Plan d'action en matière de

Sécurité des renseignements judiciaires

Quatrième édition, 2013

Préparé par Martin Felsky, PhD, JD, pour le Sous-comité de la technologie du Comité sur l'administration de la justice du Conseil canadien de la magistrature, le 4 juillet 2013.

TABLE DES MATIÈRES

Introduction 4

Portée et définitions 6

Conformité 8

Notes à la quatrième édition 9

1. informatique en nuage 10

Préoccupations concernant la sécurité de l'information 11

2. Médias sociaux 12

3. Appareils mobiles 13

4. Mégadonnées 14

Cadre de politique 14

Structure du plan d'action 15

1. Indépendance judiciaire 17

2. Politique 17

3. Organisation de la sécurité de l'information 17

4. Évaluation des risques 18

5. Gestion de l'actif 18

6. Ressources humaines 19

7. Sécurité matérielle 20

8. Exploitation et gestion des communications 20

9. Contrôle d'accès 22

10. Systèmes informatiques 23

11. Gestion des incidents 23

12. Continuité des activités 24

13. Conformité 24

Recommandations du CCT approuvées par le Conseil le 30 novembre 2001 27

Glossaire de termes ou d'acronymes définis 28

Exemple de politique de sécurité des appareils mobiles de Sophos 30

Aperçu des termes utilisés dans les ENS sur l'information judiciaire 34

INTRODUCTION

Le présent Plan d'action vise plusieurs objectifs dont le principal consiste à fournir des lignes de conduite afin d'améliorer la sécurité, l'accessibilité et l'intégrité des renseignements judiciaires. Il vise également à définir clairement les rôles et responsabilités respectifs des juges et des administrateurs en ce qui concerne la sécurité des technologies de l'information et à améliorer les relations entre les deux groupes. Enfin, le Plan d'action est conçu de manière à fournir aux juges de l'ensemble du Canada un modèle pour l'élaboration de politiques efficaces relatives à la sécurité des technologies de l'information qui tiennent compte des principes de l'indépendance judiciaire.

Le Conseil canadien de la magistrature (le Conseil) est heureux que, depuis la publication de la première édition du Plan d'action en 2004, de nombreuses cours aient adopté des politiques de sécurité inspirées du Plan d'action et compatibles avec celui-ci[1]. À l'origine, le Conseil était préoccupé par le fait que le niveau de sécurité des renseignements judiciaires dans l'ensemble du Canada était inégal et différent d'une juridiction à l'autre, mais ces préoccupations ont maintenant été résolues en grande partie. Le Conseil est d'avis que les cours et les juges devraient continuer d'uniformiser l'approche à l'égard de la sécurité des renseignements judiciaires le plus possible parmi l'ensemble des cours. Des pratiques exemplaires doivent être arrêtées, mises en œuvre et tenues à jour dans tous les cas.

Le Conseil est également préoccupé par le fait que, dans certaines cours, les juges ne participent peut-être pas à la formulation des politiques. Le Conseil veut s'assurer que les juges jouent un plus grand rôle dans l'élaboration des politiques et que toutes les mesures de sécurité prises par les cours soient compatibles avec les principes fondamentaux de l'indépendance judiciaire.

Pour les juges, la sécurité des renseignements présente des défis d'ordre pratique en raison de la situation constitutionnelle unique du Canada. Par exemple, dans la plupart des cours, des administrateurs qui ne relèvent pas de l'autorité judiciaire fournissent tous les services informatiques aux juges. Non seulement la ligne qui sépare les juges et ces administrateurs est-elle mal définie, mais il est rare qu'un lien hiérarchique existe entre les deux groupes. C'est ce qui explique qu'il est parfois difficile pour les administrateurs d'obtenir la collaboration des juges au plan de l'application d'une politique informatique, tout comme il peut être difficile pour les juges de diriger les travaux du personnel de soutien technique.

Le Conseil suggère que les administrateurs de l'informatique, le personnel de soutien et le personnel des services de dépannage qui travaillent avec les utilisateurs judiciaires soient mis au courant de la nature du rôle et de la fonction judiciaire dans le cadre de l'administration de la justice. Toutes ces personnes doivent faire la distinction entre les utilisateurs judiciaires et les autres utilisateurs afin de préserver l'indépendance judiciaire.

[1] Au moment de mettre sous presse, les cours de la Colombie-Britannique, de l'Alberta, de la Saskatchewan, de l'Ontario, du Québec, du Nouveau-Brunswick, de la Nouvelle-Écosse et de l'Île-du-Prince-Édouard ont mandaté des personnes ou des équipes pour jouer le rôle décrit dans le plan d'action sous le vocable «agent de la sécurité informatique du système judiciaire». La Cour suprême du Canada et le Service administratif des tribunaux judiciaires du gouvernement fédéral ont également mandaté des personnes pour tenir ce rôle.

Le Conseil canadien de la magistrature a donné suite à plusieurs recommandations qui ont été formulées en novembre 2001[2] et qui reposent sur les principes fondamentaux suivants :

- Les juges et les administrateurs des cours doivent faire de la sécurité des technologies de l'information (sécurité informatique) une priorité au sein de leurs cours.
- La sécurité informatique n'est pas seulement une préoccupation d'ordre technique; elle met aussi en cause les méthodes de planification, de gestion et d'exploitation ainsi que les pratiques des utilisateurs finaux.
- Toutes les mesures que prennent les cours en matière sécurité informatique doivent préserver l'indépendance judiciaire ainsi que les autres aspects uniques des rapports entre les utilisateurs judiciaires et le personnel chargé de l'administration des systèmes informatiques au sein des cours, que la gestion relève du gouvernement, d'un organisme offrant des services judiciaires ou même du secteur privé.
- La responsabilité relative aux politiques de sécurité informatique en ce qui concerne les renseignements judiciaires est une fonction judiciaire et relève donc de la magistrature.
- La gestion, l'exploitation et les mesures techniques visant à protéger les renseignements judiciaires conformément à la politique judiciaire sont des fonctions administratives qui relèvent, dans le cas de la plupart des cours, du gouvernement provincial[3].

Plus récemment, le Conseil a adopté seize politiques fondamentales touchant la gouvernance de l'information judiciaire, qui sont énoncées dans le *Cadre de politique de gestion de l'information judiciaire dans le monde numérique* (« le Cadre de politique »)[4]. On y énonce également des politiques relatives à l'accès, à la protection de la vie privée, à la sécurité, à la préservation et à la mesure du rendement. Le plan d'action a été réécrit pour qu'il soit conforme aux politiques du Cadre.

Le Plan d'action constitue une partie de l'approche du Conseil à l'égard de la sécurité des renseignements judiciaires. Le site Web du Conseil (www.cjc-ccm.gc.ca) présente de plus amples renseignements sur les initiatives connexes.

[2] Voir l'annexe 1. Le rapport complet de 2001 est confidentiel, car il traite des vulnérabilités des systèmes judiciaires.

[3] Bien que cette question ne se pose pas dans le cas des cours fédérales, comme la Cour suprême du Canada, le gouvernement fédéral considère que la fourniture de services d'accès Internet (par l'entremise de SCNet) constitue une fonction gouvernementale.

[4] http://www.cjc-ccm.gc.ca/cmslib/general/AJC/Information%20Judiciaire%20dans%20le%20monde%20numérique%202013-03.pdf

PORTÉE ET DÉFINITIONS

Même si le mandat légal du Conseil vise seulement les juges nommés par le gouvernement fédéral, il arrive souvent que ces juges partagent des ressources informatiques avec leurs collègues nommés par les gouvernements provinciaux. Cette seule raison suffit à encourager la collaboration à l'égard de l'élaboration des politiques en matière de sécurité. Le Plan d'action s'applique à tout système informatique utilisé pour l'information judiciaire. Ceci peut comprendre les ordinateurs à la maison, certains périphériques, les réseaux de transmission de données et les appareils mobiles.

Selon la définition donnée dans le Cadre de politique, l'officier de justice est « une personne qui agit à titre judiciaire ou quasi judiciaire, y compris les juges, les juges suppléants, les conseillers-maîtres, les juges de paix, les greffiers, les protonotaires ou toute autre personne autorisée à remplir une fonction judiciaire ou quasi judiciaire ». Dans ce plan d'action, l'expression « utilisateur judiciaire » englobe les officiers de justice et l'ensemble des personnes ayant accès à l'information judiciaire.

Il n'existe pas de définition largement acceptée de l'« information judiciaire ». Le Cadre de politique aborde cependant la question de la définition de l'information judiciaire. On y note que la notion d'information judiciaire peut chevaucher des expressions définies comme « dossier d'instance » ou « dossier de la cour », qui sont des catégories de l'information judiciaire. Le Conseil propose d'utiliser les définitions du Cadre de politique comme modèles permettant d'assurer une certaine uniformité entre les juridictions. Les définitions suivantes sont maintenant utilisées dans le Plan d'action :

L'***information judiciaire*** est l'information qui est stockée, reçue, produite ou utilisée par un officier de justice ou à son intention. Cela comprend aussi l'information qui est stockée, reçue, produite ou utilisée par ou pour le personnel de la cour ou les entrepreneurs qui travaillent directement pour les juges ou en leur nom, par exemple les cadres dirigeants, les stagiaires en droit, les étudiants en droit, les commis judiciaires ou les adjoints judiciaires[5].

