CI – 022M
C.G. – Technologies et vie privée à l'heure des choix de société
VERSION RÉVISÉE

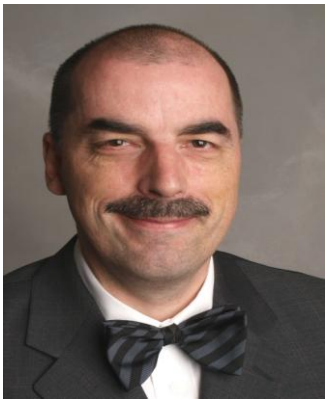
Technologies et vie privée à l'heure des choix de société

Mémoire présenté à l'assemblée nationale du Québec

2013-03-30

Table des matières

1. PRÉSENTATION DES COAUTEURS



M. Martin M. Samson
Directeur exécutif associé
Sécurité de l'information
Technologies et Sécurité
Nurun Inc,
filiale du groupe Québecor média Inc.

Professionnel en sécurité de l'information, CGEIT, CISM, CRISC et ISO 27001 lead auditor, M. Martin M. Samson possède une vaste expérience en gestion de projets informatiques et en gestion de ressources, tant humaines que matérielles.

Monsieur Samson est très familier avec le contexte gouvernemental québécois ainsi que le domaine bancaire. Monsieur Samson est également titulaire d'un diplôme universitaire de 2e cycle à la faculté d'administration de l'Université de Sherbrooke en «Gouvernance, audit et sécurité des technologies de l'information».

M. Samson est actuellement directeur exécutif associé du secteur de la sécurité et des technologies de Nurun Inc.

En cette qualité, il coordonne la vigie ainsi que le développement l'expertise en technologie et sécurité de l'information aussi bien au sein de la filiale de Québec qu'à l'international, tout en continuant à mener des projets de grande envergure dans différents ministères.

M. Elhadji M. Niang, CISA
Consultant en sécurité, Nurun Inc.,
filiale du groupe Québecor média Inc.

M. Niang cumule plus d'une dizaine d'années d'expérience professionnelle dans différents organismes publics, privés et dans le domaine de la recherche universitaire.

Il est titulaire d'un Master 2 spécialisé en Sécurité Informatique et juridique dans les Sociétés Numérisées et d'une maitrise en droit des affaires. Il détient également les certifications CISA et ITIL V3.

Au cours de son cursus professionnel, M. Niang a développé une solide expertise dans les domaines couvrant la gouvernance de la sécurité de l'information (cadre de gestion, cadre méthodologique, processus, politiques, directives procédures…), l'architecture de sécurité, la protection des renseignements personnels, l'implantation de système de gestion de la sécurité de l'information, l'audit, la gestion de la performance (conception et suivi de tableau de bord), ainsi que la cartographie de processus d'affaires.

1.1 AVIS AU LECTEUR

Veuillez prendre avis que les opinions exprimées dans le présent document le sont à titre personnel et ne traduisent pas la vision ou l'opinion de Nurun Inc.

À cet effet, Nurun Inc. ne saurait pour quelques raisons ou motifs que ce soient être tenue pour responsable des opinions exprimées par les auteurs du présent document.

Les opinions exprimées par les auteurs sont basées sur leurs expertises professionnelles respectives et traduisent leur contribution citoyenne à un débat sociétal.

Suivant cette finalité, les auteurs consentent à la diffusion et à la reproduction du document sous quelques formes, formats et supports que ce soient.

Toutes questions, remarques ou commentaires peuvent être adressés aux auteurs aux adresses courriels ci-dessous :

Martin M. Samson : martin.samson@nurun.com

Elhadji M. Niang : elhadji.niang@nurun.com

2. RÉSUMÉ

L'avènement des technologies de l'information a fondamentalement bouleversé notre existence quotidienne. L'apparition de l'informatique[1] a entre autres généré la mise en œuvre de systèmes d'information de plus en plus perfectionnés ainsi que des réseaux interconnectant des millions de machines, sans aucune limitation géographique ou territoriale.

Les pouvoirs publics, sans doute conscients des potentialités offertes par les technologies de l'information, en ont fait un tremplin privilégié pour prester leur mission de service public.

Il est souvent usité d'entendre que l'administration électronique opérera une transformation des organismes publics, et permettra de renforcer la démocratie à travers une plus grande participation citoyenne (accès à l'information), et la promotion de la relation administration - administrés (prestation électronique de services gouvernementaux).

