LA STÉGANOGRAPHIE AU QUÉBEC : LUMIÈRE TECHNIQUE, OMBRES JURIDIQUES

Antoine GUILMAIN[1]

Lex Electronica, vol. 17.2 (Automne/Fall 2012)

Sommaire

[1] Candidat à la maîtrise en Droit des affaires sous la direction de Vincent Gautrais, Faculté de Droit, Université de Montréal.

Introduction

> « *Les secrets les mieux gardés sont ceux qui sont devant notre nez et que nous sommes incapables de voir* » – Leonard de Vinci.

Si l'information est l'oxygène des temps modernes, les nouvelles technologies semblent avoir inexorablement accéléré le passage du monde anaérobie à celui aérobie. L'information est devenue une source de richesse et de pouvoir[2], car en disposer permet de mieux comprendre une situation et donc de prendre de meilleures décisions[3]. C'est particulièrement vrai dans le monde des affaires où, statistiquement, 80 % des actifs d'une entreprise prendraient désormais la forme de données informatiques[4]. Néanmoins, les entreprises le savent mieux que quiconque, cette inflation informationnelle s'accompagne d'un essor exponentiel de défis en matière de responsabilité : c'est là le revers de la médaille[5].

À la lumière de ce constat, donner une protection adéquate à l'information devient un enjeu primordial pour tous les acteurs économiques (entreprises, gouvernements, mais aussi les utilisateurs/consommateurs) et, bien entendu, pour les concepteurs de systèmes d'information. Avec toutes les nuances que suscite une telle affirmation, on peut dire que la protection de l'information se décline en deux axes principaux[6] : d'une part, la sûreté de l'information, qui consiste à protéger la donnée contre les perturbations ne provenant pas d'actes de malveillance (dégradations, pannes, etc.), d'autre part, la sécurité de l'information, qui consiste à protéger la

---

[2] Nicolas W. Vermeys, *Qualification et quantification de l'obligation de sécurité informationnelle dans la détermination de la faute civile*, thèse de doctorat en droit, Faculté de droit de l'Université de Montréal, 2009, p. 4.

[3] Theodore Roszak, *The Cult of Information, The Folklore of Computers and the True Art of Thinking*, New York, Phanteon Books, 1986.

[4] Kimberly Kiefer et al., *Information Security: A Legal, Business and Technical Handbook*, Chicago, ABA Publishing, 2004, p. 41.

[5] Comme le résument fort bien Stewart Personick et Cynthia Patterson, "*a corporation might be deemed to have an existing legal duty to protect the information of its customers or clients*" dans : Stewart D. Personick et Cynthia A. Patterson, *Critical Information Infrastructure Protection and the Law : An overview of Key Issues*, Washington, The National Academies Press, 2003, p. 46.

[6] Bruce Schneier, *Beyond Fear*, New York, Copernicus Books, 2003, p. 12 ; Bruno Doucende, *Sécurité des Systèmes d'Information*, Livre blanc du groupe, 2004, p. 19. Disponible à : <http://www.synertic.fr/sites/default/files/pdf/Livre_Blanc_SSI_v1-4c_0.pdf> (date de visite : 23 février 2012).

donnée contre les actes de malveillance et qui peut se définir comme étant la « *protection des ressources informationnelles d'une organisation, face à des risques définis, qui résulte d'un ensemble de mesures de sécurité prises pour assurer la confidentialité, l'intégrité et la disponibilité*[7] *de l'information traitée*[8] ». À cet égard, précisons que la sécurité informationnelle, objet principal du présent travail, ne devrait pas être confondue avec celle informatique. En effet, alors que la première s'attache davantage au contenu (c.-à-d. l'information), la seconde s'intéresse au contenant (c.-à-d. le support)[9] et aux traitements apportés au contenu.

Pour assurer la sécurité d'une information, une possibilité est de la rendre « secrète », c'est-à-dire difficilement accessible ou intelligible (par des moyens matériels, des mesures administratives ou techniques[10]), sauf pour la personne à laquelle elle est destinée : c'est là le domaine de la cryptographie. Mais Leonard de Vinci, qui s'y connaissait en matière de dissimulation, nous expliquerait volontiers que le meilleur moyen de protéger une information, c'est de la dissimuler, en faisant en sorte que personne – mis à part le destinataire – n'ait l'idée même de la chercher, n'imaginant pas qu'il peut y avoir, à un endroit donné, un « trésor » intéressant. On est là dans le domaine de la stéganographie, qui consiste à dissimuler (recouvrir) une information pour la faire passer inaperçue.

De manière imagée, on peut dire que mettre son argent dans un coffre-fort reviendrait à la première méthode, tandis que l'enterrer correspondrait à la seconde. Selon le proverbe chinois « *A chaque coffre sa clé, on les ouvrira tous* », et si l'on admet, comme Michel Tournier, que « *Coffre-fort fragile et provoquant, la vitrine appelle l'effraction*[11] », le bon sens conduirait plutôt à privilégier la seconde méthode : si personne ne sait qu'il y a un message caché, personne ne cherchera à le regarder ou à le récupérer[12].

---

[7] La disponibilité, l'intégrité et la confidentialité forment la « triade DIC » (*AIC Triad* en anglais), qui est au cœur de la notion de sécurité informationnelle. L'article 26 de la *Loi concernant le cadre juridique des technologies de l'information* reprend d'ailleurs ce principe en substance.

[8] Office de la langue française, « Le grand dictionnaire terminologique », disponible sur le site : <http://www.granddictionnaire.com> (date de visite : 22 février 2012).

[9] N. W. Vermeys, préc., note 1, p. 5.

[10] Article 4.7.3 du *Code type sur la protection des renseignements personnels*, CAN/CSA-Q830-96, annexe A à la *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, ch. 5.

[11] Michel Tournier, *La goutte d'or*, Paris, NRF Gallimard, 1985.

[12] A. Ali-Pacha, N. Hadj-Said, A. Belgoraf et A. M'Hamed, « Stéganographie : sécurité par dissimulation », *Revue d'Information Scientifique et Technique*, vol. 16 nº 1, 2006, p. 102, disponible à <http://www.webreview.dz/IMG/pdf/7-Ali-pacha-rist06.pdf> (date de visite : 27 février 2012).

Il y a encore mieux : coupler cryptographie et stéganographie ! Car, en supposant que, par hasard, quelqu'un de non autorisé arrive à détecter la présence du trésor, cela ne veut pas dire pour autant qu'il parviendra à l'extraire ; et si celui-ci est de surcroît bien verrouillé, il sera encore plus difficile d'accéder à l'or…

Ceci étant dit, tentons maintenant d'accorder les mots et les choses : l'art du secret se réfère à la cryptographie, tandis que la stéganographie, qui fait ici l'objet de toute notre attention, s'attache plutôt à l'art de la dissimulation. Poser des définitions claires est une étape essentielle pour une bonne compréhension du sujet, aussi circonscrirons-nous la notion de stéganographie à une « *technique qui consiste à dissimuler un message, que l'on désire transmettre confidentiellement, dans un ensemble de données d'apparence anodine, de façon que sa présence soit imperceptible*[13] ».

La stéganographie reste encore une technique assez peu connue du grand public : pour preuve, très peu de dictionnaires lui accordent aujourd'hui une entrée[14]. L'étymologie grecque du terme vient de « *stegein* », qui veut dire « couvert/recouvert[15] » et de « *graphia* », l'écriture. Il ne faut pas la confondre avec la « stéganographie », dont l'origine étymologique est différente : « *stenos* » voulant dire « étroit », d'où une écriture étroite, resserrée. Certains n'hésitent pas à dire que la stéganographie évolue dans l'ombre de la cryptographie (« *kryptein* » veut dire « cacher »), les « codes secrets » ayant toujours suscité l'imagination et la curiosité du public[16].

Aujourd'hui, ce n'est plus tout à fait vrai : la stéganographie moderne, c'est-à-dire adaptée à un environnement numérique, offre des possibilités si impressionnantes qu'on peut considérer qu'elle a acquis son autonomie par rapport à la cryptographie, mais son utilisation reste relativement jeune, et elle est mal couverte sur le plan juridique.

---

[13] Office de la langue française, « Le grand dictionnaire terminologique », disponible sur le site : <http://www.granddictionnaire.com> (date de visite : 22 février 2012).
[14] A. Ali-Pacha, N. Hadj-Said, A. Belgoraf et A. M'Hamed, préc., note 11, p. 103.
[15] Ainsi, un « stégosaure » est un saurien qui est recouvert d'une carapace (comme aujourd'hui la tortue).
[16] Johann Barbier, *La stéganographie Moderne : d'Hérodote à nos Jours*, disponible à : <http://www.novetix.fr/homepages/barbier/partage/articles/barbier07herodote.pdf> (date de visite : 27 février 2012).

En droit québécois, l'obligation d'assurer la sécurité d'informations confidentielles découle principalement de quatre dispositions législatives provinciales[17] et d'une fédérale[18]. Or, comme le résume fort bien le Professeur Vermeys, « *si la nature de ces obligations est claire, les moyens devant être employés pour les respecter laissent place à interprétation*[19] ». Alors même que bien des juristes reconnaissent la nébulosité de l'obligation de sécurité informationnelle, c'est aux entreprises et à leur responsable de la sécurité de l'information[20] (dénommé ci-après le RSI) de découvrir ce que constituent une « *mesure propre à assurer la confidentialité*[21] », un « *moyen approprié au mode de transmission*[22] », une « *mesure propre à assurer la confidentialité des renseignements personnels […] et qui soient raisonnables*[23] », et de les différencier.

Face à un corpus législatif aussi dense que confus[24], nous tenterons de voir si la stéganographie peut être considérée comme une mesure de protection que pourrait/devrait adopter un RSI raisonnablement prudent et diligent[25]. En d'autres termes, dans quelles conditions un RSI utilisant une technique stéganographique se trouverait-il dans une situation plus confortable, en cas de poursuite en responsabilité civile pour manquement à l'obligation de sécurité informationnelle[26] ?