Il y a trois principaux types d'information judiciaire :

L'***information judiciaire individuelle*** comprend les produits des travaux, les documents de recherche et l'information concernant le perfectionnement professionnel des avocats-conseils internes, des greffiers et des officiers de justice. Cette catégorie engloberait aussi l'**information concernant le greffe**, qui comprend les affaires de ressources humaines du personnel de la cour, l'information sur l'attribution des causes, les statistiques et les politiques de la cour. Les activités relatives à la participation à un comité judiciaire relèveraient aussi de cette définition.

L'***information judiciaire générale*** comprend l'information utilisée par les juges en chef, les documents des comités, les statistiques, les documents de recherche et l'information concernant le perfectionnement professionnel pour l'ensemble de la cour.

L'***information judiciaire personnelle*** comprend l'information produite par un officier de justice ou en son nom,

[5] Pour les besoins du Plan d'action, nous proposons d'ajouter également les « avocats-conseils à l'interne » à ce groupe.

ou l'information le concernant, qui n'est pas directement liée aux fonctions ou au rôle de l'officier de justice et qui n'est pas associée à une affaire[6].

Dans ce contexte, les éléments d'information suivants seraient considérés comme de l'information judiciaire[7] :

- l'information concernant les affaires personnelles ou privées et les relations sociales des juges;
- les travaux concernant un dossier d'instance qui sont de nature très confidentielle (p. ex., les projets de jugement);
- les registres de contrôle qui contiennent des sommaires des activités informatiques des juges;
- l'historique des sites Internet consultés par les juges;
- le courriel des juges qui n'est pas directement lié à un dossier d'instance;
- tous les messages textes et la messagerie vocale;
- tous les événements inscrits dans un agenda ou un calendrier, sauf les événements inscrits au registre de la cour, qui sont directement liés à un dossier d'instance;
- les coordonnées de personnes, y compris l'information contenue dans des carnets d'adresses électroniques et enregistrée dans des téléphones mobiles, des applications logicielles de bureau ou d'autres dépôts électroniques;
- l'information échangée par la voie de réseaux sociaux qui n'est pas du domaine public, par exemple les blogues privés et les réseaux collectifs fermés qu'utilisent les juges et leurs collègues professionnels;
- l'information concernant l'horaire des juges au rôle des audiences de la cour;
- le contenu des programmes de formation des juges;
- l'information concernant la participation d'un juge à des programmes de formation;
- les statistiques montrant les activités individuelles ou la charge de travail d'un juge;
- les notes personnelles, la recherche ou les documents de travail produits par un juge ou en son nom qui n'ont pas été versés à un dossier d'instance;
- les activités relatives à la participation à des comités ou à des conseils judiciaires, y compris les communications et les documents de recherche;
- les cahiers d'audience des juges.

On doit se rappeler que l'information judiciaire, selon la définition donnée ci-dessus, existe et doit être protégée non seulement sur les serveurs, appareils et dispositifs de stockage actifs mais aussi sur les systèmes d'archives, d'images et de sauvegarde.

La sécurité des systèmes informatiques est un domaine complexe et le Plan d'action ne peut en couvrir tous les aspects. Le lecteur est prié de consulter les normes, ouvrages et documents mentionnés dans

[6] Extrait du Cadre de politique : « Chaque juridiction devra fournir des directives précises aux technologues à propos des fichiers de l'historique de navigation Internet, des dépôts de courriel, des listes de contacts, des calendriers, des messages textes et du courriel, lorsqu'il s'agira de choisir les éléments d'information à inclure dans cette catégorie [information juridique personnelle] ».

[7] Exemples tirés du Cadre de politique, pages 36-37.

les références indiquées ci-dessous. De plus, le Conseil s'intéresse principalement au rôle de la magistrature dans l'élaboration des normes et politiques et non pas aux détails de la gestion d'un service informatique. À cet égard, le Plan d'action ne couvre pas chacun des aspects de l'administration de la sécurité. Il ne traite pas non plus de la sécurité relative au soutien et à l'exploitation des systèmes informatiques, de la sécurité des renseignements qui ne sont pas sous forme numérique, de la sécurité des communications par téléphone ou par télécopieur, ni de la sécurité matérielle des palais de justice et de ses occupants.

Le Plan d'action vise à améliorer les politiques et programmes gouvernementaux existants et à les remplacer *uniquement s'ils vont à l'encontre de ceux qui sont proposés dans le présent document ou s'ils sont moins stricts que ceux-ci*. Dans cette mesure, le Plan d'action est conçu pour être utilisé conjointement avec les normes, lignes directrices et pratiques exemplaires mondiales en matière de sécurité informatique, comme la norme ISO 27002, le cadre *CobiT* de l'*ISACA*[8], la norme de bonne pratique de l'*Information Security Forum*[9], ainsi que diverses publications et avant-projets de l'INST, notamment le 800-53 (Recommended Security Controls for Federal Information Systems ») et la 800-39, (« *Managing Risk from Information Systems* »)[10]. Le document publié par Ken Fogalin en 2009, intitulé « *Improving the Management of Information Security in Canadian Government Departments* »[11], présente un examen utile et détaillé des différences entre les exigences de la norme GSTI du gouvernement du Canada et la norme ISO 27001.

CONFORMITÉ

Les politiques et normes de sécurité informatique se veulent impératives. Le respect universel des exigences en matière de sécurité protège tous les utilisateurs d'un organisme. Cependant, les juges sont différents des autres utilisateurs en ce qui a trait à au moins un aspect vital : ils ne sont pas assujettis à la surveillance ni aux procédures disciplinaires de l'organisme qui assure leurs besoins informatiques.

L'idée même que certaines politiques ou procédures soient impératives préoccupe de nombreux juges. Toutefois, il y va de la sécurité et de l'intégrité de tous les renseignements judiciaires. Puisque le Conseil propose que les juges formulent ou approuvent toutes les normes et politiques les concernant, il serait plus facile d'atteindre cette conformité, même en l'absence d'un mécanisme d'application direct.

Il est indéniable que si un seul utilisateur – qu'il s'agisse ou non d'un juge – omet d'observer une norme de sécurité appropriée, cela risque de compromettre l'ensemble du réseau ainsi que la sécurité des renseignements judiciaires de tous les juges et des autres utilisateurs du réseau. Par exemple, si un seul

[8] « Control Objectives for Information and Related Technologies », www.isaca.org.

[9] https://www.isfsecuritystandard.com/SOGP07/index.htm.

[10] National Institute of Standards and Technology, http://csrc.nist.gov/. L'une des ressources originales ayant servi de fondement au Plan d'action est le *Canadian Handbook on Information Technology Security*, publié en mars 1998 par le Centre de la sécurité des télécommunications (« Manuel CST »).

[11] Voir http://www.sans.org/reading_room/whitepapers/leadership/improving_the_management_of_information_sécurité_in_canadian_government_departments_33063.

juge choisit un mot de passe faible ou omet de chiffrer convenablement un document de nature délicate joint à un courriel (comme un projet de jugement), une personne de l'extérieur non autorisée pourrait obtenir accès non seulement aux dossiers du juge imprudent, mais aussi à ceux des juges qui accordent la plus haute importance à la sécurité de leurs renseignements. C'est pourquoi le Conseil encourage tous les juges et les autres utilisateurs du système judiciaire à adopter les politiques et pratiques énoncées au présent document, non seulement dans l'intérêt de l'appareil judiciaire, mais également pour les tierces parties dont les renseignements nécessitent une protection spéciale en vertu de la loi.

Dans certains cas où les autorités provinciales ont demandé aux juges de respecter des règles gouvernementales sur la sécurité ou des politiques d'utilisation acceptable, les juges ont soutenu que leur indépendance risquait d'être compromise. Il est souhaité qu'il sera plus facile pour les juges de se conformer aux recommandations énoncées dans le Plan d'action, étant donné qu'il s'agit d'un document rédigé par des juges à l'intention des juges.

NOTES À LA QUATRIÈME ÉDITION

En plus de veiller à ce que le Plan d'action tienne compte des plus récentes innovations technologiques et des nouvelles pratiques exemplaires en matière de gestion de la sécurité de l'information, le Sous-comité de la technologie du Comité sur l'administration de la justice du Conseil canadien de la magistrature a convenu de réorganiser le document pour en faire une norme minimum très nette, par opposition à une directive générale. Cette nouvelle approche vise à aider la magistrature de l'ensemble du pays dans les négociations avec l'administration des cours, de manière à ce que l'indépendance et la protection de la vie privée des juges soient toujours prises en compte dans la conception et la mise en œuvre des systèmes de sécurité.

Cette quatrième édition du Plan d'action ne se résume donc pas à une simple mise à jour. Des développements importants en matière de technologie ont placé le débat sur l'indépendance judiciaire à l'avant-plan et ont incité la magistrature à se pencher de plus près sur un ensemble de questions touchant la gouvernance de l'information, dont la sécurité.