Nonobstant tous ces avantages réels ou supposés, il convient de relever que l'utilisation des technologies de l'information n'en comporte pas moins des enjeux en termes d'atteintes potentielles sur la vie privée des citoyens.

C'est d'ailleurs suivant ces considérations qu'il est important, du moins de l'avis des coauteurs, que les pouvoirs publics envisagent d'intégrer les bonnes pratiques de l'industrie à l'intérieur d'un référentiel gouvernemental de gestion de la sécurité de l'information.

[1] Discipline qui s'intéresse à tous les aspects, tant théoriques que pratiques, reliés au traitement automatique de l'information, à la conception, à la programmation, au fonctionnement et à l'utilisation des ordinateurs.

L'informatique est en fait la science du traitement automatique de l'information considérée comme le support des connaissances et des communications humaines

Définition tirée du grand dictionnaire terminologique de l'OQLF
http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=2071561

2. EXPOSÉ GÉNÉRAL

2.1 LES ENJEUX DE L'USAGE DES TECHNOLOGIES FACE À LA VIE PRIVÉE

De manière non exhaustive, ni limitative, les enjeux de l'usage des technologies de l'information sont succinctement décrits ci-après.

- **Un accroissement exponentiel des possibilités de collecte des renseignements personnels;**

Le développement des technologies de l'information permet de plus en plus, une collecte **avec ou sans consentement** d'une grande quantité de renseignements personnels.

Dans la majorité des cas, ces technologies **n'ont pas pour objet** de porter atteinte à la vie privée, mais **les effets** pourraient permettre de le faire.

L'avènement d'une multitude de technologies dont l'**objet** n'est pas de nous tracer mais dont les **effets** pourraient permettre de nous retracer…

Réseaux sociaux

Téléphone intelligent

Gouvernement en ligne

Appareils de géo localisation

- **La problématique de la juridiction applicable dans un contexte d'infonuagique (Cloud computing);**

L'infonuagique ou « cloud computing » consiste à mettre à la disposition du client, suivant ses besoins et sur une base contractuelle, les capacités de

traitement, espaces de stockage, ressources réseau, plateformes d'exécution ou solutions logicielles d'un fournisseur.

L'infonuagique soulève comme principale problématique l'effectivité de la mise en œuvre de la législation applicable ainsi que la sanction en cas d'inobservation.

Prenons le cas d'une compagnie privée Québécoise qui fait du commerce en ligne en prenant appui sur une plateforme technologique dont les serveurs et les bases de données sont physiquement localisés en Inde.

S'il ne fait aucun doute que cette compagnie commerçante reste assujettie à la Loi québécoise sur la protection des renseignements personnels dans le secteur privé, la question reste entière quant à la persistance des renseignements personnels sur les serveurs et bases de données du fournisseur à l'issue du contrat. L'application des dispositions pertinentes de la loi au fournisseur d'infonuagique situé en Inde et qui contrôle physiquement ces serveurs peut en effet s'avérer problématique.

- **La question du contrôle des couplages technologiques;**

Que ce soit à des fins de sécurité dans les lieux publics, ou de la recherche d'une plus grande efficacité et efficience dans l'exploitation des aéroports[2] on assiste de plus en plus à des couplages de diverses technologies.

Il s'agit dans la majorité des cas d'associer la vidéosurveillance avec la reconnaissance faciale le tout complété par une puce RFID afin d'identifier et un de repérer un individu dans un lieu public.

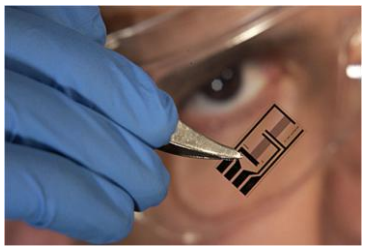
S'il est évident que le couplage technologique offre des gains réels en termes de sécurité dans l'espace public, il n'en demeure pas moins que celui-ci doit être strictement encadré par le législateur afin qu'il puisse être réalisé à l'intérieur des impératifs de protection de la vie privée des citoyens.