Dans un premier temps, nous tenterons de faire la lumière sur la notion même de stéganographie informatique (I). Dans un second temps, nous nous placerons sur le plan juridique et essaierons de dégager les enjeux d'une utilisation d'outils de stéganographie, notamment vis-à-vis de l'obligation de sécurité informationnelle (II).

---

[17] L'article 10 de la *Loi sur la protection des renseignements personnels dans le secteur privé* (L.R.Q., c. P-39.1), l'article 25 et 34 de la *Loi concernant le cadre juridique des technologies de l'information* (L.R.Q., c. C-1.1) et l'article 1457 du *Code civil du Québec* (L.Q. 1991, c. 64).

[18] Précité, note 9. L'article 5 de la *Loi sur la protection des renseignements personnels et les documents électroniques* donne un caractère contraignant à l'article 4.7.3 du *Code type sur la protection des renseignements personnels*.

[19] N. W. Vermeys, préc., note 1, p. 24.

[20] Conformément aux exigences de l'article 4.1 des Principes énoncés dans la norme nationale du Canada intitulée *Code type sur la protection des renseignements personnels*, CAN/CSA-Q830-96, annexe A à la *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, ch. 5, le responsable de la sécurité de l'information (*Chief Information Security Officer* en anglais) assure la protection de l'information au sein d'une entreprise donnée.

[21] *Loi concernant le cadre juridique des technologies de l'information*, préc., note 15, art. 25.

[22] *Ib.*, art. 34.

[23] *Loi sur la protection des renseignements personnels dans le secteur privé*, préc., note 15, art. 10.

[24] N. W. Vermeys, préc., note 1, p. 19.

[25] Nicolas W. Vermeys, *Responsabilité civile et sécurité informationnelle*, Montréal, Éditions Yvon Blais, 2010, p. 118-138.

[26] *Ib.*, p. 148.

I. L'obscurité au service de la sécurité : aspects techniques et pratiques de la stéganographie

Historiquement, Hérodote est un des premiers à avoir relaté les premiers emplois de la stéganographie lors de la Seconde Guerre médique. Dans son œuvre l'*Enquête*, l'historien grec introduit ainsi deux techniques de dissimulation de l'information qui auraient permis de donner l'avantage aux Grecs sur les Perses. En premier lieu, Démarate, ancien Roi de Spartes réfugié auprès de Xerxès, ayant appris l'existence d'une future offensive décide de transmettre l'information à sa Cité et, pour ce faire, « *prit une tablette double, en gratta la cire, puis écrivit sur le bois même les projets de Xerxès ; ensuite il recouvrit de cire son message : ainsi, le porteur d'une tablette vierge ne risquait pas d'ennuis* » (Livre VII, 239). En second lieu, pour inciter son gendre Aristagoras à se révolter contre son Roi, Darius, Histiée « *fit raser la tête de son esclave le plus fidèle, lui tatoua son message sur le crâne et attendit que les cheveux eussent repoussé ; quand la chevelure fut redevenue normale, il fit partir l'esclave pour Milet* » (Livre V, 35). Un peu plus tard, le jus de citron ou l'encre sympathique a par exemple permis d'écrire de manière invisible sur du papier : une exposition du papier de couverture devant une flamme révélait le message dissimulé.

Tous ces exemples de stéganographie « classique » reposent sur l'idée de sécurité par obscurité : si personne ne sait qu'il y a un message secret, personne ne cherchera à le regarder ou le récupérer. La stéganographie moderne ne déroge pas à ce principe et lui donne même une nouvelle dimension : en effet, avec le développement d'Internet et l'inflation informationnelle que l'on connaît, rares sont les personnes qui peuvent aujourd'hui prétendre avoir suffisamment de ressources informatiques pour vérifier/contrôler la totalité des flux. Chaque message secret s'apparente alors à une goutte d'eau dans un océan informationnel et devient, de fait, d'autant plus facilement dissimulable.

Dans la présente partie, nous tenterons de faire la lumière sur la stéganographie à l'heure du numérique. Après avoir présenté ses principes et fondements théoriques, nous la mettrons en perspective avec d'autres pratiques voisines, telles le tatouage ou l'empreinte digitale (1). L'exemple valant bien souvent les meilleures explications, nous illustrerons ensuite la

stéganographie appliquée à divers types de données numériques multimédia, à savoir une image et un texte (2).

1. La dissimulation d'information à l'heure du numérique

Le terme « dissimulation d'information[27] » est très général : il désigne le simple fait de cacher une information dans un support[28]. Avec les progrès que l'on connaît en matière informatique, ce domaine prend aujourd'hui une nouvelle ampleur.

Dans cette partie, nous tenterons de déterminer ce que recouvre la stéganographie (approche positive) et ce qu'elle exclut (approche négative). Une telle démarche nous conduira : d'une part, à faire la lumière sur la notion même de stéganographie informatique, qui, comme nous l'avons vu, se rattache directement à la dissimulation d'information, en présentant ses principes et fondements théoriques (A) ; d'autre part, à la mettre en perspective avec d'autres méthodes d'insertion de données cachées (le tatouage et l'empreinte digitale) qui, quoique présentant certains points communs, ne visent plus les mêmes fins (B).

A. La stéganographie informatique : principes et fondements théoriques

La stéganographie moderne doit beaucoup au modèle conceptuel du « problème du prisonnier » introduit en 1983 par Gustavus Simmons[29]. Le contexte est le suivant : incarcérés dans deux cellules séparées d'une prison de haute sécurité, Marine et Alexandre doivent communiquer par messages surveillés, c'est-à-dire que le message doit passer nécessairement par un gardien, afin d'élaborer un plan d'évasion. Marine et Alexandre doivent alors mettre en place un canal dit subliminal afin de dissimuler l'information qu'ils échangent dans un support qui n'éveille pas les soupçons du gardien. Si les schémas classiques de cryptographie ne permettent pas un tel canal, la stéganographie le permet : en effet, alors que dans le premier cas, l'échange de messages chiffrés suscitera la méfiance du gardien qui mettra fin à la communication entre les

[27] *Information hiding* en anglais.
[28] Frédéric Saint-Marcel, *Stéganographie VS tatouage*, Rapport pour l'étude d'approfondissement, disponible à : <http://membres-liglab.imag.fr/donsez/ujf/easrr0203/tatouagestegano/tatouagestegano.pdf> (date de visite : 28 février 2012).
[29] Gustavus J. Simmons, *The prisoner's problem and the subliminal channel*, Plenum Press, 1983.

deux détenus et les contraindra certainement à divulguer leur clé de chiffrement, dans le second cas, Marine et Alexandre dissimuleront l'information compromettante dans un « message innocent » qui n'éveillera pas les soupçons du gardien. Comme le souligne Fabien Galand, « *l'approche choisie peut dépendre du contexte dans lequel a lieu la communication : le recours au chiffrement peut être interdit ou bien les deux protagonistes peuvent vouloir dissimuler jusqu'à l'existence même de l'échange de messages confidentiels*[30] ».

De ce modèle conceptuel, en apparence fort simple, se dégagent en réalité deux procédés distincts en matière de sécurisation de l'information[31] :

- D'une part, la sécurisation de la communication (COMSEC[32]). L'information est transmise, mais elle est incompréhensible : il s'agit là du domaine de prédilection de la cryptographie. Dans ce cas de figure, le potentiel attaquant saura qu'une information est communiquée – ce qui représente déjà souvent en soi une information importante –, mais elle lui sera illisible *prima facie* : il sait qu'il ne sait pas !
- D'autre part, la sécurisation des transmissions (TRANSEC[33]). L'information et la transmission de celle-ci sont dissimulées : il s'agit là d'un domaine dans lequel la stéganographie a une place. En l'occurrence, le potentiel attaquant, ne sachant pas qu'une information a été communiquée, ne cherchera pas à l'intercepter : il ne sait pas qu'il ne sait pas !

Précisons à cet égard que la stéganographie pure, celle ne faisant intervenir aucune clé de chiffrement (l'information est alors transmise en clair, seul le procédé d'insertion étant secret), s'écarte de fait du fameux principe de Kerckhoffs[34] qui veut que : « *la sécurité d'un crypto-système ne doit reposer que sur le secret de la clef* »[35]. Toutefois, coupler stéganographie et

[30] Fabien Galand, *Construction de codes Zpk-Linéaires de bonne distance minimale, et schémas de dissimulation fondés sur les codes de recouvrement*, thèse de doctorat en informatique, Université de Caen, 2004, p. 111.
[31] B. Doucende, préc., note 5, p. 20.
[32] *Communication security* en anglais.
[33] *Transmission security* an anglais.
[34] Auguste Kerckhoffs, *La cryptographie militaire*, Journal des Sciences Militaires, 1883.
[35] François Merciol et Sébastien Lefèvre, *La stéganographie : une solution pour enrichir le contenu des vidéos numériques*, disponible à : <http://www.unicaen.fr/colloques/cnriut2011/papers/187.pdf> (date de visite : 28 février 2012).

cryptographie, ce qui est dans la pratique très courant[36], permet incontestablement de renforcer la sécurisation de l'information.

La stéganographie numérique est donc une technique qui permet d'insérer des messages (cryptés ou non) dans des fichiers innocents. Ces derniers sont appelés *médium de couverture* et dans lesquels seront dissimulés les informations que l'on souhaite cacher. Comme nous le verrons ci-après, il peut s'agir d'une image ou d'un texte. Une fois que les informations sont insérées, nous utilisons alors l'expression *stégo-médium*.

Dans le domaine de la dissimulation d'information, il faut trouver le juste équilibre entre :

- La capacité, c'est-à-dire la quantité d'informations que l'on peut incorporer dans un support ;
- L'imperceptibilité, c'est-à-dire les chances que le stégo-médium soit détecté « non stégo » par un attaquant ;
- La robustesse, c'est-à-dire l'aptitude de préservation des données cachées face aux modifications, volontaires ou non, du stégo-médium (compression, filtrage, etc.)

Ce compromis est traditionnellement représenté par un triangle. En stéganographie, la capacité et l'imperceptibilité[37] ont beaucoup d'importance, tandis que le tatouage[38] ou l'empreinte privilégient, comme nous le verrons, la robustesse.