Même s'il aborde de nouvelles questions et présente de nouvelles politiques, le Plan d'action a été raccourci et simplifié afin que sa lecture soit plus facile et ses sections reprennent celles de la norme ISO 27002, première norme mondiale en matière de sécurité de l'information, dans le but d'en faciliter la mise en œuvre. Les commentaires sont beaucoup moins nombreux que dans la version précédente : l'accent est mis sur le rôle croissant de la magistrature dans l'élaboration des politiques et la conformité de la vérification, et non sur les détails techniques de la mise en œuvre.

Dans la présente édition, nous avons évité les détails techniques pour trois raisons : d'abord parce que des instructions spécifiques deviennent rapidement périmées et ne doivent pas être utilisées comme point de référence en matière de sécurité lorsque de nouvelles méthodes, plus efficaces, deviennent disponibles; ensuite, parce que des instructions qui sont trop spécifiques ne peuvent s'appliquer qu'à certaines cours et sont inutiles pour les autres; et enfin, parce qu'il n'est ni nécessaire ni utile que le Plan d'action répète les normes et directives très détaillées et hautement techniques déjà appliquées par les différents gouvernements au pays. La valeur et l'importance réelles du Plan d'action résident dans l'accent placé sur la magistrature à titre de propriétaire de l'information et sur la façon dont le principe de l'indépendance judiciaire doit être respecté dans la planification et l'application de la sécurité informatique dans l'ensemble du système de justice.

Depuis la publication de la troisième édition en 2009, quatre technologies en particulier ont eu une incidence immense sur la réflexion en matière de sécurité informatique et soulevé de nouvelles préoccupations à propos de la cybersécurité à l'échelle internationale. Ces quatre avancées technologiques ayant eu l'effet le plus marqué sur les pratiques de sécurité informatique sont :

1. l'informatique en nuage;
2. les médias sociaux;
3. les appareils mobiles;
4. les mégadonnées.

Nous les aborderons à tour de rôle.

1. INFORMATIQUE EN NUAGE

L'informatique en nuage a soulevé des préoccupations particulières au sein de la magistrature, notamment au plan de l'indépendance judiciaire. Comme les lecteurs du Plan d'action le savent, c'est le caractère unique de l'indépendance judiciaire qui distingue le Plan d'action des autres documents de politique sur la sécurité informatique et qui fait du Plan d'action une ressource indispensable pour de très nombreux juges et administrateurs judiciaires.

Même si la technologie reste relativement jeune, l'informatique en nuage gagne rapidement en popularité. Bien que sa définition soit un peu floue, elle suppose généralement que les utilisateurs aient accès à des ressources informatiques hors site et partagées avec d'autres utilisateurs, par la magie de la virtualisation[12]. L'informatique en nuage permet à différents utilisateurs dans différentes organisations de partager le matériel, les services de réseau et même des logiciels dans un même centre de données, chaque organisation gérant de façon indépendante ses propres accès d'utilisateurs et son information. Cette façon de faire s'oppose à l'architecture informatique traditionnelle, dans laquelle chaque organisme construit ses propres centres de données et se procure son propre équipement de réseau,

[12] La virtualisation est une technologie qui permet d'installer de multiples instances d'un système d'exploitation sur un seul serveur physique ou sur une grappe de serveurs, ce qui permet la consolidation efficace du matériel des serveurs tout en maintenant la séparation des utilisateurs et des applications, ce qui n'était possible auparavant qu'en utilisant des serveurs physiques distincts.

son matériel informatique et ses logiciels. L'avantage de l'informatique en nuage tient au fait que la consolidation de l'investissement dans l'espace physique, la gestion, le matériel, les logiciels, les communications, l'alimentation électrique, la sauvegarde des données et la sécurité, permet aux utilisateurs de n'utiliser et de ne payer que la puissance informatique dont ils ont besoin, laissant l'administration de la technologie à leur fournisseur de services.

L'informatique en nuage est une technologie et pas nécessairement une entreprise commerciale. Pour cette raison, les organisations qui préfèrent ne pas impartir la fourniture de services informatiques et de réseau peuvent mettre en place une infrastructure d'informatique en nuage à l'interne (« nuage privé »). Même sans impartition, il est possible de réaliser des économies très importantes grâce à la centralisation, à la consolidation et à la virtualisation des ressources physiques, ainsi qu'à la centralisation des infrastructures régionales de gestion des TI et de soutien qui se chevauchent.

Les différents gouvernements du pays ne sont pas insensibles aux avantages offerts par la consolidation du matériel et des services de soutien informatiques, de sécurité et autres services de gestion, et ont entrepris de suivre la tendance mondiale. Les économies sont particulièrement intéressantes pour les services d'administration judiciaire, les cours étant réparties à travers le pays dans des juridictions nombreuses, parfois de très petite taille et manquant de ressources.

Un autre aspect de l'informatique en nuage pertinent à la sécurité of l'information judiciaire réside dans ce qu'on peut appeler les « nuages personnels ». Les personnes qui utilisent des applications sur appareils mobiles peuvent être tenues ou avoir l'option de sauvegarder leurs données « dans le nuage » ou de faire appel à un tiers fournisseur fonctionnant en nuage pour assurer la synchronisation entre leur appareil mobile et leurs autres appareils. Bien que ces services soient très commodes et offrent une mesure de confort (grâce à la sauvegarde des données de l'appareil mobile), il y a un risque que l'information judiciaire soit compromise, parce qu'elle est confiée à la garde d'un tiers inconnu, souvent basé à l'extérieur du pays. Les données peuvent alors ne plus être protégées par les lois sur la protection de la vie privée ou par des protections contractuelles exécutoires.

PRÉOCCUPATIONS CONCERNANT LA SÉCURITÉ DE L'INFORMATION

L'efficacité et les économies associées à l'informatique en nuage s'accompagnent habituellement d'une augmentation de la sécurité matérielle, parce que la protection d'un seul grand centre de données est beaucoup moins coûteuse que la protection d'une douzaine ou d'une centaine de petits centres répartis entre les districts judiciaires. Les préoccupations à propos de l'informatique en nuage pour les cours ne concernent pas tant la sécurité matérielle, mais plutôt la sécurité organisationnelle, la sécurité du personnel et la sécurité informatique. La tendance vers les services partagés, par exemple, qui peut être une étape vers l'informatique en nuage, est une préoccupation importante pour la magistrature, parce qu'elle soulève des questions sur la responsabilité, la ségrégation, la propriété, l'accès aux données, la garde et le contrôle de l'information judiciaire[13].

[13] Comme l'affirme la publication spéciale 800-146 du NIST, « Lorsqu'un organisme s'abonne à des services en nuages, la totalité des données produites et traitées résident physiquement dans des lieux appartenant au fournisseur et qu'il administre.

Du point de vue du gouvernement, la consolidation permet un meilleur contrôle sur les dépenses et la gestion informatiques. Du point de vue de la magistrature, par contre, la consolidation des réseaux, de l'informatique et des services de soutien se traduit par une diminution du contrôle et donc une plus grande incertitude à propos de la protection de l'information judiciaire. Pour cette raison, les magistrats de chacune des juridictions touchées ont demandé une plus grande transparence et une voix plus forte dans les processus de planification et de mise en œuvre.

En règle générale, si le pouvoir exécutif doit fournir des services d'information à la magistrature, que ce soit directement ou dans le cadre d'un partenariat avec des tiers fournisseurs, la magistrature doit jouer un rôle actif en précisant comment elle souhaite que l'information judiciaire soit gérée par son fournisseur de services. Pour cette raison, la présente version du Plan d'action présente, à l'annexe 4, un aperçu d'un accord sur les niveaux de service qui pourrait être utilisé comme modèle par toutes les juridictions. La politique 9e traite plus particulièrement de certains risques associés aux services en nuage.

2. MÉDIAS SOCIAUX

La croissance rapide et l'omniprésence des médias sociaux ont eu des répercussions importantes sur la réflexion concernant les tribunaux ouverts. Puisque l'utilisation des médias sociaux, comme le microblogage durant un procès ne constitue pas à strictement parler un enjeu de sécurité et ne concerne pas nécessairement l'information judiciaire, elle sort du champ du Plan d'action. Certaines cours ont établi des politiques régissant l'utilisation des médias sociaux dans les salles d'audience. Les préoccupations à propos des médias sociaux portent également sur l'utilisation des médias sociaux par les officiers de justice et les utilisateurs judiciaires. Par exemple, lorsque les administrateurs judiciaires utilisent les médias sociaux, représentent-ils le tribunal? Si les juges deviennent actifs sur les médias sociaux, comment doivent-ils se comporter, et est-il acceptable pour eux de se « connecter » avec des avocats ou des membres du public? Ici encore, bien que ces questions ne relèvent pas du champ du plan d'action, elles ont incité le Conseil à poser des questions difficiles sur les relations entre un procès équitable et l'omniprésence des médias sociaux. Les politiques 2b et 8e traitent de certains risques associés aux médias sociaux.

Dans ce contexte, la question fondamentale est de savoir si le consommateur peut obtenir l'assurance que le fournisseur mettra en place des contrôles au moins équivalents à ceux que le consommateur aurait lui-même mis en place ».

