d'élaborer des solutions acceptables pour tous en vue d'un développement optimal de l'Internet à l'avantage de toutes les populations, surtout celles les plus marginalisées et les plus vulnérables.

Les consultations portant sur l'organisation de la première réunion du FGI se sont très bien déroulées. L'équipe de M. Nitin Desai et le Groupe conseil ont effectué un travail remarquable et ils ont judicieusement sélectionné les thèmes de la réunion inaugurale du Forum ainsi que des règles efficaces pour le déroulement de la réunion.

Par ailleurs, les participants qui ne pourront pas se déplacer pour assister à la réunion pourront assurer leur pleine participation dans le processus grâce aux outils d'interaction qui seront mis à leur disposition. Le modèle organisationnel sélectionné est très explicite quant à l'égalité de participation des parties prenantes, et ce, qu'elles soient gouvernementales, issues d'une organisation de la société civile ou du secteur de l'entreprise privée.

Tel qu'il est indiqué dans l'Agenda de Tunis, le FGI n'a pas de pouvoir décisionnel. Aucun texte ne sera négocié, qu'il s'agisse de résolutions ou de décisions. Néanmoins, la nature non contraignante du Forum exige que les participants travaillent ensemble pour élaborer des consensus sur les thèmes sélectionnés par le Groupe conseil. Les rapports des sessions devraient nécessairement refléter ces consensus et non les désaccords entre les parties prenantes. Cette perspective semble la plus efficace et la plus constructive.

Voici les commentaires et la contribution du gouvernement du Québec aux thèmes de la diversité, de la sécurité, de l'ouverture et de l'accessibilité dans le contexte de la gouvernance de l'Internet. Puisque ce Forum concerne la gouvernance de l'Internet, les discussions sur ces thèmes devront nécessairement porter sur les règles, les procédures et les actions spécifiques ayant un impact sur la façon dont les enjeux relatifs à ces thèmes seront gouvernés.

Il est important de bien s'entendre sur la définition de chaque thème et de les circonscrire à la gouvernance de l'Internet. De plus, il est essentiel d'adresser les questions d'interdépendance des thèmes et des liens possibles qu'ils peuvent avoir entre eux. À ce sujet, il est utile de rappeler que les questions multidimensionnelles et pluridisciplinaires sont critiques pour la cohérence du processus et le développement de solutions innovatrices et efficaces. Les dimensions technologiques et leurs liens avec les aspects institutionnels de ces thèmes doivent également être pris en compte.

Une attention particulière sera portée au développement des capacités. Cet aspect doit être inclus autant dans les discussions portant sur les règles, les procédures et les actions spécifiques de chaque thème que dans l'ensemble des processus suivant les réunions du Forum. Une compréhension commune des enjeux par tous les participants est nécessaire pour atteindre les objectifs du Forum. De plus, les thèmes qui seront discutés exigent un effort considérable de développement des capacités afin de donner les moyens nécessaires aux parties prenantes pour garantir un environnement sécuritaire, accessible, ouvert et riche en diversité linguistique et culturelle.

OUVERTURE

L'ouverture est un principe fondamental à la gouvernance de l'Internet, intrinsèque à la philosophie de l'Internet de libre circulation de l'information et de technologies ouvertes assurant l'interopérabilité des systèmes. L'ouverture est critique pour s'assurer que l'Internet se développe comme un outil puissant et incontournable de développement de la société de l'information et pour l'autonomisation des individus.

Ce thème fait référence aux droits et libertés de la personne tels que le droit à la vie privée et à la liberté d'expression, en particulier à l'article 19 de la Déclaration universelle des droits de l'homme¹. L'ouverture englobe aussi l'adaptabilité culturelle et linguistique de l'Internet associée au thème de la diversité. Sans ouverture, le dialogue entre les civilisations sera limité et l'Internet fragmenté.

Ce thème est sans aucun doute celui qui porte le plus à controverse. Il peut impliquer des sensibilités culturelles et politiques opposées. Il est un marché commercial, une librairie, un outil éducatif, mais il est aussi le plus grand dépositaire de matériels pornographiques et de contenus haineux. Plusieurs gouvernements analysent d'ailleurs la possibilité de réglementer le contenu et l'accès à l'information disponibles dans Internet. D'autres gouvernements ont déjà mis en place des systèmes sophistiqués en ce qui a trait au contrôle du contenu et à la censure.