Pour finir, notons que le processus complet de stéganographie repose sur deux opérations : d'une part, la dissimulation en tant que telle, qui consiste à insérer l'information à cacher dans le médium ; d'autre part, l'extraction, qui vise à la récupérer. Le terme « détection » est également utilisé lorsqu'il s'agit simplement de vérifier la présence d'une information (par l'examen d'un signal, d'une caractéristique particulière du médium, etc.) dans le stégo-médium, sans pour autant l'extraire[39].

---

[36] Comme l'explique François Cayre, « *Les deux disciplines n'ont jamais été concurrentes, mais sont plutôt complémentaires* ». François Cayre, « Cryptographie, stéganographie et tatouage : des secrets partagés », *Interstices*, 2008, disponible à : <http://interstices.info/jcms/c_32093/cryptographie-stéganographie-et-tatouage-des-secrets-partages> (date de visite : 7 mars 2012).

[37] J. Barbier, préc., note 15.

[38] Meryem Guerrouani, *Tatouage : application aux documents XML contraints*, mémoire d'informatique, Conservatoire national des arts et métiers Paris, 2005, p. 7.

[39] A. Ali-Pacha, N. Hadj-Said, A. Belgoraf et A. M'Hamed, préc., note 11, p. 104.

B. Mise en perspective de différentes techniques d'insertion de données cachées : la stéganographie, le tatouage et l'empreinte

Comme nous l'avons vu, si la cryptographie est l'art du secret, la stéganographie est l'art de la dissimulation : plutôt que chercher à rendre un message inintelligible, on va chercher à le faire passer inaperçu.

Mais avec les progrès que l'on connait en matière informatique, le domaine de la dissimulation d'information prend aujourd'hui une nouvelle ampleur[40]. En effet, les techniques numériques ont permis l'avènement de nouvelles méthodes d'insertion de données cachées[41] qui, quoique présentant certains points communs[42] avec la stéganographie, ne visent plus les mêmes fins. À ce stade, nous distinguerons la stéganographie du tatouage et de l'empreinte digitale[43].

Le tatouage a pour objectif principal de permettre l'identification de l'entité à l'origine du document[44], autrement dit l'ayant droit. De manière plus ou moins discrète, des données difficilement altérables sont alors insérées dans le document afin d'éviter, autant que faire se peut, copies et contrefaçons du document d'origine. Plus précisément, réussir à altérer ces données devrait aboutir à une détérioration du document[45]. Cette technique vise à prévenir les contournements de droits d'auteur en permettant de « signer » les copies et de vérifier leur intégrité, c'est-à-dire qu'elles sont rigoureusement identiques au document d'origine (et qu'elles n'ont pas été tronquées, par exemple).

Tout comme le tatouage, l'empreinte a également un but d'identification. Mais il ne s'agit plus d'identifier l'émetteur, mais plutôt le destinataire (c.-à-d. l'utilisateur final). Chaque copie du document d'origine contient alors une information différente, une empreinte propre à l'utilisateur (on parle alors d'identifiant), les rendant *de facto* uniques. En d'autres termes, l'empreinte joue un rôle de numéro de série visant, là encore, à limiter le nombre de copies[46]. À

---

[40] J. Barbier, préc., note 15.
[41] Hugo Alatrista Salas, *La stéganographie moderne : l'art de la communication secrète*, Mémoire de stage Master 2, Université Montpellier II Sciences et Techniques du Languedoc, 2010, p. 11.
[42] Pour chacune de ces techniques, on cherche à incorporer dans un document une information additionnelle sans le détériorer de manière notable. F. Galand, préc., note 29, p. 108.
[43] Nous traduisons respectivement « *watermarking* » et « *fingerprinting* » par « tatouage » et « empreinte ».
[44] F. Saint-Marcel, préc., note 27.
[45] F. Galand, préc., note 29, p. 108.
[46] *Ib.*, p. 108.

cet égard, notons que si une copie illégale était produite, l'empreinte devrait permettre de retracer la source ayant servi de base à sa construction.

En définitive, le tatouage correspond à l'insertion de marques destinées à identifier l'ayant droit d'un document (*copyright*), tandis que les empreintes ont pour objet de tracer les différentes copies autorisées d'un document (équivalent d'un numéro de série)[47]. Ainsi, à l'inverse de la stéganographie qui vise avant tout à protéger le contenu (message secret, imperceptibilité), le tatouage et l'empreinte doivent se préoccuper davantage du contenant, de la fiabilité du médium de couverture, de sa robustesse : un attaquant peut donc savoir qu'un tatouage ou qu'une empreinte est présent quelque part dans le médium de couverture, mais il ne doit pas être en mesure de le/la retirer.

Le tableau ci-dessous offre une vue d'ensemble[48], volontairement simplifiée, des trois principales techniques d'insertion de données cachées que nous venons d'évoquer :

Caractéristiques	**STÉGANOGRAPHIE** ***Steganography***	**TATOUAGE** ***Watermarking***	**EMPREINTE** ***Fingerprinting***
Données	Le message à transmettre	Une marque dépendant du support et/ou du propriétaire	Une empreinte dépendant du support et de son utilisateur
Support	Sans importance, le plus « banalisé » possible	Le document hôte dont on veut protéger les droits	Le document hôte dont on souhaite prévenir la diffusion de copie illégale
But de l'utilisateur	Cacher de l'information	Identifier l'émetteur (l'ayant droit)	Identifier le destinataire (l'utilisateur)
But de l'attaquant	Détecter les données et les extraire	Supprimer les données	Supprimer les données
Utilisation courante	Échapper à la censure	Copyrights, monitoring	Maîtrise de la diffusion

Notons qu'il existe encore bien d'autres techniques de dissimulation d'information[49], mais celles-ci ne rentreront pas dans le cadre de notre étude.

[47] Fabien Galand, *Stéganographie*, p. 2, disponible à : <http://www.spiritofhack.net/repository/stegano.pdf> (date de visite : 28 février 2012).
[48] F. Saint-Marcel, préc., note 27, p. 7 ;
[49] Thomas Berthe, Jérôme Coppens et Thibault Deregnaucourt, *Stéganographie et Watermarking*, Rapport de veille technologique Cours d'Applications Réparties, Université des sciences et technologies de Lille, p. 9.

2. Quelques applications classiques de la stéganographie

« *Le chemin est long par les préceptes et court par les exemples* », notait François des Rues dans son ouvrage *Les marguerites françaises*. Aussi, après avoir présenté les aspects techniques de la dissimulation à l'heure du numérique, nous proposons quelques illustrations de stéganographie appliquée à divers types de données numériques multimédia, en l'occurrence une image (A) et un texte (B). Nous verrons ainsi qu'en plus d'être une opération séduisante sur le plan technique, la stéganographie peut être relativement facile à mettre en œuvre.

A. Une image peut en cacher une autre

Franz Kafka, précurseur à bien des égards, relevait au début du XX^{ème} siècle : « *Le regard ne s'empare pas des images, ce sont elles qui s'emparent du regard* ». La stéganographie appliquée aux images numériques en est, aujourd'hui, une excellente preuve.

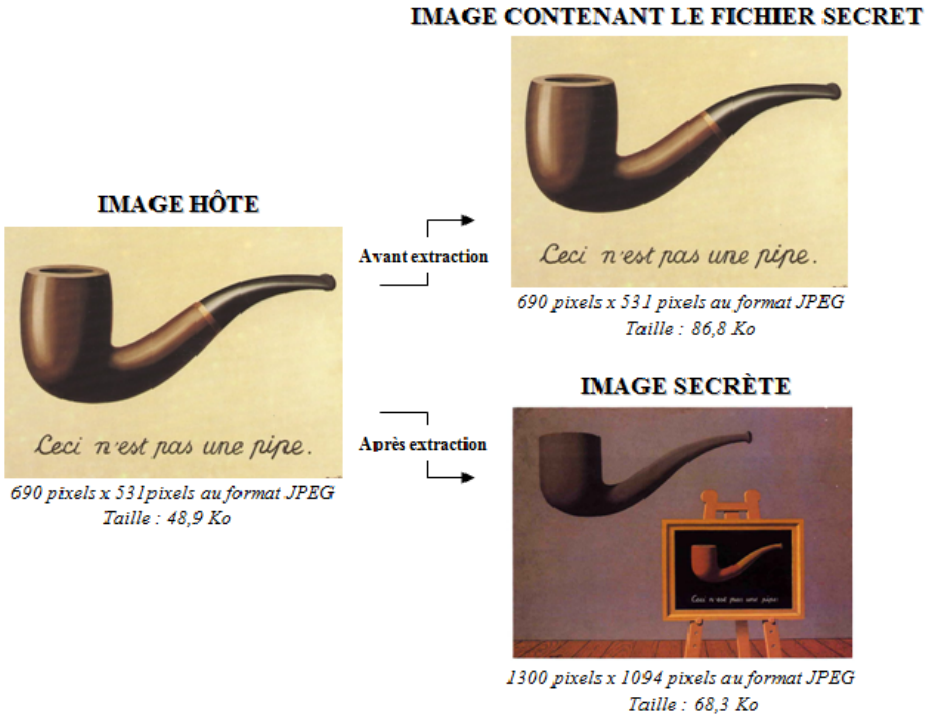
Il s'agit alors d'« encapsuler » un fichier secret dans un document hôte qui ne sera autre qu'une image. De la sorte, sans conséquence sur l'apparence (l'image pourra être visionnée sans problème), l'image contiendra en fait un message caché.

Les méthodes pour cacher un message secret dans une image numérique sont multiples[50]. Par souci de simplicité, nous nous limiterons à celle consistant à manipuler les bits de poids faibles des pixels[51]. En l'occurrence, il s'agit de « rogner » sur les bits de chaque pixel d'une image et d'y ajouter le code binaire du fichier numérique secret. Considérant qu'un pixel d'image (RVB[52]) est souvent codé sur trois octets (soit 24 bits d'information) ce qui donne 16,8 millions de couleurs, on comprend aisément qu'une telle dégradation de l'image soit indiscernable à l'œil nu[53].