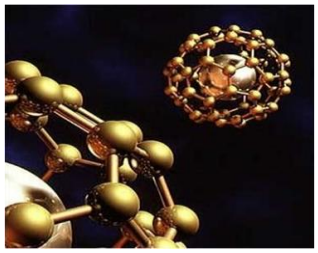
[2] Technologie de reconnaissance faciale et puce de géo localisation par RFID intégrée dans les billets d'avion, voir http://www.transport-research.info/web/projects/project_details.cfm?ID=35661

- **L'avènement de la nanotechnologie;**

L'Office québécois de la langue française défini la nanotechnologie comme un « *Domaine multidisciplinaire qui concerne la conception et la fabrication, à l'échelle des atomes et des molécules, de structures moléculaires qui comportent au moins une dimension mesurant entre 1 et 100 nanomètres, qui possèdent des propriétés physicochimiques particulières exploitables et qui peuvent faire l'objet de manipulations et d'opérations de contrôle* ».

Plus particulièrement, il s'agit d'une diversité de technologies pouvant être utilisées sous plusieurs formes et finalités et qui sont la plupart du temps indétectables des organes sensoriels de l'être humain (ouïe, vue, odorat).





Face aux multiples possibilités d'usage des nanotechnologies et de l'existence de projets de recherches avec un financement public au Québec[3], les auteurs du présent rapport sont d'avis, que le législateur doit à l'instar de certains pays tel que la France se saisir du débat[4].

Le législateur devrait en effet veiller à instituer un véritable **cadre de gouvernance des nanotechnologies** fondé sur l'équilibre entre les plus values économiques et les impératifs de protection des droits et libertés individuelles, ainsi que des impacts environnementaux, et sur la santé et la sécurité des citoyens également.

[3] http://www.nanoquebec.ca/fr/index.php

[4] http://www.debatpublic-nano.org/debat/debat_public.html

2.2 LA NÉCESSITÉ DE PRENDRE APPUI SUR LES BONNES PRATIQUES EN TECHNOLOGIES ET PROCESSUS DE GESTION DE LA SÉCURITÉ DE L'INFORMATION

Les rédacteurs du présent rapport endossent la pertinence des recommandations contenues dans le rapport quinquennal de la Commission d'accès à l'information (CAI).

La substance de notre opinion est à l'effet que le corpus légal en matière de la protection de la vie privée des citoyens dans le secteur public devrait s'accompagner d'une meilleure prise en considération des bonnes pratiques de l'industrie en matière de sécurité de l'information.

Le législateur devrait en effet favoriser la mise en œuvre d'un Référentiel de bonnes pratiques en sécurité de l'information[5]. L'objectif recherché serait d'harmoniser les façons de faire au niveau des organismes publics en la matière.

Cela permettrait à la Commission sur l'accès à l'information dans sa fonction juridictionnelle, de disposer d'un Référentiel lui permettant de mesurer lorsque requis (en cas de plainte par exemple), le niveau de conformité des mesures techniques mises en œuvre par l'organisme objet de la plainte[6]. Plus précisément, il s'agira pour la CAI de vérifier que l'organisme a fait preuve de diligence et de prudence dans la mise en œuvre des moyens raisonnables compte tenu des meilleures pratiques préconisées par le Référentiel.

Ce Référentiel pourrait également être utilisé par des organisations tel le Secrétariat aux institutions démocratiques et à la participation citoyenne du

---

[5] Cette façon de faire est adoptée par le gouvernement français à travers le référentiel général de sécurité. Voir http://references.modernisation.gouv.fr/rgs-securite

[6] Nous Faisons ici référence à un contentieux fondé sur les articles 24 et 25 de la *loi concernant le cadre juridique des technologies de l'information* reproduits en annexe.
Le sens de nos propos est d'initier à l'instar de pays tel que la France, la mise en œuvre d'un référentiel de bonnes pratiques, piloté par le Comité pour l'harmonisation de la loi concernant le cadre juridique des technologies de l'information ainsi que le bureau de normalisation du Québec et tout autre organisme public compétent.
Il s'agirait de définir des **critères objectifs** à travers des **normes** et **standards** qui pourraient être éventuellement utilisés pour mesurer ou promouvoir selon le cas, les moyens technologiques mis en œuvre afin d'atteindre les objectifs visés par ces articles.

Ministère du conseil exécutif, afin de promouvoir la **bonne gouvernance** dans la mise en œuvre des mesures technologiques et processuelles en matière de protection des renseignements personnels. Il permettrait en effet d'instituer une véritable **gouvernance des données** dans une perspective de protection de la vie privée alignées sur les meilleures pratiques de l'industrie[7].

Un tel Référentiel permettrait en définitive de bénéficier de la souplesse de mises à jour à la lumière des avancées technologiques et processus de gestion, comparativement à une règle de droit dont la modification ou la mise à jour peut prendre du temps.