3. APPAREILS MOBILES

Les appareils mobiles sont de plus en plus intelligents et commodes. Les téléphones intelligents sont en mesure de faire tourner les centaines de milliers d'applications logicielles offertes sur le marché, et on s'attend à ce que les ventes de tablettes électroniques dépassent bientôt les ventes d'ordinateurs portables. Ces appareils, qu'ils soient fournis par les cours – ou, ce qui est la tendance lourde – achetés par les utilisateurs eux-mêmes, soulèvent plusieurs questions de sécurité.

Premièrement, les appareils mobiles peuvent être configurés pour accéder facilement et de partout aux ressources d'information en réseau. Cependant, et contrairement aux ordinateurs de bureau ou aux ordinateurs portables, qui sont achetés, fournis et entretenus par l'administration judiciaire, les appareils mobiles ne sont généralement pas conçus ou construits et configurés avec les mêmes capacités de sécurité.

Deuxièmement, les appareils mobiles sont des ordinateurs qui peuvent générer, manipuler et conserver des données. Cependant, la protection par mot de passe sur ces appareils peut être faible, les options de cryptage limitées ou inexistantes, et les appareils eux-mêmes sont souvent perdus ou volés, donnant lieu à de graves transgressions de sécurité ou de protection de la vie privée.

Troisièmement, la popularité des applications gratuites et peu coûteuses est largement responsable de la montée en popularité des appareils mobiles. L'utilisation de ces applications est immensément commode mais présente des risques importants, les données créées par l'utilisateur et les données concernant l'utilisateur étant transmises – souvent à l'insu de l'utilisateur – au tiers ayant créé le logiciel.

Quatrièmement, les appareils mobiles sont branchés en permanence sur Internet et les capacités GPS intégrées leur permettent de suivre en temps réel la position et les activités de l'utilisateur, dans certains cas, même lorsque l'appareil est fermé. Si l'appareil est compromis, le microphone et la caméra intégrés peuvent aussi être utilisés pour enregistrer et transmettre des événements et des conversations sans que l'utilisateur ne le sache.

Bien que cela ne relève pas du champ du plan d'action, les appareils mobiles présentent également des défis réels en cas d'enquête ou de projet de communication préalables par voie électronique.

Qu'ils soient fournis par l'administration judiciaire, utilisés dans le cadre d'une politique sur l'utilisation des appareils personnels ou utilisés entièrement en dehors du programme de sécurité de la cour, les appareils mobiles posent un défi aux approches traditionnelles en matière de sécurité de l'information. La politique 8f traite de certains aspects de la sécurité des appareils mobiles.

4. MÉGADONNÉES

Le terme mégadonnées renvoie à la quantité énorme et en croissance rapide de renseignements numériques créés et conservés par les organismes publics et privés. Les mégadonnées peuvent constituer un problème important tout comme une occasion importante pour les organisations. Pour les fins limitées du Plan d'action, les métadonnées soulèvent des questions de protection de la vie privée non seulement pour les utilisateurs judiciaires, mais pour l'ensemble des intervenants du système de justice. Les cours sont confrontées à des problèmes de mégadonnées, par exemple au moment de numériser les anciens rapports juridiques imprimés afin d'en permettre l'accès via CanLII. L'information autrefois disponible uniquement dans des dossiers papier peut maintenant faire l'objet de recherches en ligne. Les renseignements personnels des parties à un litige, relativement difficiles à obtenir en raison de ce qu'on appelait « l'obscurité pratique » du papier, deviennent facilement accessibles à toute personne disposant d'un téléphone intelligent. Bien qu'en principe ces renseignements aient toujours été publics, les décisions passées n'ont pas été formulées en vue d'une publication mondiale et d'un accès public instantané.

Afin d'aider les organisations à organiser et fouiller l'énorme quantité de données structurées et non structurées qu'elles accumulent aujourd'hui, les gouvernements et les grandes organisations privées utilisent une nouvelle série d'outils puissants regroupés sous le vocable « analytique ». Appliqués aux systèmes actuels et à venir des cours, ces processus et programmes peuvent jeter un éclairage très utile sur toutes sortes de données intéressantes, par exemple des statistiques sur la production d'éléments, les délais et les résultats des litiges. En même temps, des renseignements que l'on n'aurait jamais cru disponibles peuvent être extraits, combinés, réunis et présentés sous forme de rapports.

À mesure que les cours continuent de mettre en place des outils automatisés de gestion des dossiers, le dépôt de documents par voie électronique, les procès électroniques et autres technologies similaires, les avantages et les risques associés aux mégadonnées apparaissent rapidement. En plus des préoccupations relatives à la protection de la vie privée, il existe des préoccupations relatives à la propriété des données, à l'exactitude de l'information produite par l'analytique et à l'utilisation qui peut en être faire. La politique 10b traite de certains risques associés aux mégadonnées.

CADRE DE POLITIQUE

Le Cadre de politique offre une approche fondée sur des principes permettant d'établir un large éventail de politiques d'information judiciaire, notamment la sécurité de l'information. L'un des aspects du mandat de mise à jour du Plan d'action consiste donc à assurer la cohérence avec les valeurs, les principes, les politiques et les définitions énoncés dans le Cadre de politique, auquel le lecteur du Plan d'action devrait se référer[14].

[14] http://www.cjc-ccm.gc.ca/cmslib/general/AJC/Information%20Judiciaire%20dans%20le%20monde%20numérique%202013-03.pdf

STRUCTURE DU PLAN D'ACTION

Lors de la conception du premier *Plan d'action* il y a maintenant plus de douze ans, il était important d'adjoindre aux politiques énoncées des notes explicatives afin de rehausser le degré de sensibilisation aux différents aspects de la sécurité de l'information. Depuis ce temps, les qualifications et les compétences du personnel de TI du gouvernement ont augmenté et la sécurité est prise beaucoup plus au sérieux par les différents gouvernements du pays. Dans la présente révision, nous avons tenté d'éliminer les chevauchements avec les normes bien connues de l'industrie, comme la norme ISO 27002 et avec d'autres normes détaillées appliquées dans l'ensemble du gouvernement, notamment :

- *British Columbia Information Security Policy* (octobre 2012), publiée par le Bureau du Premier dirigeant de l'information du gouvernement de la Colombie-Britannique;
- Normes en matière de technologies de l'information du gouvernement de l'Ontario, par exemple la norme 25.18 « *Physical Security Requirements for Data Centres* »;
- *Standard of Good Practice for Information Security*, publiée par l'Information Security Forum (ISF) et utilisée au Nouveau-Brunswick.

Dans cette quatrième édition du Plan d'action, l'important n'est pas de reprendre les éléments de base bien connus de la sécurité informatique, mais de mettre en lumière la nature unique de l'information judiciaire et de guider les personnes responsables de la mise en œuvre des politiques à l'égard des besoins particuliers des utilisateurs judiciaires.

Afin de faciliter l'intégration des politiques du Plan d'action aux politiques et normes gouvernementales existantes, cette quatrième édition du Plan d'action a été réorganisée afin de mieux suivre la structure de la norme ISO/IEC 27002. À cette fin, nous avons préparé le tableau de concordance qui suit[15].

[15] Certaines politiques de la 3e édition peuvent figurer plus d'une fois parce qu'elles sont pertinentes à plus d'un chapitre de la norme ISO.

Chapitre ISO 27002	Plan d'action, 4e édition (2013)	Plan d'action, 3e édition (2009)
	1. Indépendance judiciaire	10. Indépendance judiciaire
4. Évaluation des risques	4. Évaluation des risques	4. Évaluation des menaces et des risques
5. Politique de sécurité	2. Politique	2. Politique et planification
6. Organisation de la sécurité de l'information	3. Organisation de la sécurité de l'information	1. Agent de la sécurité informatique du système judiciaire
7. Gestion de l'actif	5. Gestion de l'actif	7. Classification de l'information judiciaire
8. Ressources humaines	6. Ressources humaines	3. Sensibilisation et formation en matière de sécurité
9. Sécurités physiques et environnementales	7. Sécurité matérielle	6. Sécurité matérielle
10. Exploitation et gestion des communications	8. Exploitation et gestion des communications	13. Systèmes de détection d'intrusion 14. Protection contre les codes malveillants, les pourriels et les menaces connexes
11. Contrôle d'accès	9. Contrôle d'accès	8. Contrôle de l'accès aux systèmes des cours 9. Contrôle de l'accès à distance et réseaux sans fil 10. Indépendance judiciaire 12. Pare-feux
12. Acquisition, développement et maintenance des systèmes informatiques	10. Systèmes informatiques	7. Classification de l'information judiciaire 11. Chiffrement
13. Gestion des incidents	11. Gestion des incidents	
14. Continuité des activités	12. Continuité des activités	5. Sauvegarde et continuité des opérations
15. Conformité	13. Conformité	Introduction

POLITIQUES[16]

1. INDÉPENDANCE JUDICIAIRE

Politique 1a : Les principes de l'indépendance judiciaire doivent être incorporés dans tout système informatique traitant de l'information judiciaire ou servant les utilisateurs judiciaires.

Politique 1b : Tous les juges et tout le personnel des cours devraient utiliser un domaine Internet commun qui est séparé de celui du gouvernement et ils devraient employer ce domaine pour toutes leurs communications (Cadre de politique, politique fondamentale 8).