---

[50] A. Ali-Pacha, N. Hadj-Said, A. Belgoraf et A. M'Hamed, préc., note 11, p. 110.
[51] F. Merciol et S. Lefèvre, préc., note 34.
[52] Abréviation de Rouge-Vert-Bleu (ou « *RGB* » de l'anglais *Red-Green-Blue*).
[53] Ken Sala relève à cet égard : « *Chaque image contient 3 600 pixels sur 2 400 pixels, et chaque pixel compte 24 bits. Je peux facilement voler six bits à chaque pixel sans altérer de façon visible les couleurs. Cela signifie donc que je peux cacher un message de plus de 50 mégabits dans chaque image. Le texte complet de la Bible compte moins de 50 mégabits* ».

De nombreux logiciels permettent aujourd'hui de coder aisément des messages à l'intérieur d'une image. L'exemple valant bien souvent les meilleures explications, nous nous sommes soumis à l'exercice.



L'image hôte et l'image secrète sont deux tableaux du peintre René Magritte, respectivement : *La Trahison des images* (1929) et *Les Deux mystères* (1966).

La dégradation de l'image passe alors inaperçue et seul le logiciel adéquat permet de retrouver les données cachées[54].

Centre de recherches sur les communications Canada, « Coup d'œil technologique », disponible à : <http://www.crc.gc.ca/fr/html/crc/home/mediazone/eye_on_tech/2009/issue10/steganography> (date de visite : 8 mars 2012).

[54] A. Ali-Pacha, N. Hadj-Said, A. Belgoraf et A. M'Hamed, préc., note 11, p. 110.

B. Dissimuler un message dans un texte

Quoique très anciennes et simples à mettre en œuvre, les techniques stéganographiques consistant à dissimuler un message dans du texte restent toujours d'actualité[55]. Ceci d'autant plus que la quantité de courriels échangés ne cesse de prendre un essor croissant.

Comme nous allons le voir, la dissimulation d'information dans du texte n'a pas grand-chose à voir avec l'image. En effet, alors que la dégradation de l'image pouvait passer inaperçue (l'œil devant de fait détecter 16,8 millions de couleurs), l'altération d'un texte sera aisément discernable : soit le texte est identique à l'original, soit il ne l'est pas[56]. Dès lors, toutes les méthodes que nous allons présenter vont avoir pour objectif de tendre vers un endommagement minimal du texte original.

Méthodes des « espaces » (en fin de phrases ou entre les mots)

S'agissant de l'utilisation de cette méthode en fin de phrase, il faut toujours se définir un code à suivre.

EXEMPLE 1

Code à suivre : 0 espace en fin de phrase correspond à 0 ; 1 espace en fin de phrase correspond à 1.

Texte contenant le message secret tel que perçu :

René Magritte ou la trahison des images … Le peintre belge Magritte (1898-1967) est une figure marquante du mouvement réaliste. Il s'est fait remarquer notamment par son art du décalage entre le titre et le sujet représenté. La trahison des images est un de ses tableaux les plus célèbres. Il représente une pipe accompagnée de la légende suivante : « ceci n'est pas une pipe ». Son intention était de montrer que, même peinte de la manière la plus réaliste qui soit, un tableau qui représente une pipe n'est pas une

[55] J. Barbier, préc., note 15.
[56] A. Ali-Pacha, N. Hadj-Said, A. Belgoraf et A. M'Hamed, préc., note 11, p. 108.

pipe. On ne peut ni la bourrer ni la fumer. De même que « le mot “chien” ne mord pas ».

Texte contenant le message secret où les espaces sont remplacés par « _ » pour davantage de lisibilité :

René Magritte ou la trahison des images_… Le peintre belge Magritte (1898-1967) est une figure marquante du mouvement réaliste. Il s’est fait remarquer notamment par son art du décalage entre le titre et le sujet représenté_. La trahison des images est un de ses tableaux les plus célèbres_. Il représente une pipe accompagnée de la légende suivante : « ceci n’est pas une pipe ». Son intention était de montrer que, même peinte de la manière la plus réaliste qui soit, un tableau qui représente une pipe n’est pas une pipe_. On ne peut ni la bourrer ni la fumer_. De même que « le mot “chien” ne mord pas ».

→ Nous avons codé dans notre message : 1 espace, 0 espace, 1 espace, 1 espace, 0 espace, 1 espace, 1 espace, 0 espace. **10110110 soit un octet de dissimulé.**

Comme vous pouvez le constater, il faut beaucoup de phrases pour coder un peu de texte (en l’occurrence, 8 phrases pour coder 1 octet) et une personne attentive aura vite fait de détecter les espaces. En revanche, cette méthode reste très simple à implémenter et il y a possibilité de la moduler à votre gré (par exemple, en rajoutant des espaces pour coder davantage de caractères sur moins de texte).

S’agissant de la méthode des espaces entre les mots, il faut là encore se définir au préalable un code à suivre.

EXEMPLE 2

Code à suivre : un espace entre 2 mots suivi de deux entre deux mots correspond à 0 ; deux espaces entre deux mots suivis d'un espace entre les deux mots suivants correspond à 1.

Texte contenant le message secret tel que perçu :

> En 1966 Magritte apporte la touche finale à son œuvre avec *Les deux mystères* représentant un chevalet sur lequel est posée *La trahison des images*, tandis qu'au-dessus est représentée une seconde pipe extérieure au tableau dans le tableau.

Texte contenant le message secret où les espaces sont remplacés par « _ » pour davantage de lisibilité :

> En_1966__Magritte__apporte_la__touche_finale_à__son_œuvre__avec__*Les_deux_mystères*__représentant__un_chevalet sur lequel est posée *La trahison des images*, tandis qu'au-dessus est représentée une seconde pipe extérieure au tableau dans le tableau.

→ Nous avons codé dans notre message : 0 (_ __), 1 (__ _), 1 (__ _), 0 (_ __) ; 0 (_ __) ; 1 (__ _) ; 0 (_ __) ; 1 (__ _), etc. **01100101 soit un octet de dissimulé.**

Méthode des synonymes

Une autre technique consiste à utiliser des dictionnaires de paires de synonymes. Un des mots de la paire codera 0 et l'autre 1.

EXEMPLE 3

Peintre de la métaphysique et du surréel, Magritte a traité les évidences avec **humour**. Il s'est glissé entre les **choses** et leur représentation, les images et les **mots**. Au lieu d'inventer des techniques, il a préféré aller au fond des choses, user de la peinture qui devient l'**instrument** d'une **connaissance** inséparable du **mystère**. « *Magritte est un **grand** peintre, Magritte n'est pas un peintre* », écrivait dès 1947 Scutenaire.

→ Dans ce texte, d'apparence innocente, est dissimulé en réalité 1 octet (01100100).

0	1
Peintre	Artiste
Gaieté	**Humour**
Objets	**Choses**
Mots	Termes
Instrument	Outil
Savoir	**Connaissance**
Mystère	Énigme
Grand	Important

Quoiqu'amusante, cette méthode n'en demeure pas moins fort difficile à implémenter, la langue ne permettant en effet pas toutes les structures de phrases.

« *Enfin, une technique plus évoluée consiste à générer automatiquement un texte qui ressemble à du langage naturel, en choisissant des mots en fonction des bits du message à dissimuler. Pour cela, le texte généré doit être grammaticalement correct et les mots utilisés doivent appartenir au même corpus pour donner un minimum de sens au texte*[57] ».

Tous ces exemples montrent bien que la stéganographie sur un support texte, contrairement à celle sur support image, supporte mal la fantaisie, chaque retouche restant directement visible par un lecteur attentif et scrupuleux.

[57] J. Barbier, préc., note 15.

II. La stéganographie à l'aune de l'obligation de sécurité informationnelle : quels enjeux juridiques ?

Comme nous avons pu le voir, la stéganographie est une opération séduisante sur le plan technique, relativement facile à mettre en œuvre aujourd'hui grâce à des outils informatiques puissants, compte tenu de l'importance des flux échangés. Néanmoins, son utilisation étant relativement jeune, la stéganographie moderne demeure aujourd'hui un procédé mal couvert sur le plan juridique.

L'objectif de la présente partie est de la présenter sous deux angles radicalement opposés. D'une part, nous nous intéresserons aux perspectives offertes par ce procédé en matière de protection de l'information. Nous tenterons en particulier de définir les conditions dans lesquelles un RSI utilisant une technique stéganographique se trouverait dans une situation plus confortable, en droit commun, puis en droit spécial, en cas de poursuite en responsabilité civile pour manquement à l'obligation de sécurité informationnelle[58] (1). D'autre part, nous aborderons le dilemme induit par la stéganographie, car il s'agit d'une mesure technique de protection pouvant à la fois influer sur la sécurité publique, mais également sur l'accessibilité et l'intégrité de l'information (2).

1. La stéganographie au service du Droit : les perspectives

Aussi bien d'un point de vue théorique que pratique, distinguer le droit commun et le droit spécial est une habitude fortement ancrée chez les juristes[59]. Sans nier les faiblesses d'une telle *summa divisio*, nous avons fait le choix d'utiliser sa vertu ordonnatrice dans la présente partie. D'une part, compte tenu de l'obligation de sécurité informationnelle découlant des dispositions de droit commun, nous montrerons que la stéganographie a une place en tant que moyen alternatif de protection de l'information pouvant être mis en œuvre par un RSI raisonnablement prudent et diligent (A). D'autre part, nous nous intéresserons plus particulièrement aux données

[58] N. W. Vermeys, préc., note 24, p. 148.
[59] Nicolas Delegove, *Le droit commun et le droit spécial*, thèse de doctorat en droit, Faculté de droit de l'Université Paris 2 Panthéon-Assas, 2011. Résumé disponible à : <http://assasrecherche.u-paris2.fr/ori-oai-search/notice.html?id=2011PA020020&printable=true> (date de visite : 6 mars 2012).

sensibles et à certaines dispositions, propres à des secteurs d'activités, influant sur l'obligation de sécurité informationnelle. Nous montrerons l'intérêt, pour des données sensibles, de cumuler une sécurisation de la communication – par cryptographie – et une sécurisation de la transmission – par exemple par stéganographie – (B).