Finalement, les rédacteurs du présent rapport sont d'avis que la protection de la vie privée face aux avancées technologiques dans le secteur public devrait se faire en tenant en compte les objectifs de contrôle ci-dessous :

- **Concevoir des <u>processus</u> qui permettent de s'assurer en amont de l'équilibre entre les exigences de respect de la vie privée et les finalités du système.**

Cela requiert pour chaque organisme public qui conçoit ou met en œuvre un système d'information comportant une collecte, traitement et/ou stockage de renseignements personnels, de réaliser et de documenter de manière systématique une **analyse des risques** afin de s'assurer du respect des principes de finalité, de proportionnalité, de reconnaissance d'un droit d'accès, de modification et de suppression (droit à l'oubli).

- **Réaliser suivant une périodicité définie des analyses de vulnérabilités des systèmes contenant des renseignements personnels afin de s'assurer de leur niveau de sécurité**

Il s'agit de promouvoir au niveau de l'ensemble des ministères et organismes, une évaluation périodique du niveau de sécurité de l'infrastructure technologique comportant des renseignements personnels.

[7] Voir à cet effet la gouvernance des données préconisée par Microsoft http://www.microsoft.com/privacy/datagovernance.aspx

Les analyses de vulnérabilités devront nécessairement être suivies de la **documentation des résultats obtenus** et la mise en œuvre des mesures de mitigation appropriées pour corriger les vulnérabilités découvertes.

- **Gérer les accès utilisateurs en fonction de la sensibilité des renseignements personnels contenus dans le système**

Il s'agit de mettre en œuvre un dispositif comportant les fonctionnalités de sécurité nécessaires pour la création de comptes utilisateurs et la gestion des habilitations. Le but recherché est de s'assurer que les utilisateurs n'ont accès qu'aux renseignements personnels d'un citoyen nécessaire à leur fonction. Cet objectif est d'autant plus important dans un contexte de transfert de renseignements personnels entre organismes.

- **Favoriser la mise en œuvre de solution de lutte contre la fuite d'information pour les systèmes sensibles**

Pour les systèmes gouvernementaux sensibles contenant par exemple des dossiers médicaux, des dossiers fiscaux ou des informations bancaires des citoyens…, il convient de mettre en œuvre des solutions technologiques permettant d'avoir un certain niveau de granularité quand à la mise en œuvre de mesures de sécurité des dossiers.

Ces solutions devraient permettre par exemple de mettre en œuvre des mécanismes de **protection anti copie** sur un support amovible, d'**interdire l'impression** ou encore leur **transfert par courriel**.

- **Promouvoir la formalisation de processus de gestion des incidents mettant en jeu des renseignements personnels**

Les rédacteurs du présent rapport sont d'avis que la recommandation de la Commission sur l'accès à l'information à l'effet de déclarer les failles de sécurité devrait corrélativement s'accompagner d'une obligation de mise en œuvre d'un processus de gestion des incidents/failles de sécurité impliquant les renseignements personnels.

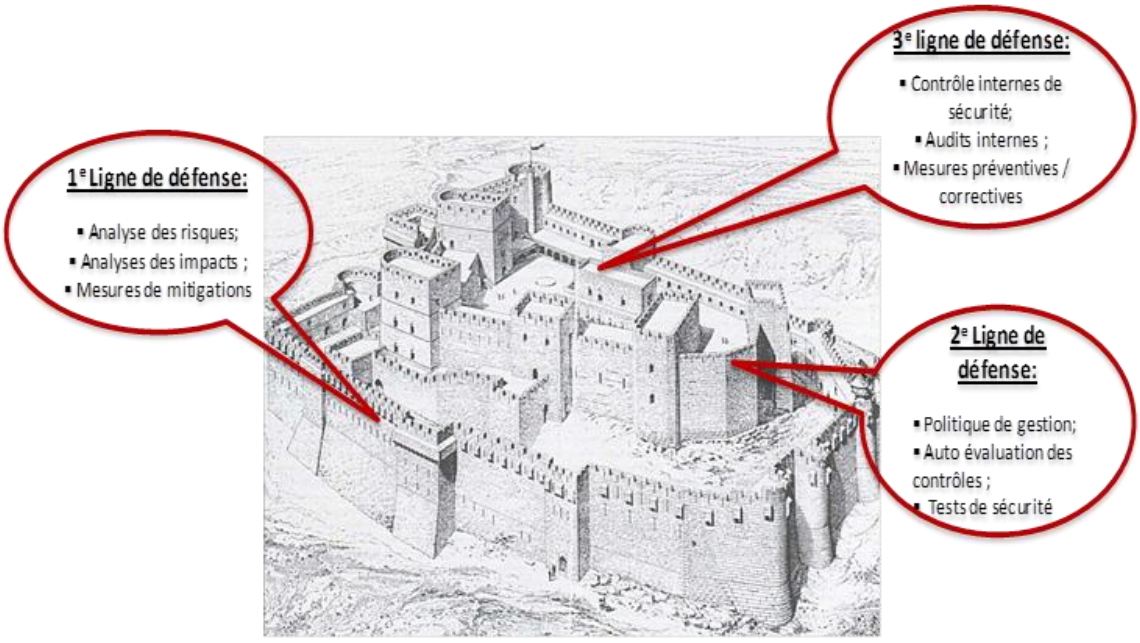
Pour des raisons d'harmonisation, la formalisation d'un tel processus devrait être confiée à un organisme public ayant l'expertise approprié en collaboration avec la CAI et tout autre organisme public ayant de l'expertise dans le domaine par exemple le Secrétariat aux institutions démocratiques et à la participation citoyenne du Ministère du conseil exécutif. .