2. POLITIQUE

Politique 2a : La magistrature est responsable de la préparation et de l'approbation des politiques de sécurité ayant une incidence sur les utilisateurs judiciaires ou l'information judiciaire. Toutes les politiques de sécurité des cours doivent être interprétées et appliquées conformément aux directives de surveillance du Conseil.

Politique 2b : Afin de préserver la réputation du système de justice et d'assurer l'équilibre entre les principes d'audience publique et d'impartialité des procédures, la magistrature doit établir des politiques et des codes de conduite pour l'utilisation des médias sociaux par les utilisateurs judiciaires.

Politique 2c : Les politiques de gestion de l'information seront publiées sur le site Web de la cour. (Cadre de politique, politique d'accès 7).

3. ORGANISATION DE LA SÉCURITÉ DE L'INFORMATION

Politique 3a : La gestion de la sécurité de l'information judiciaire doit s'insérer dans un programme de sécurité formel et documenté, autorisé et adéquatement financé par l'instance gouvernementale responsable de l'administration judiciaire.

Commentaire : La sécurité de l'information judiciaire ne peut être laissée à des processus ad hoc, informels et non documentés, et sa responsabilité ne peut être déléguée à des employés subalternes. Des budgets adéquats doivent y être consacrés afin d'assurer la sécurité et l'intégrité de l'information judiciaire, selon l'évaluation de la menace et du risque (Politique 4).

Politique 3b : Chaque juridiction doit nommer un agent de la sécurité informatique du système judiciaire, responsable devant la magistrature, afin de superviser la gestion des opérations technologiques de sécurité de l'information.

Politique 3c : Des évaluations de l'incidence sur la protection de la vie privée seront réalisées à l'étape de la conception de systèmes de gestion de l'information des cours qui tiennent compte de la collecte

[16] Le Plan d'action comprend 13 catégories de politiques et 45 politiques individuelles au total.

potentielle, de l'accès, de l'utilisation ou de la diffusion des renseignements personnels (Cadre de politique, politique de protection de la vie privée 3).

4. ÉVALUATION DES RISQUES

Politique 4 : Chaque cour doit planifier et effectuer, sur une base régulière, une évaluation des menaces et des risques (EMR) en collaboration avec la magistrature. Le degré de détail requis dans une EMR, sa portée et l'intervalle entre les évaluations peuvent varier d'une cour à une autre, selon les circonstances.

5. GESTION DE L'ACTIF

Politique 5a : La totalité de l'information judiciaire, incluant l'équipement de gestion, est considérée comme un actif; à ce titre, on doit en faire l'inventaire et y affecter des propriétaires et des gardiens.

Politique 5b : L'équipement, le matériel et les supports utilisés pour conserver l'information judiciaire doivent être éliminés de façon sécurisée.

Politique 5c : Peu importe qui en a la garde, la magistrature est toujours propriétaire de l'information judiciaire.

Politique 5d : Les cours doivent adopter un modèle de classification permettant de désigner l'information judiciaire pour isolement.

Commentaire : Lorsque nous pensons actif, nous pensons généralement aux serveurs, aux ordinateurs mobiles aux autres composantes matérielles qui constituent un système informatique complexe, avec les imprimantes, les numériseurs, les moniteurs et les différents périphériques qui se trouvent dans un centre de données. Parce que tellement de ces actifs physiques et éléments peuvent contenir ou sauvegarder de l'information judiciaire, et parce que les appareils mobiles sont si faciles à oublier ou à perdre, il est important que tout l'équipement physique soit inventorié, étiqueté, suivi et sécurisé physiquement (ou sécurisé par chiffrement si possible).

Il peut être plus difficile de concevoir l'information elle-même comme un élément d'actif. En fait, traiter l'information comme un actif permet de comprendre plus facilement pourquoi il est si important de la protéger. Si les cours accumulaient des stocks de diamants, personne ne s'interrogerait sur la nécessité de dépenser les sommes nécessaires pour en assurer la protection, les diamants ayant une valeur monétaire établie. Bien qu'il soit probablement impossible d'attribuer une valeur monétaire précise à l'information judiciaire, il est clair qu'en son absence le système judiciaire ne pourrait tout simplement pas fonctionner.

Ayant reconnu l'information comme un actif, même invisible, nous devons l'inventorier, l'étiqueter, le surveiller et le sécuriser, tout comme nous le faisons pour les biens d'équipement plus visibles et plus faciles à protéger physiquement. Nous avons une tâche additionnelle, rendue plus difficile par la nature même de l'information : celle de la propriété. Il est important de déterminer la propriété de chaque

catégorie d'information dans le système judiciaire, y compris les bases de données, les logiciels, les dossiers de cour, les plaidoiries, etc.

La politique 5b n'est pas une proclamation de propriété juridique. Le mot « propriété » est plutôt utilisé dans le sens de « prendre la responsabilité de quelque chose ». Les discussions juridiques sur les droits de propriété, s'ils existent, sont extérieures à notre propos ici. Rien dans cette politique n'empêche, s'il y a lieu, la propriété conjointe lorsque des renseignements peuvent appartenir à la fois à l'information judiciaire et non judiciaire.

Dans certains cas, l'isolement de l'information sensible dont il est fait état dans l'énoncé de la politique 5d peut nécessiter le recours à des systèmes complètement externes à la cour, comme JUDICOM.

6. RESSOURCES HUMAINES

Politique 6a : Toutes les cours doivent s'assurer de disposer de procédures documentées pour l'orientation et les départs, et de programmes de formation continue pour les employés et les fournisseurs ayant accès à l'information judiciaire. Des processus doivent être mis en place pour confirmer que les employés et les fournisseurs disposent du niveau d'autorisation de sécurité approprié. Les procédures doivent prévoir des mesures disciplinaires en cas d'infraction aux politiques sur la sécurité de l'information judiciaire.

Politique 6b : Nul ne devrait avoir un accès de niveau utilisateur à l'information judiciaire à moins de satisfaire au minimum aux conditions suivantes :

- besoin de savoir;
- avoir fait l'objet d'une vérification policière des antécédents de sécurité;
- avoir satisfait aux autres procédures applicables en matière de vérification de sécurité;
- avoir été informé de la nature particulière de l'information judiciaire (« Des stratégies de formation du personnel doivent être adoptées afin de mieux faire comprendre le caractère délicat de l'***information judiciaire »,*** Cadre de politique, politique de sécurité 4);
- avoir reçu une formation sur l'ensemble des politiques, procédures et pratiques de sécurité applicables;
- avoir signé une entente documentant ses obligations en matière de sécurité de l'information judiciaire (« Les contrats d'engagement du personnel, des consultants et des entrepreneurs doivent contenir des ententes de confidentialité pour prévenir la divulgation d'information judiciaire confidentielle » (Cadre de politique, politique de sécurité 2).

Politique 6c : Nul ne devrait avoir un accès de niveau administrateur à l'information judiciaire à moins de satisfaire au minimum aux conditions suivantes de la politique 6b et d'avoir obtenu une autorisation de sécurité gouvernementale d'un niveau correspondant à son rôle.

7. SÉCURITÉ MATÉRIELLE

Politique 7a : L'ensemble de l'équipement et des installations utilisés dans le traitement de l'information judiciaire doit être situé dans un lieu physiquement sécurisé, dont l'accès est limité aux personnes autorisées.

Politique 7b : Des mesures fermes doivent être prises pour assurer la protection physique des câbles de réseau et d'alimentation des installations de traitement.

Politique 7c : Les mesures de sécurité matérielle doivent être conçues pour protéger l'information judiciaire contre les catastrophes naturelles et les menaces humaines, conformément à l'évaluation des menaces et des risques.

Politique 7d : Seuls les utilisateurs autorisés peuvent emporter hors de l'environnement sécurisé de l'équipement qui contient de l'information judiciaire ou permet d'y accéder.

Commentaire : La sécurité matérielle renvoie à la protection des bâtiments et de l'équipement (ainsi que de l'information et des logiciels qui y sont contenus) contre l'intrusion par effraction, le vol, le vandalisme, les catastrophes naturelles ou artificielles et les dommages accidentels. Les gestionnaires doivent s'intéresser à la construction des bâtiments destinés aux services informatiques, à l'affectation des salles, aux procédures de mesures d'urgence, aux règlements qui régissent la disposition et l'utilisation de l'équipement, à l'alimentation en énergie et en eau, à la manutention des produits et aux relations avec le personnel, les entrepreneurs externes, les autres cours ainsi que les ministères, organismes et tribunaux gouvernementaux.

8. EXPLOITATION ET GESTION DES COMMUNICATIONS

Politique 8a : Les programmes de sécurité judiciaire doivent comprendre des contrôles, des procédures et des pratiques documentées et approuvées en matière d'exploitation, et des responsabilités bien définies. Des politiques, procédures et contrôles formels additionnels doivent être utilisés afin de protéger l'échange et la publication de l'information judiciaire par n'importe quel type de moyen ou de technologie de communication.

Politique 8b : La surveillance des utilisateurs judiciaires, s'il y a lieu, doit se faire en conformité avec les *Lignes de conduite sur la surveillance informatique* (2002) du Conseil canadien de la magistrature. (« En principe absolu, la surveillance informatique des juges et du personnel judiciaire relevant directement des juges doit avoir un motif bien défini et justifiable n'empiétant pas sur le secret des délibérations, la confidentialité, le droit à la vie privée ou l'indépendance judiciaire »).

