Métadonnées : Plaidoyer pour des mal aimées et des incomprises

Patrick GINGRAS et François SENÉCAL

Résumé

Les métadonnées sont les mal aimées et les incomprises des documents technologiques. Malgré toute la richesse documentaire qu'elles comportent, elles sont souvent laissées pour compte tant par la jurisprudence et la doctrine que les juristes. Une meilleure compréhension de leur nature, de leur pertinence, voire même de leur nécessité, notamment en matière de preuve, assurerait un droit plus stable et prévisible, et surtout, mieux arrimé aux réalités technologiques.

Le présent article vise, dans un premier temps, à démystifier les métadonnées rattachées aux documents technologiques et à identifier les risques afférents à la perte ou la modification de ces métadonnées lors de la reproduction du document auxquelles elles sont rattachées. Dans un second temps, à l'aide d'exemples d'application, notamment jurisprudentiels, les auteurs exposent l'utilité de métadonnées pour démontrer l'intégrité des documents technologiques et pour établir un lien entre un document technologique et une personne, un évènement ou une activité.

Métadonnées : Plaidoyer pour des mal aimées et des incomprises

Patrick GINGRAS et François SENÉCAL*

* Patrick Gingras, LL.M., M.B.A., est avocat et agent de marques de commerce au ministère de la Justice du Québec. François Senécal, LL.M, est avocat au sein de l'équipe Gestion de l'information et administration de la preuve électronique chez KPMG S.E.N.C.R.L. Les opinions exprimées dans le présent article n'engagent que les auteurs et ne représentent pas nécessairement celles de leurs employeurs respectifs.

J'ai besoin qu'on m'aime
Mais personne ne comprend
Ce que j'espère et que j'attends
Qui pourrait me dire qui je suis ?
Et j'ai bien peur
Toute ma vie d'être incompris
Car aujourd'hui : je me sens mal aimé[1]

INTRODUCTION

Bien qu'elles existaient déjà avant l'arrivée des supports technologiques[2], les métadonnées ont suscité, et suscitent toujours, de nombreuses interrogations[3], notamment en matière de preuve.

Qui sont-elles exactement ? De quoi sont-elles composées ? Font-elles partie intégrante du document technologique[4] ? L'oubli ou la décision de ne pas en tenir compte lors de la reproduction d'un document technologique peut-il avoir un impact sur l'intégrité du document et, incidemment, son admissibilité en preuve ?

---

1. *Le mal aimé*, auteur : Terry DEMPSEY, traduction/adaptation : Eddy MARNAY (1974), notamment popularisée par Claude FRANÇOIS, en ligne : <https ://www.youtube.com/watch?v=Ls6GdDjMcrk>.
2. Bernard STIEGLER, « Pharmacologie des métadonnées », dans Bernard STIEGLER, Alain GIFFARD et Christian FAURÉ, *Pour en finir avec la mécroissance : quelques réflexions d'Ars Industrialis*, Paris, Flammarion, 2009, p. 87-88 : « [l]es premières métadonnées connues sont très anciennes : elles remontent à la Mésopotamie, où les assyriologues ont découvert que les tablettes d'argile supportant des caractères cunéiformes, et que l'on a retrouvées en masse dans les vallées du Tigre ou de l'Euphrate, étaient en général rangées dans des paniers d'osier, le contenu de chaque panier étant décrit par une tablette où étaient inscrites des métadonnées catégorisant les données contenues dans le panier. » Voir aussi : François SENÉCAL, « Du témoin à l'écrit ; du papier à l'électronique : la notion de faux en toile de fond », (2014) 26(1) *Cahiers de propriété intellectuelle* 161, en ligne : <http://lccjti.ca/doctrine/senecal-notion-faux> ; et Vincent GAUTRAIS, *Preuve technologique*, LexisNexis, Montréal, 2014, 411 p., par. 162 et s.
3. Entre autres à l'égard de la vie privée. À ce sujet, voir notamment : COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Métadonnées et vie privée : Un aperçu technique et juridique*, octobre 2014, en ligne : <https://www.priv.gc.ca/information/research-recherche/2014/md_201410_f.asp> ; et INFORMATION AND PRIVACY COMMISSIONER ONTARIO, *A Primer on Metadata: Separating Fact from Fiction*, juillet 2013, en ligne : <http://www.privacybydesign.ca/content/uploads/2013/07/Metadata.pdf>.
4. Aux fins du présent article, nous discuterons uniquement des métadonnées se rattachant aux documents technologiques, et non de celles afférentes aux documents papier et ce, dans un seul contexte de preuve.