Les raisons évoquées pour adopter la voie de la censure sont nombreuses. Néanmoins, il en existe deux principales. D'une part, la censure fait allusion au contenu illicite ou préjudiciable à l'individu normalement identifié universellement comme étant haineux et illégal (ex : la pornographie infantile et les propos racistes). Le contrôle du contenu est devenu une préoccupation d'actualité pour la plupart des gouvernements dans la lutte contre la cybercriminalité. D'autre part, la censure est aussi envisagée pour limiter un contenu contraire aux mœurs locales ou s'opposant au discours politique officiel incluant les questions de sécurité nationale. Ce qui peut être considéré comme un contenu acceptable dans un pays peut ne pas l'être dans un autre pays. Néanmoins, la censure exercée par certains gouvernements fait l'objet de contestations toujours grandissantes. Les acteurs principaux, nommés les cyberdissidents, contestent les mesures draconiennes de censure en soutenant qu'elles constituent une atteinte à la liberté d'expression et au droit à la vie privée.

En plus de la censure, le phénomène de la surveillance illégitime dans l'Internet risque aussi de miner la confiance des utilisateurs en affectant leur droit à la vie privée, à la liberté d'expression et à l'accès à l'information. Un utilisateur change son comportement quand il s'exprime ou accède à l'information dans un environnement où il se sent surveillé.

La technologie est un élément central dans les stratégies et les mécanismes utilisés pour effectuer la censure. Malgré le certain degré d'anonymat qu'offre l'Internet, les avancées technologiques permettent de localiser facilement les utilisateurs et le contenu dans l'Internet sur une base géographique, de filtrer et d'intercepter l'information, de bloquer l'accès à l'information et d'emmagasiner toute information pertinente concernant un utilisateur.

L'Internet doit favoriser la diversité et la liberté d'expression et non pas l'avènement d'un comportement standardisé. Il est primordial de continuer à définir la portée des principes concernant la liberté d'expression, l'accès à l'information et la vie privée dans l'Internet. Ce processus devrait normalement s'insérer à l'intérieur de mécanismes internationaux de droit public et de droit privé pour assurer un minimum d'application et définir les obligations des parties prenantes, en particulier les registraires de noms de domaine et les fournisseurs d'accès à l'Internet.

DIVERSITÉ

Tout d'abord, il est heureux que le Forum soit saisi de cette problématique considérée comme fondamentale. Les discussions sur ce thème doivent nécessairement amener tous les participants vers des solutions dans le sens de l'article 53 de l'Agenda de Tunis et de la

¹ « 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. »

Convention sur la protection et la promotion de la diversité des expressions culturelles de l'UNESCO.

Le thème de la diversité réfère principalement aux enjeux de l'adaptabilité linguistique et culturelle de l'Internet. La technologie propre à l'Internet et les aspects institutionnels entourant sa gestion ne doivent pas favoriser ou privilégier une langue ou une culture, mais permettre l'expression de toute forme de langue et de culture. Cette diversité doit s'exprimer tant au niveau du contenu et de sa description (métadonnées) qu'au niveau des outils d'accès et de fonctionnalités du réseau, tels que les noms de domaine, les logiciels, les protocoles, etc.

Un ordinateur connecté à l'Internet demeure pratiquement inutile pour une majorité de personnes s'il n'est pas adapté à leurs contextes culturel et linguistique. Sans un Internet réellement multilingue, le réseau demeurera inaccessible à la très grande majorité de la population mondiale. Ces personnes seront privées de son utilisation aux fins éducatives, commerciales, culturelles, etc. ou se verront grandement limitées en ces domaines.

Le gouvernement du Québec salue tous les efforts qui ont été faits dans cette thématique. Néanmoins, ceux-ci sont insuffisants, comme le note le Groupe de travail sur la gouvernance de l'Internet (GTGI)². Toutes les parties prenantes sont donc invitées à accélérer les travaux pour parvenir à des solutions acceptables et viables pour tous.