Politique 8c : Il incombe aux cours de mettre en place les contrôles nécessaires pour se protéger contre le code malveillant, les attaques de déni de service et les menaces externes similaires.

Politique 8d : Lorsqu'un tiers fournit des services reliés à l'information judiciaire, la conformité avec le Plan d'action doit être exigée par l'entente et faire l'objet d'une surveillance.

Politique 8e : Aucun élément d'information judiciaire ne peut être publié, partagé, échangé ou fourni à un tiers, y compris à tout organisme gouvernemental, sans l'autorisation écrite préalable de la magistrature et conformément aux lois applicables.

Politique 8f : Les cours doivent se doter d'une politique conforme au Plan d'action pour les appareils mobiles et mettre en place des protocoles de sécurité prévoyant l'effacement des données des appareils perdus ou volés[17].

Politique 8g : Les systèmes et les technologies d'information des cours doivent être obtenus, conçus et mis en œuvre de manière à faciliter l'interopérabilité et l'échange de données entre différents systèmes, sans compromettre l'indépendance des systèmes, l'indépendance judiciaire ni le rôle des cours comme dépositaires des dossiers de la cour (Cadre de politique, politique fondamentale 4).

Commentaire : Les contrôles opérationnels traitent généralement les aspects fondamentaux suivants des activités judiciaires :

- documentation appropriée de toutes les fonctions normales et d'urgence des cours;
- procédures de gestion du changement;
- séparations des responsabilités;
- capacité du système et planification des ressources;
- politiques et procédures de sauvegarde et de restauration;
- infrastructure, outils, processus et formation de chiffrement;
- manutention des supports, y compris la manutention des supports amovibles et disposition sécuritaire de l'ensemble de l'équipement et des supports informatiques;
- surveillance des systèmes, gestion du journal et vérification;
- protection contre le code malveillant et mobile;
- protection contre les attaques de déni de services et autres attaques similaires;
- contrôles et procédures de sécurité pour les supports physiques contenant des données en transit dans et à l'extérieur de la cour;
- services de commerce électronique y compris la sécurité des dépôts électroniques, des registres en ligne et de l'information disponible au public.

[17] Voir l'exemple de politique à l'annexe 3. Même avec des outils efficaces d'effacement à distance, si l'appareil n'est pas connecté à Internet ou s'il est placé en mode « avion », l'effacement à distance n'est pas possible.

9. CONTRÔLE D'ACCÈS

Politique 9a : Toutes les décisions de contrôle concernant l'information judiciaire relèvent de la responsabilité de la magistrature.

Politique 9b : La configuration des systèmes de contrôle d'accès d'un tribunal doit appuyer le principe de l'indépendance judiciaire. Les utilisateurs judiciaires doivent disposer d'un accès exclusif à leurs propres ressources de réseau, à moins qu'il ne puisse être démontré que l'architecture, la configuration, les contrôles d'accès, le soutien opérationnel et les modèles de classification de l'information du réseau sont suffisants pour fournir le degré de confiance le plus élevé dans la séparation entre l'information judiciaire et non judiciaire, la conformité au Plan d'action et la conformité aux Lignes de conduite sur la surveillance informatique du Conseil. (« L'information judiciaire doit être protégée contre l'accès non autorisé en conformité avec le Plan d'action du Conseil canadien de la magistrature en matière de sécurité des renseignements judiciaires », Cadre de politique, Politique de sécurité 1.)

Politique 9c : Tous les utilisateurs qui accèdent à l'information judiciaire ont la responsabilité d'utiliser et de gérer leur mot de passe conformément aux politiques établies.

Politique 9d : Les systèmes contenant de l'information judiciaire « personnelle » ou « individuelle » doivent être fournis avec un environnement informatique isolé et réservé.

Politique 9e : L'information judiciaire ne peut pas être déplacée ou transmise par l'entremise d'un fournisseur commercial de services en nuage, qu'il soit public, privé ou hybride, sans l'autorisation écrite expresse de la magistrature, et dans ce cas, sous réserve des conditions d'un accord de niveau de service strictement conforme au Plan d'action.

Politique 9f : Des protocoles d'échange d'information seront négociés et établis avec les organismes gouvernementaux avant de concevoir et de mettre en œuvre des systèmes judiciaires. Ces protocoles seront élaborés en conformité avec les principes de traitement équitable de l'information (Cadre de politique, politique d'accès 8).

Politique 9g : Les cours doivent mettre en place et tenir à jour des pratiques exemplaires pour la sécurisation des réseaux locaux sans fil (WLAN) et s'assurer que les utilisateurs ne compromettent pas la sécurité de l'information judiciaire lorsqu'ils utilisent les réseaux sans fil. (« Si un point d'accès public sans fil à Internet est installé dans un palais de justice, il ne doit pas compromettre l'information judiciaire » - Cadre de politique, politique de sécurité 6).

Politique 9h : L'accès en bloc à une partie ou à l'ensemble des dossiers de la cour doit être régi par une entente écrite conclue avec la cour et portant sur les principales questions et les principaux risques (Cadre de politique, politique d'accès 5).

Commentaire : Cette politique n'affirme par que la magistrature a le pouvoir exclusif de déterminer les rôles et les niveaux d'autorisation de sécurité; l'administration judiciaire doit aussi avoir le pouvoir de déterminer le niveau d'accès approprié pour les utilisateurs, parce que le personnel des cours a une responsabilité de reddition de compte double. Selon les principes généraux énoncés au Cadre de politique, cependant, l'administration judiciaire ne peut fournir à un utilisateur un niveau d'accès plus élevé que celui accepté par la magistrature.

Les ressources comme les *Guidelines for Securing Wireless Local Area Networks (WLANs)* (NIST Special Publication 800-153), février 2012, peuvent être utiles[18]. Voir également *Cloud Computing Synopsis and Recommendations* (NIST Special Publications 800-146), mai 2012[19]. Pour une présentation abrégée, voir Steiner, *An Introduction To Securing a Cloud Environment*, juin 2012, SANS Institute[20].

10. SYSTÈMES INFORMATIQUES

Politique 10a : Les processus d'acquisition, de développent et de maintenance des systèmes d'information de la cour doivent être conçus et appliqués afin de préserver la qualité, l'intégrité et la disponibilité à long terme de l'information judiciaire et de l'information de la cour. (« Un objectif essentiel du système consiste à assurer la cohérence, l'exactitude et la rapidité de l'information judiciaire et de l'information des cours » - Cadre de politique, politique fondamentale 10.)

Politique 10b : L'application des outils d'analyse à l'information judiciaire ne doit pas se faire sans l'avis et l'approbation de la magistrature.

Politique 10c: l'information judiciaire doit faire l'objet d'une protection additionnelle au-delà des mesures de sécurité applicables à l'information de la cour (Cadre de politique, politique de sécurité 5).

Commentaire : La « protection additionnelle » peut inclure, par exemple, les politiques de chiffrement des données.

11. GESTION DES INCIDENTS

Politique 11: Les incidents touchant la sécurité de l'information doivent être signalés promptement et uniquement par la voie des canaux approuvés.

Commentaire : Toute personne ayant des motifs de croire qu'une atteinte à la sécurité menace ou est survenue doit prendre des mesures pour signaler l'incident, le signaler promptement, et le signaler à la personne ou aux personnes appropriées. Un processus de rapport d'incident comprend des mesures de sensibilisation et de formation pour tous les employés en ce qui concerne les mesures de sécurité, les signes avertisseurs d'une intrusion, et les mécanismes de signalement appropriés.

[18] http://csrc.nist.gov/publications/nistpubs/800-153/sp800-153.pdf
[19] http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf
[20] http://www.sans.org/reading_room/whitepapers/cloud/introduction-securing-cloud-environment_34052.

Chaque cour doit mettre en place un protocole pour le signalement des incidents de sécurité ayant trait aux utilisateurs judiciaires et/ou à l'information judiciaire, afin d'assurer le respect des principes de l'indépendance judiciaire.

Il faut inclure parmi les différents types d'atteintes à la sécurité la publication de dossiers de la cour faisant l'objet d'un interdit de publication ou avant leur publication approuvée par la cour.

Les *Lignes de conduite sur la surveillance informatique* (2002) du Conseil canadien de la magistrature précisent : « Toute surveillance doit être administrée par des employés qui relèvent directement du juge en chef de la cour et qui ne sont responsables que devant lui ».

12. CONTINUITÉ DES ACTIVITÉS

Politique 12 : Les cours doivent protéger l'information judiciaire en cas de catastrophe ou d'autres défaillances du système, et fournir un degré élevé d'assurance que toute perturbation du service résultant d'un tel événement sera la plus brève possible.

Commentaire : Un plan de continuité des activités (PCA) doit reposer sur l'évaluation du risque et des menaces et inclure un processus de maintenance régulière, y compris la formation, les tests et les mises à jour. Tous les plans de continuité des activités doivent respecter les protocoles de sécurité de l'information. Un plan de continuité des activités simple doit comprendre les éléments suivants[21] :

1. gouvernance;
2. analyse des effets sur les activités;
3. plans, mesures et arrangements pour la continuité des activités;
4. procédures de préparation;
5. techniques d'assurance de qualité (exercices, entretien et vérification).