De même, peuvent-elles être utiles en preuve – peuvent-elles permettre de démontrer l'intégrité du document technologique auxquelles elles sont rattachées ou d'établir un lien entre celui-ci et son auteur ?

Toutes ces questions, et bien d'autres d'ailleurs, valent leur pesant d'or au moment où, d'une part, bon nombre de documents commerciaux et des communications entre les citoyens sont créés ou effectués par des moyens technologiques mais où, d'autre part, la littératie, les outils de gestion documentaire et le cadre juridique ne sont pas suffisamment développés ou accessibles à l'ensemble des justiciables. La certitude devant qualifier l'état du droit n'est malheureusement pas à la hauteur de la prégnance du médium technologique – et de ses métadonnées – dans la société.

Alors que les métadonnées peuvent, dans les faits, bien souvent permettre à un juriste aguerri d'entrevoir un filon[5] lui permettant d'étayer, d'un point de vue factuel, sa preuve[6] et même de faciliter la démonstration de son authenticité, la question des métadonnées est généralement ignorée ou rapidement écartée[7]. À ce jour, les juristes semblent préférer utiliser comme preuve un document technologique ayant fait l'objet d'une reproduction sur un support papier bien souvent au détriment des métadonnées que comporte un document technologique dans son format d'origine, dit le format natif[8]. Par ailleurs, le recours au témoignage semble aussi être fréquemment utilisé pour démontrer l'authen-

5. Comme le souligne Vincent GAUTRAIS, « [l]a voie de l'avenir passe sans aucun doute par une meilleure considération probatoire des métadonnées liées aux documents technologiques, et ce, encore une fois, en dépit du silence de la [Loi concernant le cadre juridique des technologies de l'information] ». Vincent GAUTRAIS, *supra*, note 3, par. 164.
6. Le cas classique, et quelque peu risible est celui d'un assuré qui demande un remboursement de la valeur de biens prétendument volés à son assureur et, ce faisant, transmet des photographies numériques où, à la suite de la consultation des métadonnées, l'assureur constate que la date de prise des photographies est postérieure à la déclaration de vol. *Scallon* c. *Desjardins Assurances générales*, 2013 QCCQ 3497. Voir aussi : Belinda GRANT GEARY, « EXCLUSIVE : Daredevil photographer dubbed 'Spiderman' who boasted of his 'pursuit of art in the face of death' STOLE gear he used to take the amazing pictures », *Daily Mail Australia*, 9 juillet 2015, en ligne : <http://www.dailymail.co.uk/news/article-3153049/Daredevil-photographer-dubbed-Spiderman-boasted-pursuit-art-face-death-took-amazing-pictures-15-000-worth-STOLEN-equipment.html>.
7. Voir notamment : *Stadacona, s.e.c.* / *Papier White Birch* c. *KSH Solutions inc.*, 2010 QCCS 2054, concernant des échéanciers de travaux ayant fait l'objet de reproductions par le mode de transfert, soit un enregistrement dans un format PDF.
8. À titre d'exemple, voir : *Sécurité des Deux-Rives ltée* c. *Groupe Meridian construction restauration inc.*, 2013 QCCQ 1301, concernant un courriel ayant fait l'objet d'une impression sur une feuille de papier.

ticité d'un document technologique, lequel s'avère bien souvent dépourvu de ses métadonnées et où, dans certains cas, celles-ci auraient pu être d'une utilité certaine[9]. Force est toutefois d'admettre qu'en pratique, nous avons, à ce jour, répertorié peu de décisions où l'absence des métadonnées semble avoir été problématique ou désavantageuse pour l'une des parties[10] – l'admissibilité de la preuve se faisant généralement de consentement entre les parties. Néanmoins, le passé n'est pas garant de l'avenir.