Les solutions doivent correspondre aux besoins des utilisateurs et non aux seules volontés – ou visions – des ingénieurs et des techniciens. Les normes et les standards sur l'adaptabilité culturelle et linguistique de l'Internet doivent être élaborés selon le principe de neutralité linguistique. Ainsi, à la base, aucune langue « pivot » ne devrait être incontournable. Ceci implique que l'anglais doit être traité comme les autres langues. De plus, les solutions proposées doivent nécessairement être transparentes et simples d'utilisation pour les différents usagers. Enfin, toutes les langues du monde doivent pouvoir être utilisées. Ce principe implique le respect de l'environnement linguistique et culturel distinctif de chaque utilisateur.

Pour qu'une langue soit utilisée ou présente sur le réseau mondial, une masse critique d'utilisateurs de cette langue doit exister. La fracture numérique est donc réellement accentuée par une prépondérance de l'anglais par rapport aux autres langues, en particulier celles parlées par un nombre de locuteurs limités. De ce fait, il faut favoriser l'accessibilité des utilisateurs de langue et de culture minoritaires à l'univers d'Internet. En conséquence, les produits et les fonctionnalités technologiques doivent préalablement être adaptables à ces langues et cultures pour augmenter la vitesse de pénétration de la technologie.

L'internationalisation ou l'adaptation linguistique du système des noms de domaine est une étape importante et prioritaire pour permettre aux utilisateurs de différentes langues et cultures de rapidement accéder aux sites Internet voulus ou identifier un contenu culturel ou linguistique spécifique.

Une des difficultés à l'adaptabilité linguistique des noms de domaine réside dans le rôle que doivent jouer les normes ou les standards technologiques utilisés dans le système. Une importante avancée serait que toutes les pratiques entourant la formulation des standards techniques pouvant affecter l'adaptabilité linguistique du système des noms de domaine (incluant les adresses courriels) fassent l'objet d'enquêtes élargies à l'ISO³. Ce faisant, ce processus permettrait que les solutions avancées deviennent des normes internationales consensuelles vraiment équilibrées politiquement, et ce, à l'échelle mondiale. Ces normes internationales deviendraient alors incontournables pour toutes les parties prenantes.

En effet, le processus de normalisation de l'ISO (en collaboration avec la Commission électrotechnique internationale et l'Union internationale des télécommunications, qui forment avec elle le système mondial de normalisation reconnu par l'Organisation mondiale du commerce) présente d'immenses avantages pour l'adaptabilité linguistique des fonctionnalités du réseau. L'ISO apparaît être la seule organisation permettant d'atteindre un consensus dans la recherche d'une méthode normalisée commune contribuant à réduire ou à supprimer les obstacles linguistiques. Les avantages de la normalisation sont nombreux et font l'unanimité dans certains secteurs d'activité. Des normes internationales ISO aideraient les entreprises et les gouvernements en assurant l'interopérabilité entre les

² Rapport du GTGI, juin 2005, p. 7

³ Organisation internationale de normalisation

systèmes, en diminuant la complexité des technologies, en rationalisant la conformité aux règlements et en aidant à échanger des informations de manière sécuritaire et inclusive. L'ISO présente donc tous les atouts pour la gestion de normes de diversité linguistique dans un cadre favorisant la communication entre les différentes parties concernées.

Il est essentiel d'établir une politique publique mondiale sur l'enregistrement et la gestion des noms de domaine multilingues pour minimiser les risques de cybersquatage et de typosquatage, ou tout autre risque pouvant affecter la sécurité et la stabilité du réseau, la protection du consommateur et le commerce électronique. Cette politique doit être établie sur une base démocratique et consensuelle, toutes les parties prenantes étant amenées à participer dans l'esprit de l'Agenda de Tunis. De plus, elle doit inclure des règles de base ou des principes directeurs pour les registraires en vue de l'approbation de nouveaux noms de domaine multilingues et de leur gestion. Ces principes doivent nécessairement respecter les pratiques acceptées mondialement en propriété intellectuelle.