13. CONFORMITÉ

Politique 13a : L'ensemble des politiques, des procédures et des pratiques d'information judiciaire doit être conforme aux lois et aux règlements applicables et aux exigences contractuelles valides.

Politique 13b : Toutes les opérations de la cour doivent être menées conformément aux politiques applicables de sécurité de l'information, y compris le Plan d'action.

Politique 13c : L'accès aux outils de conformité et leur utilisation doivent être limités à un petit nombre de personnes autorisées seulement.

Politique 13d : Les listes de contrôle doivent être surveillées de près afin de pouvoir identifier facilement les utilisateurs qui ont accès à l'information judiciaire à n'importe quel moment (Cadre de politique, politique de sécurité 3).

[21] Voir le Guide de planification de la continuité des activités, Sécurité publique Canada, http://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/bsnss-cntnt-plnnng/index-fra.aspx

Politique 13e : La conformité aux politiques précédentes doit faire l'objet d'une vérification indépendante sur une base régulière, en fonction de l'évaluation des menaces et des risques. Lorsque les vérifications portent sur l'information judiciaire et les utilisateurs judiciaires, elles doivent être faites conformément aux Lignes de conduite sur la surveillance du Conseil.

PRINCIPALES RÉFÉRENCES

- ISO/IEC 27002:2005
- Publications spéciales du NIST, dont 800-53 (Recommended Security Controls for Federal Information Systems) et 800-39, (Managing Risk from Information Systems)
- Improving the Management of Information Security in Canadian Government Departments, par Ken Fogalin, 2009
- Information Security Guide: Effective Practices and Solutions for Higher Education, publié par le Higher Education Information Security Council.
- Salle de lecture sur la sécurité de l'information de SANS : http://www.sans.org/reading_room/

ANNEXE 1

RECOMMANDATIONS DU CCT APPROUVÉES PAR LE CONSEIL LE 30 NOVEMBRE 2001

1. Que le Conseil canadien de la magistrature tienne un séminaire à sa prochaine réunion semestrielle sur les questions urgentes de sécurité mises au jour dans le présent rapport (Sécurité technologique dans les cours : rapport du Comité consultatif sur l'utilisation des nouvelles technologies par les juges).

2. Que le président du Conseil canadien de la magistrature transmette le présent rapport au Conseil canadien des juges en chef.

3. Que le président du Conseil canadien de la magistrature transmette le présent rapport aux sous-procureurs généraux et leur demande de collaborer à la mise en œuvre des recommandations.

4. Que le Conseil canadien de la magistrature demande à l'Institut national de la magistrature et au Bureau du commissaire à la magistrature fédérale de coordonner la formation (sur les questions de sécurité du système d'information, y compris les préoccupations relatives à l'indépendance de la fonction judiciaire et à l'intégrité de l'information judiciaire) à l'intention des juges fédéraux et provinciaux ainsi que du personnel des technologies de l'information.

5. Que le Conseil canadien de la magistrature demande à tous les juges en chef de nomination fédérale ou provinciale :

   a) de faire la priorité à la sécurité du système d'information des cours;

   b) de veiller à l'élaboration immédiate d'une politique de sécurité, avant que la conversion à un système électronique ne survienne;

   c) d'identifier et d'obtenir les ressources financières requises, de personnel et autres ressources essentielles à la mise en œuvre des mesures de sécurité appropriées;

   d) de faire en sorte qu'un membre du personnel en technologies de l'information relevant du juge en chef soit nommé à la gestion de la sécurité informatique des cours.

6. Pour des besoins d'uniformité, que le Conseil canadien de la magistrature assume un rôle de direction en autorisant le Comité consultatif sur la technologie à élaborer un document provisoire englobant toutes les mesures de sécurité recommandées pour toutes les cours canadiennes et fasse en sorte que le Comité dispose des ressources nécessaires à cette fin.

ANNEXE 2

GLOSSAIRE DE TERMES OU D'ACRONYMES DÉFINIS

Terme ou acronyme	Sens
Analytique	« L'application de l'informatique, de la recherche opérationnelle et de la statistique à la résolution de problèmes ». Voir http://fr.wikipedia.org/wiki/Analytique_(recherche).
Anonymisation	Le processus par lequel les renseignements personnels sont retirés des ensembles de données.
Apps	Applications logicielles téléchargées pour utilisation sur des appareils mobiles.
Chiffrement	Transformation d'un texte lisible par l'utilisateur en code illisible afin de protéger l'information de l'accès non autorisé.
Code malveillant	Programmes ou code conçu pour effacer des données, empêcher l'accès ou autrement nuire au bon fonctionnement d'un système informatique – terme générique regroupant les virus et vers informatiques, les logiciels-espions, les chevaux de Troie, les maliciels, les attaques de déni de service, etc.
Cryptographie	La science du chiffrement.
DDoS	Déni de service distribué; type de cyberattaque évolué qui surcharge un site Web et empêche les utilisateurs d'y accéder
EMR	Évaluation des menaces et des risques.
ENS	Entente de niveau de service. L'ENS cristallise la compréhension des parties sur les services, les priorités, les responsabilités et les garanties. Chaque partie de la portée des services doit faire l'objet d'un « niveau de service » précis. L'ENS peut préciser le degré de disponibilité, la serviabilité, le rendement, l'exploitation ou autres attributs du service, comme la facturation. Traduit de Wikipedia, http://en.wikipedia.org/wiki/Service-level_agreement.
FAI	Fournisseur d'accès Internet - organisme qui fournit l'accès à l'Internet
FSN	Fournisseur de services en nuage
IDS	Système de détection d'intrusion – système qui surveille les tentatives d'accès non autorisées à un réseau.
Intrusion	L'intrusion est définie comme une tentative visant à compromettre la sécurité d'un ordinateur ou d'un réseau. La détection d'intrusion est le processus qui consiste à surveiller les évènements qui surviennent dans le système informatique ou dans le réseau et à les analyser pour détecter des signes d'intrusions.
Mégadonnées	Définition courante : un volume de données tel qu'il est impossible de les traiter sans outils logiciels spécialisés. On trouvera une bonne explication ici : http://www-01.ibm.com/software/data/bigdata/.
Microblogage	Publication en temps réel de messages courts sur le Web, comme les gazouillis (sur Twitter) ou les mises à jour de statut (sur Facebook) ou tout autre média social.

Nuage (voir aussi Nuage hybride et Nuage privé)	« L'informatique en nuage est un modèle permettant un accès systématique, commode et à la demande à un bassin partagé de ressources informatiques configurables (p. ex. réseaux, serveurs, stockage, applications et services) pouvant être fournies et libérées rapidement avec un minimum d'effort de gestion et d'interaction avec le fournisseur de service. » Traduit de NIST, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
Nuage hybride (voir aussi Nuage et Nuage privé)	Un nuage hybride se compose d'au moins un nuage privé et d'au moins un nuage public. Un nuage hybride est généralement offert de deux façons : un fournisseur possède un nuage privé et forme un partenariat avec un fournisseur de nuage public, ou un fournisseur de nuage public forme un partenariat avec un fournisseur qui offre des plateformes de nuage privé. http://searchcloudcomputing.techtarget.com/definition/hybrid-cloud
Nuage privé (voir aussi Nuage et Nuage hybride)	« Expression utilisée pour décrire une plateforme d'informatique en nuage mise en œuvre à l'intérieur du pare-feu d'une entreprise, sous le contrôle du service des TI. » Traduit de *What is Private Cloud?* Webopedia, http://www.webopedia.com/TERM/P/private_cloud.html
Pare-feu	Un produit matériel ou un logiciel programmé pour filtrer les intrusions non désirées d'un ordinateur ou d'un réseau à un autre.
PAP	Abréviation de l'expression « Prenez vos appareils personnels », une politique qui permet aux employés d'accéder aux réseaux d'affaires à partir d'appareils mobiles qui sont leur propriété personnelle.
RL	Réseau local - système qui relie des utilisateurs à des ressources informatiques partagées à l'intérieur d'un immeuble.
RL sans fil	Réseau local qui fonctionne par radiofréquence au lieu d'être branché au moyen de câbles.
Sécurité informatique	Sécurité des technologies de l'information
Sécurité matérielle	La sécurité matérielle s'entend de la protection des immeubles et de l'équipement (ainsi que des renseignements et logiciels qui s'y trouvent) des introductions par effraction, vols, actes de vandalisme, catastrophes naturelles et autres et dommages accidentels.
Services partagés	L'expression services partagés renvoie à la prestation de services par un groupe au sein de l'organisme, lorsque ces services étaient auparavant assurés par plus d'un groupe au sein de l'organisation. Le financement et le ressourcement des services sont partagés et le groupe qui les fournit devient à toutes fins utiles un fournisseur de services interne. Traduit de Wikipedia, http://en.wikipedia.org/wiki/Shared_services.
Téléphone intelligent	Un téléphone cellulaire muni d'un écran et d'un clavier et d'une puissance informatique suffisante pour faire tourner différentes applications, dont un fureteur Web.
TI	Technologie de l'information
Virtualisation	« La virtualisation consiste à faire fonctionner un ou plusieurs systèmes d'exploitation ou applications comme un simple logiciel, sur un ou plusieurs ordinateurs, serveurs ou système d'exploitation, au lieu de ne pouvoir en installer qu'un seul par machine. Grâce à la virtualisation, une entreprise peut gérer plus facilement les mises à jour et les modifications du système d'exploitation et des applications sans nuire à l'utilisateur. » Traduit

	de http://en.wikipedia.org/wiki/Virtualization
WiFi	Utilisé de façon interchangeable avec RL sans fil, bien que techniquement il s'agisse d'un RL sans fil configuré selon une norme particulière.