A. En droit commun : un moyen alternatif de protection de l'information

En droit québécois, il existe une obligation générale de sécurité informationnelle. Celle-ci résulte d'un nombre limité de dispositions[60]. Dans le présent travail, nous ferons référence à l'article 25 de la *Loi concernant le cadre juridique des technologies de l'information*[61] (dénommé ci-après « *LCCJTI* »), pour au moins deux raisons : d'une part, il ne se limite pas aux principes généraux de responsabilité contenus à l'article 1457 du *Code civil du Québec*, d'autre part, à l'inverse de l'article 10 de la *Loi sur la protection des renseignements personnels dans le secteur privé*, cette disposition vise tous les renseignements confidentiels et pas seulement ceux liés à la vie privée de personnes physiques[62].

S'il est vrai que la *LCCJTI* reste *« fort nébuleuse*[63] » en matière de sécurité, certains exemples s'avèrent être pertinents pour comprendre ce que peuvent revêtir des « *mesures de sécurité propres à assurer la confidentialité de l'information* ». L'article 25 dispose ainsi :

> « *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* » [nous soulignons].

Loin de dresser une liste limitative (l'usage de l'adverbe notamment est clair et sans ambigüité à cet égard), l'article 25 vient plutôt prévoir trois hypothèses reconnues comme étant

[60] Précité, notes 16 et 17.
[61] *Loi concernant le cadre juridique des technologies de l'information*, préc., note 16.
[62] N. W. Vermeys, préc., note 24, p. 141.
[63] Vincent Gautrais, « Droit et sécurité : pas si sûr ! », *Plan*, 2007, p. 32. Disponible à : <http://www.gautrais.com/IMG/pdf/PLAN_2007_Notarius.pdf> (date de visite : 8 mars 2012).

des « *mesures propres à assurer la confidentialité de l'information* ». Dans la présente partie, nous tenterons de voir si la stéganographie est visée par une ou plusieurs de ces hypothèses et, par analogie, si ce procédé peut, en soi, constituer une mesure de sécurité propre à assurer la confidentialité de l'information.

Premièrement, l'article 25 vise « *un contrôle d'accès effectué au moyen d'un procédé de visibilité réduite* ». Une telle exigence sous-tend l'existence de deux éléments cumulatifs : d'une part, celle d'un contrôle d'accès, d'autre part, la mise en place d'un procédé de visibilité réduite. S'agissant de la stéganographie, s'il y a bien une volonté de rendre des données informatiques confidentielles invisibles à l'écran[64], c'est-à-dire au minimum indiscernables à l'œil nu, nous ne considérons pas que ce procédé puisse constituer un réel moyen de contrôle d'accès : en effet, tout le monde peut accéder à l'information confidentielle, sous réserve d'avoir la présence d'esprit de contrôler le document contenant le fichier secret et de disposer d'un logiciel approprié. Dès lors, le « *procédé de visibilité réduite* » introduit par la *LCCJTI* ne vise manifestement pas la stéganographie puisqu'une telle technique ne permet qu'au mieux un « filtrage de l'accès », sans véritable contrôle d'accès (qui suppose l'identification, voire l'authentification, de l'accédant).

Deuxièmement, est constitutif d'une mesure propre à assurer la confidentialité de l'information « *un procédé qui empêche une personne non autorisée de prendre connaissance du renseignement* ». En l'occurrence, cette hypothèse nous paraît englober davantage d'éléments que la première. En effet, loin de fixer des modalités précises (par exemple, l'existence d'un contrôle d'accès ou la mise en place d'un procédé de visibilité réduite), celle-ci s'intéresse plutôt au résultat du procédé, à savoir empêcher une personne non autorisée à prendre connaissance du renseignement. Le terme « empêcher » se réfère à l'idée de « gêner quelqu'un dans son action », de « faire obstacle à quelque chose »[65]. Or, c'est bien là l'objectif même d'un procédé stéganographique : l'information est cachée ou masquée de façon astucieuse parmi d'autres données afin de gêner/faire obstacle à la personne non autorisée à prendre connaissance du renseignement. Aussi, sans dire que cet aspect de la *LCCJTI* vise expressément la stéganographie

[64] Ministère des services gouvernementaux, *Loi annotée par article*, disponible sur le site : <http://www.msg.gouv.qc.ca/gel/loi_ti/articles/chap2/art25.asp> (date de visite : 6 mars 2012).

[65] Linternaute, *Dictionnaire*, disponible sur le site : <http://www.linternaute.com/dictionnaire/fr/definition/empecher/> (date de visite : 6 mars 2012).

(nous avons, par exemple, vu que le tatouage et l'empreinte digitale sont d'autres techniques d'insertion de données cachées), nous pensons tout du moins qu'elle ne l'exclut pas. Dans notre esprit, et par suite logique, la stéganographie peut donc être constitutive d'une « *mesure propre à assurer la confidentialité de l'information* ».

Troisièmement, il faut mettre en place des procédés qui empêchent une personne non autorisée « *d'avoir accès au document ou aux composantes qui permettent d'accéder à l'information* ». Là encore, il y a ici l'idée d'un contrôle sélectif de l'accès, pour lequel la stéganographie, utilisée seule, est assez mal adaptée. Ceci peut être sujet à interprétation, mais, pour simplifier, nous retiendrons dans la suite de ce document que cette exigence ne peut être satisfaite par la seule utilisation de moyens stéganographiques.

En plus de l'article 25 qui a trait à l'accès à un document au sens large, l'analyse doit être complétée par l'article 34 de la LLCJTI. En effet, en visant spécifiquement la transmission de données confidentielles, celui-ci vient conforter l'idée selon laquelle la stéganographie a une place en tant que moyen alternatif de protection de l'information pouvant être mis en œuvre par un RSI raisonnablement prudent et diligent :

> « *Lorsque la loi déclare confidentiels des renseignements que comporte un document, leur confidentialité doit être protégée par un moyen approprié au mode de transmission, y compris sur des réseaux de communication* » [nous soulignons].

En introduisant une notion aussi large que « *moyen approprié* », le Législateur provincial a vraisemblablement voulu laisser aux RSI le choix des moyens « *quant à la façon d'assurer la protection des renseignements confidentiels lors de la transmission d'un document*[66] ». Ces derniers devront toutefois être en mesure de fournir, si besoin est, la documentation exposant comment le procédé stéganographique a pu permettre d'assurer la protection de la confidentialité[67].

En définitive, si la *LCCJTI* ne retient pas explicitement et expressément la stéganographie en tant que « *mesure de sécurité propres à assurer la confidentialité de l'information* » ou

[66] Ministère des services gouvernementaux, *Loi annotée par article*, disponible sur le site : <http://www.msg.gouv.qc.ca/gel/loi_ti/articles/chap2/art34.asp> (date de visite : 12 mars 2012).
[67] *Ib.*

« *moyen approprié au mode de transmission* », nous pensons tout du moins qu'elle ne l'exclut pas. De sorte que, les articles 25 et 34 ne comportant qu'une liste non limitative de mesures propres à assurer la confidentialité pouvant être mises en œuvre, nous pensons qu'un RSI raisonnablement prudent et diligent peut inclure l'utilisation de la stéganographie comme mesure technique alternative de protection de l'information.

En droit fédéral, le *Code type sur la protection des renseignements personnels* s'avère être également une référence pertinente, par exemple lorsqu'un RSI est amené à détenir des données concernant des personnes ou des entités canadiennes résidant à l'extérieur du Québec[68]. Tirant son caractère contraignant de l'article 5 de la *Loi sur la protection des renseignements personnels et les documents électroniques*[69], il prévoit aux termes de son article 4.7.3 :

> « *Les méthodes de protection devraient comprendre :*
> *a) des moyens matériels, par exemple le verrouillage des classeurs et la restriction de l'accès aux bureaux ;*
> *b) des mesures administratives, par exemple des autorisations sécuritaires et un accès sélectif ; et*
> *c) <u>des mesures techniques</u>, par exemple l'usage de mots de passe et du chiffrement* » [nous soulignons].

La cryptographie figure explicitement dans la liste des mesures techniques envisageables (« *par exemple l'usage […] du chiffrement* ») et semble être une mesure de protection de l'information bien établie[70].

Mais qu'en est-il de la stéganographie ? Ni le corpus législatif, ni la jurisprudence n'en parle. Ne pouvant directement répondre à cette question, il faut alors tenter de circonscrire la notion même de « mesure technique » pour voir si la stéganographie peut en faire partie.

---

[68] N. W. Vermeys, préc., note 24, p. 107.
[69] Précité, note 9.
[70] La Commissaire à la protection de la vie privée du Canada écrit d'ailleurs « *le fait que le chiffrement figure dans la liste des mesures de protection au principe 4.7.3 de la LPRPDE laisse croire qu'il s'agit d'une mesure de protection bien établie* ». *Rapport d'enquête sur la sécurité, la collecte et la conservation des renseignements personnels*, 2007 CANLII 41283 (C.V.P.C.), par. 76.

T. J. Smedinghoff en propose la définition suivante: « *technical security measure, involve the use of safeguards incorporated into the computer hardware, software, and related devices. They are designed to ensure system availability, provide access control, authenticate persons seeking access, protect the integrity of information communicated via and stored on the system, and ensure confidentiality where appropriate*[71] ».

À la lecture d'une telle définition, il apparaît que le Législateur fédéral, en introduisant un terme aussi large que mesure technique, n'a certainement pas voulu se limiter aux seules technologies existantes pour le contrôle d'accès[72]. Mais, comme nous l'avons déjà souligné, la stéganographie utilisée seule n'est en l'occurrence pas en mesure de fournir un contrôle d'accès au système, encore moins d'identifier/authentifier les personnes cherchant l'accès.

Il n'empêche que, au vu des dispositions tant provinciales que fédérales, la stéganographie informatique trouve une place, à nos yeux, comme moyen alternatif de protection de l'information pouvant être mis en œuvre par un RSI raisonnablement prudent et diligent. En d'autres termes, un procédé stéganographique peut faire partie de l'ensemble des mesures techniques qu'un RSI doit mettre en œuvre pour se prémunir contre une éventuelle poursuite en responsabilité civile pour manquement à son obligation de sécurité informationnelle[73].