- **Implanter une véritable stratégie de défense en profondeur pour la sécurité des systèmes contenant des renseignements personnels**

Les impératifs de protection de la vie privée des citoyens devraient conduire les organismes publics à mettre en œuvre une véritable stratégie de défense en profondeur sur leurs systèmes informatiques contenant des renseignements personnels.

À l'instar de l'architecture des châteaux forts, la stratégie de défense en profondeur consiste à corréler plusieurs lignes de défense à telle enseigne que si une mesure de sécurité est compromise, il en existera d'autres pour empêcher toute élévation de privilèges.

Exemple de stratégie de défense en profondeur



3. CONCLUSION

Les caractéristiques des technologies de l'information en termes d'instantanéité, d'automaticité et d'extra-territorialité soulèvent de toute évidence une problématique quant à la protection de la vie privée des citoyens.

Il s'agit ici de raisonner sur un corpus de règles spécifiques, consacrées par les chartes des droits et libertés et qui sont le fondement de toute société libre et démocratique.

Dans un État de droit, la volonté de légiférer ne doit pas conduire à recourir de manière automatique à la mise en en œuvre de dispositions modificatives chaque fois qu'un phénomène nouveau se présente.

Les avancées technologiques ne doivent pas en effet conduire à une frénésie législative. Les nouvelles dispositions modificatives de la loi devront être peu nombreuses et mûrement réfléchies afin d'éviter que les délinquants ne profitent des failles contenues dans la loi qui selon toute vraisemblance, ne pourra jamais suivre la cadence des avancées technologiques.

En définitive, les règles de droit ne peuvent pas, à elles seules, régir la protection de la vie privée des citoyens face à des technologies de plus en plus complexes, mieux élaborées et souvent indétectables.

C'est en sens qu'il faut encourager le recours des organismes publics aux bonnes pratiques de l'industrie en technologies et processus de gestion de la sécurité de l'information. C'est là à notre avis, une des alternatives crédible et apte à garantir une meilleure protection de la vie privée des citoyens.

4. ANNEXE 1 : DISPOSITIONS PERTINENTES DE LA LOI CONCERNANT LE CADRE JURIDIQUE DES TI

[Les soulignements sont nôtres]

24. *L'utilisation de fonctions de recherche extensive dans un document technologique qui contient des renseignements personnels et qui, pour une finalité particulière, est rendu public doit être restreinte à cette finalité. Pour ce faire, la personne responsable de l'accès à ce document doit voir à ce que soient mis en place les moyens technologiques appropriés. Elle peut en outre, eu égard aux critères élaborés en vertu du paragraphe 2° de l'article 69, fixer des conditions pour l'utilisation de ces fonctions de recherche.*

25. *La personne responsable de l'accès à un document technologique qui porte un renseignement confidentiel doit prendre les mesures de sécurité propres à en assurer la confidentialité, notamment par un contrôle d'accès effectué au moyen d'un procédé de visibilité réduite ou d'un procédé qui empêche une personne non autorisée de prendre connaissance du renseignement ou, selon le cas, d'avoir accès autrement au document ou aux composantes qui permettent d'y accéder.*