ANNEXE 3

EXEMPLE DE POLITIQUE DE SÉCURITÉ DES APPAREILS MOBILES DE SOPHOS

Traduit sans modifications depuis http://www.sophos.com/en-us/medialibrary/PDFs/other/Example%20Mobile%20Device%20Security%20Policy.docx.

Exemple de politique de sécurité des appareils mobiles

Utilisation de la politique

L'un des défis auxquels sont confrontés les services de TI aujourd'hui porte sur la sécurisation des appareils mobiles appartenant aux individus et à l'organisme, comme les téléphones intelligents et les tablettes informatiques. Cet exemple de politique vise à service de guide pour les organismes qui souhaitent mettre à jour leur politique de sécurité des appareils mobiles ou en adopter une.

N'hésitez pas à l'adapter à votre organisme. Au besoin, modifiez, retirez ou ajoutez des éléments en fonction de vos besoins et de votre attitude à l'égard du risque. Il ne s'agit pas d'une politique complète, mais d'un modèle pragmatique destiné à servir de base pour l'élaboration de votre propre politique.

Contexte de la politique

Le principal défi vient du fait que les utilisateurs ne reconnaissent pas que les appareils mobiles représentent une menace pour la sécurité des TI et des données. Pour cette raison, ils n'appliquent souvent pas les mêmes lignes directrices en matière de sécurité et de protection des données qu'ils appliquent sur d'autres appareils, comme les ordinateurs personnels.

Le second défi vient du fait que les utilisateurs, lorsqu'ils fournissent leur propre appareil, sont souvent plus portés à donner plus de poids à leurs droits sur l'appareil qu'au besoin de l'employeur de protéger les données

Ce modèle de politique fournit un cadre pour la sécurisation des appareils mobiles et devrait être rattaché aux autres politiques qui appuient la position de votre organisme en matière de sécurité des TI et des données.

Exemple de politique

1. Introduction

Les appareils mobiles, comme les téléphones intelligents et les tablettes informatiques, sont des outils importants pour leur organisation et leur utilisation est appuyée pour atteindre les objectifs de l'organisation.

Cependant, les appareils mobiles représentent aussi un risque important pour la sécurité de l'information et des données puisqu'ils peuvent constituer une voie d'accès non autorisé à l'infrastructure de données et de TI de l'organisme si les applications et les procédures de sécurité ne sont pas appliquées. Ceci peut ensuite conduire à des pertes de données et à une infection du système.

<Nom de l'organisme> doit protéger ses actifs d'information afin de protéger ses clients, ses propriétés intellectuelles et sa réputation. Ce document donne les grandes lignes d'un ensemble de pratiques et d'exigences pour l'utilisation sécuritaire des appareils mobiles.

2. Portée

1. Tous les appareils mobiles, qu'ils soient la propriété de <Nom de l'organisme> ou de ses employés, qui ont accès aux réseaux, aux données et aux systèmes de l'organisation, à l'exclusion des ordinateurs mobiles gérés par les services de TI de l'organisme. Ceci comprend les téléphones intelligents et les tablettes informatiques.

2. Exemptions : lorsqu'il existe un motif opérationnel d'exclure un appareil de l'application de la politique (trop coûteux, trop complexe, répercussions négatives sur les autres exigences opérationnelles), une évaluation des risques doit être effectuée avec l'autorisation de la direction de la sécurité.

3. Politique

3.1 Exigences techniques

1. Les appareils doivent utiliser l'un des systèmes d'exploitation suivants : Android 2.2 ou plus récent, IOS 4.x ou plus récent. <ajouter ou retirer au besoin>
2. Les appareils doivent conserver tous les mots de passe sauvegardés par l'utilisateur dans un répertoire chiffré.
3. Les appareils doivent être configurés avec un mot de passe sûr, conforme à la politique sur les mots de passe de <Nom de l'organisme>. Ce mot de passe ne doit pas reprendre tout autre authentifiant utilisé au sein de l'organisme.
4. À l'exception des appareils sous la gestion des TI, aucun appareil ne peut être branché directement au réseau interne de l'organisme.

3.2 Exigences relatives aux utilisateurs

1. Les utilisateurs ne doivent charger dans leurs appareils mobiles que les données essentielles à l'exécution de leurs fonctions.
2. Les utilisateurs doivent signaler sans délai le vol ou la perte de leurs appareils mobiles aux services de TI de <Nom de l'organisme>.
3. Si un utilisateur a des raisons de croire qu'un accès non autorisé aux données de l'organisation a pu avoir lieu à partir d'un appareil mobile, l'utilisateur doit signaler l'incident conformément au processus de signalement des incidents de <Nom de l'organisme>.
4. Les appareils ne doivent pas être « déverrouillés » et on ne doit pas y installer de logiciel ou de micrologiciels conçus pour donner accès à des fonctionnalités qui ne sont pas destinées à être portées à la connaissance de l'utilisateur.
5. Les utilisateurs ne doivent pas installer de logiciels piratés ou de contenu illégal dans leurs appareils.
6. Les applications ne doivent être installées qu'à partir de sources officiellement approuvées par le propriétaire de la plateforme. L'installation de code provenant de sources non sécurisées est interdite. Si vous n'êtes pas certain que l'application provient d'une source approuvée, veuillez communiquer avec les TI de <Nom de l'organisme>.
7. Les appareils doivent être tenus à jour avec les rustines fournies par le fabricant ou le réseau. Au minimum, l'utilisateur doit vérifier l'émission de rustine au moins toutes les semaines et appliquées une fois par mois.
8. Les appareils ne doivent pas être branchés à un ordinateur qui n'est pas doté d'une protection anti-maliciel à jour et conforme à la politique de l'organisme.
9. Les appareils doivent être chiffrés selon les normes de conformité de <Nom de l'organisme>.
10. Les utilisateurs doivent faire preuve de prudence s'ils utilisent des comptes personnels et d'affaires sur leurs appareils. Ils doivent tout particulièrement veiller à ce que les données de l'organisme ne soient transmises que par l'entremise du système de courriel de l'organisme. Si un utilisateur soupçonne que des données de l'organisation ont pu être transmises via un compte de courriel personnel, dans le texte ou en pièce jointe, il doit en aviser immédiatement les TI de <Nom de l'organisme>.
11. (Si applicable à votre organisation) Les utilisateurs ne doivent pas utiliser les postes de travail de l'organisme pour sauvegarder ou synchroniser du contenu comme des fichiers médias, à moins que ce contenu ne soit requis pour des motifs professionnels légitimes.

*Le déverrouillage d'un appareil signifie en retirer les limites imposées par le fabricant. Ceci donne accès au système d'exploitation, ce qui en déverrouille toutes les caractéristiques et permet l'installation de logiciels non autorisés.

ANNEXE 4

APERÇU DES TERMES UTILISÉS DANS LES ENS SUR L'INFORMATION JUDICIAIRE

TERME (avec renvoi à la politique du Plan d'action)	SUJET
Relations entre les parties	Aucun partenariat Aucune cession ou sous-traitance sans le consentement de la magistrature En cas de sous-traitance, toutes les dispositions de l'ENS doivent être reprises dans le sous-contrat Aucun conflit d'intérêts n'est autorisé
Provision	Accord ou entente générale sur la prestation de services Exploitation du système Accès au système et aux données Norme générale de service
Indépendance judiciaire (Politique 1)	Le cadre de politique, le plan d'action et les lignes directrices sur la vérification ont préséance sur les dispositions incompatibles de toute autre norme de sécurité des TI applicable
Propriété (Politique 5)	Propriété des données Restrictions d'accès et d'utilisation Les données ne doivent être conservées et transportées que dans des lieux approuvés Les données doivent rester au Canada, sauf entente à l'effet contraire Isolement des données y compris la sauvegarde
Gouvernance (Politique 3)	Comité mixte de politique et de gestion Signalement des incidents Avis d'accès légal Exigences de rapport Conformité et vérification Règlement des différends
Niveaux de service	Portée Rôles et responsabilités Heures de service Disponibilité et maintenance Soutien des utilisateurs finaux
Sécurité	Conformité aux politiques de sécurité (Politique 2) Gestion de l'actif (Politique 5) Ressources humaines (Politique 6) Sécurité matérielle (Politique 7) Sécurité des communications et de l'exploitation (Politique 8) Contrôle de l'accès (Politique 9)

TERME (avec renvoi à la politique du Plan d'action)	SUJET
	Systèmes informatiques (Politique 10) Gestion des incidents (Politique 11) Continuité des activités (Politique 12) Conformité (Politique 13)