B. En droit spécial : un moyen cumulatif de protection de l'information

L'obligation de sécurité d'un RSI varie, bien sûr, selon le secteur d'activité de son entreprise[74]. Il est aisément compréhensible que, s'agissant de données sensibles, des mesures complémentaires s'imposent aux RSI[75]. L'article 4.7.2 du *Code type sur la protection des renseignements personnels* va d'ailleurs en ce sens en précisant :

---

[71] Thomas J. Smedinghoff, « The Developing Legal Standard for Information Security », *Practicing Law Institute*, 2004, p. 477.
[72] N. W. Vermeys, préc., note 24, p. 159.
[73] *Ib.*, p. 148.
[74] Thomas J. Smedinghoff, "The Emerging Law of Data Security: A Focus on the Key Legal Trends", *Practicing Law Institute*, 2008, p. 20.
[75] Nicolas Samarcq et Luc Masson, « Les agissements en ligne des salariés : un risque majeur pour les entreprises », *Juriscom*, 2006, p. 3, disponible à : <http://juriscom.net/documents/resp20060605.pdf> (date de visite : 7 mars 2012).

« *La nature des mesures de sécurité variera en fonction du degré de sensibilité des renseignements personnels recueillis, de la quantité, de la répartition et du format des renseignements personnels ainsi que des méthodes de conservation. Les renseignements plus sensibles devraient être mieux protégés* » [nous soulignons].

Toutes les informations ne méritent pas la même protection[76] et certains secteurs d'activité vont se voir imposer des exigences plus ou moins restrictives selon le cas[77].

Notons toutefois que la présomption selon laquelle « *specialia generalibus derogant* » ne s'applique pas : en effet, les dispositions propres à certains secteurs d'activités n'exonèrent pas les entreprises concernées de satisfaire aux exigences de droit commun en matière de sécurité informationnelle. Par exemple, une institution financière, contrainte à des dispositions particulières[78], ne peut pas écarter l'article 25 de la LCCJTI. En définitive, comme le résume fort bien le Professeur Vermeys « *ces obligations [particulières] ne viennent pas remplacer [celles de droit commun] ; elles s'y additionnent*[79] ».

Dans un tel schéma, nous tenterons de voir si la stéganographie fait partie des mesures de sécurité qui se doivent d'être mises en œuvre par un RSI en charge de données sensibles.

À ce stade, nous nous référons à l'auteur John Jay Fossett qui a proposé en 1987 un test en cinq étapes permettant de quantifier l'obligation de sécurité d'une entreprise[80]. Malgré ces limites, ce test « *permet d'offrir certains éclaircissements lorsqu'un RSI hésite à incorporer un processus ou une technologie dans la politique de sécurité informationnelle de l'entreprise*[81] ». Nous allons donc essayer de soumettre le procédé stéganographique à ce test :

1. « *La technologie est-elle raisonnablement accessible ?* »

OUI : Quoique peu connu du grand public, il aujourd'hui désormais très facile de se procurer un logiciel assurant à la fois des fonctions stéganographique et cryptographique.

[76] N. W. Vermeys, préc., note 24, p. 108.
[77] *Ib.*, p. 145.
[78] Notamment, la *Loi sur les sociétés d'assurance* (L. C. 1991, c. 47), la *Loi sur les sociétés de fiducie et de prêt* (L. C. 1991, c. 45), la *Loi sur les banques* (L. C. 1991, c. 46), la *Loi sur la distribution de produits et services financiers* (L.R.Q., c. D-92), etc. qui, à certains égards, imposent des obligations sécuritaires plus strictes.
[79] N. W. Vermeys, préc., note 24, p. 108.
[80] John J. Fossett, "The development of Negligence in Computer Law", 14 *Northern Kentucky Law Review*, 1987, p. 302.
[81] N. W. Vermeys, préc., note 24, p. 128.

Pour nous être livré à l'exercice, l'utilisation de tels logiciels ne présente *a priori* rien de complexe. À titre d'exemple, un tutoriel d'« *Invisible Secrets* » vient exposer de manière simple comment mettre en œuvre un procédé stéganographique en six étapes[82].

2. « *L'entreprise en question peut-elle raisonnablement se permettre d'acquérir cette technologie ?* »

OUI : Si l'on raisonne en terme de ratio coût/avantage/attente, l'acquisition de logiciels offrant des fonctionnalités stéganographiques peut aisément se justifier. En effet, la stéganographie présente un avantage indéniable en ce qui a trait à la dissimulation ; or, le coût marginal pour se doter d'un tel logiciel reste très faible, donc fort acceptable, d'autant qu'il en existe même en *freeware* (mais avec tous les inconvénients que cela peut présenter[83]…).

3. « *Cette technologie est-elle déjà utilisée, même de façon minimale, dans le domaine de l'entreprise ?* »

OUI : Il est encore difficile, voire impossible, de fournir des statistiques décrivant l'usage de pratiques stéganographiques par les entreprises, pour deux raisons : la jeunesse du procédé, et le fait qu'il impacte le jardin secret de l'entreprise, l'objectif visé est bien de dissimuler l'existence même d'une transmission d'information. Si les entreprises ne souhaitent pas vraiment communiquer sur le sujet, certaines données laissent toutefois supposer qu'elles l'utilisent, fut-ce de façon minimale. D'ailleurs, un récent rapport français sur la sécurité à l'usage des PME et TPE recommande une dissimulation d'information passant par de la stéganographie[84] : c'est bien la preuve qu'aux yeux des experts, ce procédé présente un réel intérêt pour le monde de l'entreprise.

4. « *Les mesures de sécurité sont-elles à ce point essentielles qu'elles nécessitent l'utilisation de cette technologie ?* »

---

[82] « Initiez-vous à la stéganographie », *Sciences & Avenir*, n° 653, juillet 2001, disponible à : <http://strategique.free.fr/archives/textes/ech/archives_ech_08.htm> (date de visite : 12 mars 2012).

[83] Ce n'est pas parce qu'un logiciel est libre (*freeware* en anglais) qu'il est moins cher à l'usage : si la communauté de développeurs ayant écrit le logiciel n'est pas suffisamment fournie, le logiciel sera peu performant, ne sera pas entretenu et apportera non seulement des vulnérabilités, mais les pires problèmes…

[84] Ouvrage collectif sous la direction de Gérard Péliks, « La sécurité à l'usage des PME et TPE », *Etna France*, 2005, p. 9. Disponible à : <http://www.mag-securs.com/mag/IMG/pdf/PMETPE-3.pdf> (date de visite : 6 mars 2012).

OUI : En l'occurrence, essentiellement pour les données sensibles. Car il est évident que des données sans importance ne nécessitent pas un couplage de cryptographie et de stéganographie. Cela reviendrait à enfermer dans un coffre-fort un journal, puis de l'enterrer : aucun intérêt !

5. « *L'absence de technologie est-elle la cause directe du préjudice ?* »
OUI : Que soit mise en place ou non une sécurisation de la communication (COMSEC), par exemple par le biais d'un procédé cryptographique, reste que c'est bien la non-sécurisation des transmissions (TRANSEC) qui souvent permet à l'attaquant de causer un préjudice. En effet, si à la fois la donnée et la transmission sont dissimulées, l'attaquant ne sait même pas quoi attaquer. La stéganographie concourant à la sécurisation de la transmission, son absence peut être la cause directe du préjudice.

En répondant par la positive à toutes ces questions pour les données sensibles, un constat *a contrario* peut être fait : un RSI n'ayant pas su mettre efficacement en œuvre un procédé stéganographique pourrait se le voir reprocher par sa hiérarchie, et en cas de plainte, son degré de responsabilité pourrait augmenter. Dès lors, quand il s'agit de transmettre des données sensibles, nous ne saurions trop recommander de cumuler une sécurisation de la communication – par exemple par moyen cryptographique – à une sécurisation de la transmission – où la stéganographie peut jouer un rôle.

2. La stéganographie à l'encontre du Droit : le dilemme

Au vu du potentiel de la stéganographie en tant que moyen de protection de l'information, faudrait-il en conclure que la solution la plus sécuritaire pour un RSI serait celle de systématiquement « stéganographier » et crypter l'information, en plus de mettre en œuvre des moyens matériels et des mesures administratives ? Évidemment non. Comme le souligne le Professeur Vermeys : « *si la loi impose l'adoption d'un seuil de sécurité minimal que se doit de respecter un RSI raisonnablement prudent et diligent, elle impose également certains maxima que celui-ci se doit de ne pas dépasser*[85] ». Dans un premier temps, nous porterons notre attention sur le difficile équilibre entre sécurité informationnelle et sécurité publique : un usage abusif et

[85] N. W. Vermeys, préc., note 24, p. 151.

excessif de la stéganographie pouvant de fait gâter son potentiel et ses vertus (A). Dans un second temps, nous nous intéresserons aux impacts d'une telle mesure technique de protection sur l'accessibilité et l'intégrité de l'information (B).

A. Pour un juste équilibre entre sécurité informationnelle et sécurité publique

« *Comme nous le savons tous trop bien, le paysage de la sécurité publique et nationale a évolué considérablement au cours de la dernière décennie. Ce ne sont pas tant les événements du 11 septembre qui ont créé cette nouvelle réalité ; ces événements ont plutôt accéléré et amplifié des changements qui se préparaient déjà dans les sociétés occidentales*[86] », déclarait, le 17 octobre 2011, la Commissaire adjointe à la protection de la vie privée du Canada. En ajoutant : « *Deux grands facteurs redéfinissent les modalités de la sécurité publique et nationale. Outre les sombres événements d'il y a dix ans, les progrès technologiques ont également eu une influence sur le domaine de la sécurité. Une nouvelle génération d'appareils mobiles, de télécapteurs, de caméras à haute résolution et de logiciels analytiques a révolutionné les pratiques de surveillance. Présentement, la collecte, le traitement et le partage des données se passent réellement à l'échelle mondiale et à la vitesse de la lumière*[87] ».