Le gouvernement du Québec reconnaît que la gestion des noms de domaine associée aux codes des États (ccTLD) relève de la souveraineté des États, tel que cela est stipulé dans l'Agenda de Tunis. Cependant, pour assurer un minimum de cohérence dans l'implantation d'une politique publique mondiale sur l'enregistrement et la gestion des noms de domaine multilingues, les registraires des noms de domaine associés aux codes des États doivent nécessairement souscrire à cette politique pour assurer un minimum de cohérence et éviter une fragmentation du réseau. Cette politique mondiale sur l'enregistrement et la gestion des noms de domaine multilingues ne doit pas concerner les aspects juridiques propres aux législations de chaque pays, mais uniquement s'attarder aux aspects linguistiques des noms de domaine.

SÉCURITÉ

Il est fondamental d'établir et de garantir la confiance et la sécurité dans l'utilisation de l'Internet de manière à permettre le développement de l'Internet, où les utilisateurs peuvent transiger et communiquer sans crainte que leurs droits soient enfreints ou que la pérennité et l'intégrité de leurs données soient menacées. La confiance doit reposer sur des technologies et des règles qui respectent, notamment, le principe de la transparence.

À l'instar des autres gouvernements, le gouvernement du Québec a identifié cette thématique dès le tout début de ses travaux pour mettre en place le « gouvernement en ligne ». En effet, au Québec, il a été constaté que les craintes relatives à la sécurité constituent une des principales raisons pour lesquelles un citoyen ou une entreprise n'utilise pas un service en ligne dans l'Internet.

De nombreux instruments pour contrer ce problème et établir la confiance des citoyens ont été mis en place. Ces instruments sont d'ordres légal, normatif, organisationnel et technologique. Ils comprennent, entre autres, la mise en œuvre des meilleures pratiques basées sur les normes et les standards internationaux ainsi que sur des mécanismes de coordination des incidents et des vulnérabilités qui eux sont basés sur le modèle CERT⁴. Récemment, le gouvernement du Québec a appuyé la création de l'Institut de la sécurité de l'information du Québec (ISIQ), qui est une plateforme publique-privée d'échange d'information et de connaissances en matière de sécurité de l'information, ainsi qu'une base d'intervention au sein de la société civile et des petites et moyennes entreprises. Cet institut doit également développer des partenariats publics-privés pour la cybersécurité en général.

Les démarches entreprises au Québec révèlent à quel point aucune organisation ne peut, à elle seule, faire face aux problématiques de sécurité de l'information découlant de l'utilisation croissante des technologies de l'information, plus particulièrement de l'Internet. Il est donc important que toutes les parties prenantes concernées aux niveaux national et international partagent leurs connaissances et leurs meilleures pratiques et coopèrent entre elles pour assurer la sécurité de l'information d'une manière cohérente et efficace.

Les problématiques de sécurité sont complexes et dépendent de l'évolution rapide des TIC. Les techniques utilisées par les pirates ont grandement évolué et les menaces ne sont plus de simples gestes de curiosité technologique.

⁴ Computer Emergency Response Team

Le thème de la sécurité, tant sur le plan technologique qu'institutionnel, comprend plusieurs sous-thèmes ou enjeux. Les enjeux directement liés à la sécurité sont la cybercriminalité et la cybersécurité, laquelle comprend les phénomènes de pourriels, de maliciels, de logiciels espions et d'hameçonnage. De plus, il y a les enjeux du respect de la vie privée, en particulier la protection des renseignements personnels, et ceux de la protection de la propriété intellectuelle qui exigent la mise en place de nombreuses mesures de sécurité.

Tel qu'il est indiqué dans la Déclaration de principe du SMSI, les mesures proposées pour assurer la sécurité ne doivent pas aller à l'encontre des valeurs démocratiques et, en particulier, des droits de la personne. Les éléments de la thématique de l'ouverture, précédemment discutés, doivent être reflétés dans les mesures de sécurité.

Une importance particulière doit être accordée au respect de la vie privée et de la protection des renseignements personnels. À cet effet, il est important de mentionner que la sécurité de l'information est essentielle pour assurer la protection des renseignements personnels, mais qu'elle ne peut à elle seule garantir le respect des dispositions légales de protection des renseignements personnels. Cette distinction est fondamentale et doit nécessairement être établie lors des discussions.

L'atteinte d'un niveau de sécurité adéquat nécessite une étroite collaboration avec toutes les parties prenantes à l'échelle nationale et internationale et une adhésion à une vision et à une compréhension communes de la sécurité.