D'une telle allocution, d'apparence contextuelle, peuvent être dégagées deux raisons profondes expliquant les nombreuses craintes et passions que suscite bien souvent la dissimulation d'information, et plus particulièrement la stéganographie.

En premier lieu, des raisons d'ordre conjoncturel. Certains ont en effet prétendu que la stéganographie avait joué un rôle déterminant dans la préparation des attentats du 11 septembre 2001 aux États-Unis. Les réseaux terroristes auraient caché des messages et des plans dans des images postés sur des forums de discussions[88] et dans des photos pornographiques. La

[86] Allocution de Chantal Bernier, Commissaire adjointe à la protection de la vie privée du Canada, « Intégrer le droit à la vie privée aux mesures de sécurité publique du 21e siècle : Une expérience canadienne », *Commentaires dans le cadre de la Conférence internationale sur la circulation de l'information organisée par le Centre de recherche en droit public de l'Université de Montréal*, le 17 octobre 2011 Montréal (Québec), disponible à : <http://www.priv.gc.ca/speech/2011/sp-d_20111017_cb_f.cfm> (date de visite : 8 mars 2012).
[87] *Ib.*
[88] AMBA, « Encyclopédie du Web », disponible à <http://www.amba.fr/definition-stéganographie-ref00911.html> (date de visite : 8 mars 2012).

stéganographie aurait alors constitué un outil important de cyberplanification – technique qui consiste à utiliser les technologies de l'information pour gérer les activités d'un groupe[89] – et aidé « *les différents membres d'un ou plusieurs réseaux terroristes à communiquer entre eux*[90] ». Si un tel usage néfaste de la stéganographie est probable, notons toutefois que celui-ci n'est pas avéré : certains ont pu prétendre qu'il ne s'agissait que « *de rumeurs propagées par des gens souhaitant voir voter une loi limitant l'usage de la stéganographie*[91] ».

En second lieu, des raisons d'ordre structurel. Comme nous avons pu le voir, avec les progrès en matière informatique, le domaine de la dissimulation d'information prend aujourd'hui une nouvelle ampleur. De ce constat, Ken Sala explique que « *Cette situation et la récente prolifération de logiciels stéganographiques peu coûteux et faciles à utiliser signifient que ces personnes possèdent peut-être déjà, à leur insu, des fichiers modifiés ou "sales" dans leur ordinateur. Une telle situation inquiète beaucoup d'entreprises et de ministères. La majorité des logiciels stéganographiques servent à des fins légitimes, mais on craint que ces puissants programmes soient utilisés pour dissimuler des activités illégales, comme le vol de secrets commerciaux ou l'échange de pornographie juvénile. Les entreprises privées et les ministères cherchent comment protéger leurs ordinateurs et leurs sites Web contre les fichiers corrompus*[92] ».

Face à une telle situation, différentes réalités législatives vont émerger en matière de sécurité informationnelle, certaines d'obédience fort interventionniste, d'autres moins.

L'exemple étatsunien est représentatif d'une politique interventionniste reposant sur l'idée : « *Faute de pouvoir voir clair, nous voulons, à tout le moins, voir clairement les obscurités* ». Ainsi, tout en imposant une obligation de sécurité informationnelle contenue à l'article 404 de la « *Sarbanes-Oxley Act of 2002*[93] », le Législateur est venu prévoir une exception à travers l'article

---

[89] Benoît Gagnon, « La révolution dans les affaires terroristes », *Journal of Military and Strategic Studies*, vol. 7, n° 3, 2004, p. 8. Disponible à : <http://www.jmss.org/jmss/index.php/jmss/article/view/139/155> (date de visite : 8 mars 2012).
[90] *Ib.*, p. 8-9.
[91] La cryptographie expliquée, « Petite histoire de la stéganographie », disponible à : <http://www.bibmath.net/crypto/stegano/histstegano.php3> (date de visite : 8 mars 2012).
[92] K. Sala, préc., note 52.
[93] *Public Company Accounting Reform and Investor Protection Act of 2002*, Pub. L. 107-204, 116 Stat. 745.

215 du « *Patriot Act*[94] » qui permet notamment un accès à tout renseignement jugé utile par le gouvernement américain. Le risque d'un tel modèle étant de « *plonger le pays de l'Oncle Sam dans un climat de panique et surtout… d'impuissance*[95] ».

Le cas du Québec, et plus généralement du Canada, est plus nuancé. En effet, s'il existe des maxima sécuritaires auxquels doit se plier un RSI raisonnablement prudent et diligent, les dispositions proscrivant certaines mesures de sécurité et les considérant comme trop dangereuses pour des fins de sécurité publique, restent très limitées[96]. De la sorte, il semble qu'il y ait au Québec « *assez de lumière pour ceux qui ne désirent que de voir, et assez d'obscurité pour qui ont une disposition contraire*[97] ».

Finalement, loin de nous rallier à Rivarol qui considérait que « *nous sommes dans un siècle où l'obscurité protège mieux que la Loi, et rassure plus que l'innocence* », nous pensons à tout le moins que l'élaboration d'un modèle sécuritaire en matière informationnelle ne devrait pas écarter certaines vertus indéniables de la stéganographie.

B. De l'interaction entre confidentialité, accessibilité et intégrité

En matière informationnelle, un modèle sécuritaire adéquat repose nécessairement sur une bonne adéquation entre confidentialité, accessibilité et intégrité. Comme nous l'avons vu, la stéganographie, surtout lorsqu'elle est couplée avec la cryptographie, permet d'assurer une meilleure confidentialité des informations. Mais quels sont les impacts de son utilisation sur l'accessibilité et l'intégrité de l'information ?

Comme le résume fort bien le professeur Vermeys, « *si la garantie d'intégrité d'une information n'est pas en soi incompatible avec la notion de confidentialité, les concepts*

---

[94] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*, Pub. L. 107-56, 115 Stat. 272.
[95] L'économiste, « Stéganographie : l'anonymat qui fait peur », édition n° 1126, 19 octobre 2001, disponible à <http://www.leconomiste.com/article/stéganographie-lanonymat-qui-fait-peur> (date de visite : 8 mars 2012).
[96] N. W. Vermeys, préc., note 24, p. 163.
[97] Blaise Pascal, *Pensées*, 1670, p. 430.

d'accessibilité et de confidentialité sont nécessairement aux antipodes d'un même modèle sécuritaire[98] ».

Nous traiterons d'abord l'exigence d'intégrité : elle peut poser problème quand, après un traitement du stégo-medium qui « lave plus blanc que blanc », les données sont altérées de façon durable, voire perdues pour de bon. Un RSI devra toujours tenir compte de ce risque lors de la transmission, et, pour ne pas être inquiété, prévoir un ensemble de procédures qui permettent de sauvegarder les données transmises par stéganographie, de manière à pouvoir les retransmettre si nécessaire.

Concernant l'accessibilité, précisons au préalable que la disponibilité d'une ressource est indissociable de son accessibilité : il ne suffit pas qu'elle soit disponible, elle doit être également utilisable avec des temps de réponse acceptables[99]. En renforçant la confidentialité d'une information, on pourrait croire que la stéganographie vient de fait « entraver » les droits d'accès d'un tiers, ce qui va à l'encontre même de l'article 430 (1.1) du Code criminel[100] :

> « *Commet un méfait quiconque volontairement, selon le cas :*
> *a) détruit ou modifie des données ;*
> *b) dépouille des données de leur sens, les rend inutiles ou inopérantes ;*
> *c) empêche, interrompt ou gêne l'emploi légitime des données ;*
> *d) empêche, interrompt ou gêne une personne dans l'emploi légitime des données ou refuse l'accès aux données à une personne qui y a droit* ».

En réalité, la réponse est plus complexe. À ce stade, nous distinguerons deux sous-hypothèses :

- D'une part, les schémas de stéganographie pure (c'est-à-dire sans cryptographie)[101] : l'information n'est ni modifiée (intégrité assurée) ni protégée (accessibilité assurée) pour

[98] N. W. Vermeys, préc., note 24, p. 152-153.
[99] Voir site Internet : <http://excerpts.numilog.com/books/9782100521562.pdf> (date de visite : 9 mars 2012).
[100] L.R.C. 1985, c. C-46.
[101] F. Saint-Marcel, préc., note 27, p. 8.

assurer sa confidentialité, elle est simplement cachée ou masquée de façon astucieuse parmi d'autres données[102].

Dans ce cas de figure, s'il y a bien mise en place d'une mesure technique qui pourra d'ailleurs être qualifiée de « préventive[103] »[104], il n'y a pas de contrôle d'accès, que ce soit par voie d'identification ou d'authentification des individus[105]. On reste dans un schéma libertaire : tout le monde peut éventuellement accéder à l'information confidentielle, sous réserve d'avoir la présence d'esprit de contrôler le document contenant le fichier secret et de disposer d'un logiciel approprié. Il n'y a donc aucun problème juridique réel quant à l'emploi d'un tel procédé.

- D'autre part, les schémas de stéganographie avec chiffrement à clé privée ou publique (c'est-à-dire avec cryptographie)[106] : l'information est alors protégée par chiffrement (accessibilité réduite) pour assurer sa confidentialité et elle est de surcroît cachée ou masquée de façon astucieuse parmi d'autres données.

  La personne qui veut avoir accès à l'information confidentielle doit alors connaître la clé, dont la forme la plus simple peut être ce qu'elle sait[107], par exemple un mot de passe. On tombe alors dans le cadre juridique prévu pour l'utilisation de moyens cryptographiques : à moins que « ce qu'elle sait » ne soit constitué de renseignements personnels[108], un tel procédé ne présente rien d'illégal.

Tous ces éléments semblent indiquer que la mise en œuvre de moyens techniques stéganographiques (qu'il y ait couplage ou non avec de la cryptographie) par un RSI ne cause, en soi, aucun problème juridique supplémentaire. Sous réserve toutefois que le RSI fasse correctement son travail en optimisant, en fonction des objectifs qui lui sont assignés, l'équilibre

---

[102] NTX Research, *Glossaire sécurité*, disponible sur le site : <http://www.ntx-research.com/fr_glossaire.php> (date de visite : 6 mars 2012).

[103] "*Preventive security measures are designed to prevent the occurrence of events that compromise security. An example of a preventative security measure is lock on a door (to prevent access to a room), or a firewall (to prevent unwanted access to a computer system)*". Thomas J. Smedinghoff, "The Developing Legal Standard for Information Security", *Practicing Law Institute*, 2004, p. 477.

[104] *A contrario* des méthodes « détectives » ou « réactives », telles qu'introduites par T. J. Smedinghoff. *Ib.*, p. 477.

[105] Dès lors, l'article 40 de la *Loi concernant le cadre juridique des technologies de l'information* ne s'applique donc pas.

[106] F. Saint-Marcel, préc., note 27, p. 9.

[107] Pour authentifier une personne, il existe trois moyens distincts et complémentaires : utiliser ce qu'elle sait (mot de passe, par exemple), ce qu'elle a (carte d'accès, par exemple) ou ce qu'elle est (identifiant biométrique, par exemple).

[108] N. W. Vermeys, préc., note 24, p. 160.

entre confidentialité, accessibilité et intégrité : car nous avons vu en effet que, si la stéganographie améliorait, du fait de la sécurisation de la transmission, la confidentialité de l'information, elle pouvait également impacter l'accessibilité et l'intégrité.

Conclusion

Pour conclure, tous les éléments présentés dans le présent travail – qui, précisons-le, n'a pas la prétention d'avoir fait le tour de la question, mais simplement de sensibiliser et d'apporter une pierre à l'édifice – montrent qu'aujourd'hui, la mise en œuvre et l'utilisation de moyens techniques stéganographiques ne causent, en tant que telle, aucune difficulté nouvelle sur le plan juridique. Sous réserve, bien sûr, que le RSI d'une entreprise satisfasse à son devoir « *d'ajuster les mesures visant à assurer la confidentialité d'informations pour qu'elles respectent les différentes dispositions législatives relatives à l'accès*[109] ».

Mais il pourrait en être différemment demain, compte tenu des possibilités fantastiques offertes par la stéganographie. C'est pourquoi il convient d'être vigilant, pour à la fois ne pas tomber dans un schéma trop restrictif – comme peut l'être l'utilisation de la cryptographie dans certains pays – et préserver les libertés individuelles fondamentales et certains droits, parmi lesquels le droit d'auteur et la propriété intellectuelle.

[109] *Ib.*, p. 153.

Bibliographie

Législation

- Code civil du Québec, L.Q. 1991, c. 64.
- Code criminel, L.R.C. 1985, c. C-46.
- Code type sur la protection des renseignements personnels, CAN/CSA-Q830-96, annexe A à la Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, ch. 5.
- Loi concernant le cadre juridique des technologies de l'information, L.R.Q., c. C-1.1.
- Loi sur la protection des renseignements personnels dans le secteur privé, L.R.Q., c. P-39.1.
- Loi sur la distribution de produits et services financiers, L.R.Q., c. D-92.
- Loi sur les banques, L. C. 1991, c. 46.
- Loi sur les sociétés d'assurance, L. C. 1991, c. 47.
- Loi sur les sociétés de fiducie et de prêt, L. C. 1991, c. 45.
- Public Company Accounting Reform and Investor Protection Act of 2002, Pub. L. 107-204, 116 Stat. 745.
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. 107-56, 115 Stat. 272.

Doctrine

Monographies et ouvrages collectifs :

- KIEFER K. *et al.*, *Information Security: A Legal, Business and Technical Handbook*, Chicago, ABA Publishing, 2004.
- PERSONICK D. S. et PATTERSON A. C., *Critical Information Infrastructure Protection and the Law : An overview of Key Issues*, Washington, The National Academies Press, 2003.
- ROSZAK T., *The Cult of Information, The Folklore of Computers and the True Art of Thinking*, New York, Phanteon Books, 1986.

- SCHNEIER B., *Beyond Fear*, New York, Copernicus Books, 2003.
- SIMMONS G. J., *The prisoner's problem and the subliminal channel*, Plenum Press, 1983.
- TOURNIER M., *La goutte d'or*, Paris, NRF Gallimard, 1985.
- VERMEYS N. W., *Responsabilité civile et sécurité informationnelle*, Montréal, Éditions Yvon Blais, 2010.

Articles de revue :

- ALI-PACHA A., HADJ-SAID N., BELGORAF A. et M'HAMED A., « Stéganographie : sécurité par dissimulation », *Revue d'Information Scientifique et Technique*, vol. 16 nº 1, 2006, p. 101, disponible à <http://www.webreview.dz/IMG/pdf/7-Ali-pacha-rist06.pdf> (date de visite : 27 février 2012).
- CAYRE F., « Cryptographie, stéganographie et tatouage : des secrets partagés », *Interstices*, 2008, disponible à : <http://interstices.info/jcms/c_32093/cryptographie-stéganographie-et-tatouage-des-secrets-partages> (date de visite : 7 mars 2012).
- FOSSETT J. J., « The development of Negligence in Computer Law », 14 *Northern Kentucky Law Review*, 1987, p. 289.
- GAGNON B., « La révolution dans les affaires terroristes », *Journal of Military and Strategic Studies*, vol. 7, n° 3, 2004, p. 8. Disponible à : <http://www.jmss.org/jmss/index.php/jmss/article/view/139/155> (date de visite : 8 mars 2012).
- GAUTRAIS V., « Droit et sécurité : pas si sûr ! », *Plan*, 2007, p. 32. Disponible à : <http://www.gautrais.com/IMG/pdf/PLAN_2007_Notarius.pdf> (date de visite : 8 mars 2012).
- KERCKHOFFS A., « La cryptographie militaire », *Journal des sciences militaires*, vol. IX, janvier 1883, p. 5.
- SAMARCQ N. et MASSON L., « Les agissements en ligne des salariés : un risque majeur pour les entreprises », Juriscom, 2006, disponible à : <http://juriscom.net/documents/resp20060605.pdf> (date de visite : 7 mars 2012).
- SMEDINGHOFF T. J., « The Developing Legal Standard for Information Security », *Practicing Law Institute*, 2004, p. 465.

- SMEDINGHOFF T. J., « The Emerging Law of Data Security : A Focus on the Key Legal Trends », *Practicing Law Institute*, 2008, p. 13.
- « Initiez-vous à la stéganographie », *Sciences & Avenir*, n° 653, juillet 2001, disponible à : <http://strategique.free.fr/archives/textes/ech/archives_ech_08.htm> (date de visite : 12 mars 2012).

Thèses, mémoires et rapports :

- ALATRISTA SALAS H., La stéganographie moderne : l'art de la communication secrète, Mémoire de stage Master 2, Université Montpellier II Sciences et Techniques du Languedoc, 2010.
- BERTHE T., COPPENS J. et DEREGNAUCOURT T., Stéganographie et Watermarking, Rapport de veille technologique Cours d'Applications Réparties, Université des sciences et technologies de Lille.
- DELEGOVE N., Le droit commun et le droit spécial, thèse de doctorat en droit, Faculté de droit de l'Université Paris 2 Panthéon-Assas, 2011. Résumé disponible à : <http://assasrecherche.uparis2.fr/orioaisearch/notice.html?id=2011PA020020&printable=true> (date de visite : 6 mars 2012).
- DOUCENDE B., Sécurité des Systèmes d'Information, Livre blanc du groupe, 2004, p. 19 : <http://www.synertic.fr/sites/default/files/pdf/Livre_Blanc_SSI_v1-4c_0.pdf> (date de visite : 23 février 2012).
- GALAND F., Construction de codes Zpk-Linéaires de bonne distance minimale, et schémas de dissimulation fondés sur les codes de recouvrement, thèse de doctorat en informatique, Université de Caen, 2004.
- GUERROUANI M., Tatouage : application aux documents XML contraints, mémoire d'informatique, Conservatoire national des arts et métiers Paris, 2005.
- SAINT-MARCEL F., Stéganographie VS tatouage, Rapport pour l'étude d'approfondissement, disponible à : <http://membres-liglab.imag.fr/donsez/ujf/easrr0203/tatouagestegano/tatouagestegano.pdf> (date de visite : 28 février 2012).

- VERMEYS N. W., Qualification et quantification de l'obligation de sécurité informationnelle dans la détermination de la faute civile, thèse de doctorat en droit, Faculté de droit de l'Université de Montréal, 2009.

Autres documents :

- BARBIER J., La stéganographie Moderne : d'Hérodote à nos Jours, disponible à : <http://www.novetix.fr/homepages/barbier/partage/articles/barbier07herodote.pdf> (date de visite : 27 février 2012).
- GALAND F., Stéganographie, p. 2, disponible à : <http://www.spiritofhack.net/repository/stegano.pdf> (date de visite : 28 février 2012).
- MERCIOL F. et LEFEVRE S., La stéganographie : une solution pour enrichir le contenu des vidéos numériques, disponible à : <http://www.unicaen.fr/colloques/cnriut2011/papers/187.pdf> (date de visite : 28 février 2012).
- Ouvrage collectif sous la direction de PELIKS G., « La sécurité à l'usage des PME et TPE », Etna France, 2005, p. 9. Disponible à : <http://www.mag-securs.com/mag/IMG/pdf/PMETPE-3.pdf> (date de visite : 6 mars 2012).
- L'économiste, « Stéganographie : l'anonymat qui fait peur », édition n° 1126, 19 octobre 2001, disponible à <http://www.leconomiste.com/article/stéganographie-lanonymat-qui-fait-peur> (date de visite : 8 mars 2012).
- Rapport d'enquête sur la sécurité, la collecte et la conservation des renseignements personnels, 2007 CANLII 41283 (C.V.P.C.), par. 76.

Sites Internet :

- AMBA: http://www.amba.fr.
- Centre de recherches sur les communications Canada : http://www.crc.gc.ca/fr/html/crc/home/home.
- Commissariat à la protection de la vie privée du Canada : http://www.priv.gc.ca.
- Grand dictionnaire terminologique : http://www.granddictionnaire.com.
- Linternaute : http://www.linternaute.com.
- Ministère des services gouvernementaux : http://www.msg.gouv.qc.ca.