Une des étapes importantes pour faire face aux enjeux de sécurité en matière de gouvernance de l'Internet est l'adoption d'instruments légaux et équivalents entre les pays et leur mise en application par toutes les parties prenantes. Les gouvernements, l'industrie, les entreprises et les consommateurs doivent travailler ensemble et adopter une variété de mesures axées sur des lois claires, prévoyant des sanctions sévères et des mesures puissantes de mise en application de la loi, en plus de pratiques administratives efficaces. Ces instruments légaux et réglementaires doivent minimalement être harmonisés les uns avec les autres pour garantir leur application dans un espace numérique sans frontières.

De nombreux efforts internationaux vont dans cette direction. De nombreux guides et outils ont été développés, comme ceux de l'Organisation de coopération et de développement économiques (OCDE) sur le développement des stratégies de cybersécurité et la protection des données personnelles. Ces guides énumèrent des principes qui correspondent à la base à une vision commune. Néanmoins, leurs applications demeurent limitées. Les pays en voie de développement doivent être en mesure d'assurer la mise en œuvre d'instruments législatifs et réglementaires. À cet effet, le développement des capacités et l'échange d'information sont des éléments-clés.

Ces mesures impliquent aussi l'élaboration et l'application communes de normes et de bonnes pratiques reconnues internationalement. Enfin, toutes les parties prenantes doivent travailler ensemble pour effectuer des campagnes de sensibilisation des consommateurs et procéder à l'éducation du public. Ces programmes de sensibilisation doivent permettre aux utilisateurs de bien assimiler et gérer les risques liés à la sécurité et au respect de la vie privée dans le cadre de leur utilisation de l'Internet. Enfin, des mécanismes de coordination au niveau mondial doivent être élaborés pour permettre et assurer l'échange d'information et de bonnes pratiques, surtout pour répondre efficacement aux incidents cybernétiques.

ACCESSIBILITÉ

Le thème de l'accessibilité est fortement associé au thème général du développement. L'accessibilité fait référence à l'accès universel de toutes les populations à l'Internet tant au niveau de l'accès physique du réseau par un ordinateur et une connexion « Internet » qu'à celui de l'accès au contenu et aux fonctionnalités (logiciels et services). L'accès au contenu passe nécessairement par le respect des principes de liberté d'expression et d'accès à l'information. Les besoins pour l'accès universel sont gigantesques dans la majorité des pays de la planète. Les changements institutionnels majeurs, sur les plans international et national, sont nécessaires pour favoriser un environnement propice à la connectivité. Les stratégies nationales pour l'éducation doivent être mises à contribution pour former de véritables utilisateurs.

L'accès aux fonctionnalités passe avant tout par l'éducation, le développement des capacités et la formation des utilisateurs aux technologies de l'Internet. Toutefois, cet accès dépend aussi de l'adaptabilité des outils technologiques aux conditions de l'utilisateur. Cette adaptabilité se fait au niveau de la langue et de la culture, mais doit aussi prendre en compte toutes les incapacités vécues par les personnes handicapées, quelles soient d'ordres visuel, physique, auditif, verbal, cognitif, neurologique, etc., qui ont pour effet de limiter leur utilisation de l'Internet.

Les parties prenantes doivent s'entendre sur des mesures favorisant l'adaptabilité linguistique et culturelle des produits informatiques et l'accessibilité des personnes handicapées. Tout comme pour l'adaptabilité linguistique et culturelle qui passe par l'élaboration et la mise en place de normes consensuelles neutres sur le plan linguistique. L'accès des personnes handicapées à l'Internet et à ses fonctionnalités devrait passer aussi par ce processus. Une initiative importante en ce sens est celle du Web Accessibilité, initiative du W3C⁵ qui a élaboré des standards et des mesures permettant aux personnes ayant des incapacités d'utiliser l'Internet pour percevoir, comprendre et interagir avec d'autres utilisateurs.

Enfin, une avenue intéressante pour résoudre en partie les enjeux entourant l'accessibilité et la fracture numérique est celle du logiciel libre qui permet l'accès ouvert et moins coûteux à de nouvelles technologies. De plus, le logiciel libre est un moyen intéressant pour l'adaptabilité linguistique et culturelle rapide des logiciels.

⁵ World Wide Web Consortium