Considérant la jurisprudence peu bavarde[11] et la doctrine un tantinet timide[12] à l'égard des métadonnées (notamment puisque

9. À titre d'exemples, voir : *Richard* c. *Gougoux*, 2009 QCCS 2301 et *Vandal* c. *Salvas*, 2005 CanLII 40771, concernant des courriels ayant fait l'objet d'une reproduction par le mode de transfert, soit une impression sur une feuille de papier ; *Lefebvre Frères ltée* c. *Giraldeau*, 2009 QCCS 404, concernant des extraits d'agendas électroniques ayant fait l'objet d'une reproduction par le mode de transfert, soit une impression sur une feuille de papier ; *Commission scolaire de la Beauce-Etchemin* c. *Syndicat du personnel de soutien de la commission scolaire de la Beauce-Etchemin*, 2014 QCSAT 58472 concernant une photographie numérique ayant fait l'objet d'une reproduction par le mode de transfert, soit une impression sur une feuille de papier.
10. Voir : *Deslauriers Jeansonne, s.e.n.c.* c. *Panther Publications inc.*, 2011 QCCQ 4293 ; *Protection de la jeunesse – 112213*, 2011 QCCQ 10222, par. 21 et 70 ; *Kuwait Airways Corporation* c. *Iraqi Airways Company*, 2011 QCCS 6365 ; *Demian* c. *Teesdale*, 2011 QCCS 4686, par. 23 ; et *George* c. *Montréal (Ville de),* 2015 QCCQ 4314, par. 11 et suiv., concernant des modifications qui auraient été apportées à des documents, dont des courriels. Voir aussi : *Stadacona, s.e.c.* / *Papier White Birch* c. *KSH Solutions inc.*, *supra*, note 7 ; *TD General Insurance Company* v. *Matei*, 2015 CanLII 39150, par. 30 ; et *GLP Paysagiste inc.* c. *Thibodeau*, 2015 QCCQ 6970, par. 37.
11. Voir notamment : *Richard* c. *Gougoux*, *supra*, note 9 ; *Stadacona, s.e.c.* / *Papier White Birch* c. *KSH Solutions inc.*, *supra*, note 7 ; et *Sécurité des Deux-Rives ltée* c. *Groupe Meridian construction restauration inc.*, *supra*, note 8.
12. Voir notamment : Éric DUNBERRY, *La preuve et l'archivage des documents électroniques*, Montréal, Wilson & Lafleur, 2000, 148 p., notamment à la page 20, en ligne : <http://edoctrine.caij.qc.ca/wilson-et-lafleur-livres/99/469473649/> ; Jean-François DE RICO et Dominic JAAR, « Le cadre juridique des technologies de l'information », dans Service de la formation permanente du Barreau du Québec, *Congrès annuel du Barreau 2009*, Cowansville, Éditions Yvon Blais, 2009, p. 3, en ligne : <http://edoctrine.caij.qc.ca/congres-du-barreau/2009/1733703430/> ; Dominic JAAR et François SENÉCAL, « DéonTIlogie : les obligations de l'avocat face aux technologies de l'information », dans Service de la formation continue du Barreau du Québec, *Développements récents en déontologie, droit professionnel et disciplinaire*, Cowansville, Éditions Yvon Blais, 2010, p. 101, en ligne : <http://edoctrine.caij.qc.ca/developpements-recents/323/368006724> ; Nicolas W. VERMEYS et Patrick GINGRAS, « Je tweet, tu clavardes, il blogue : les aléas juridiques de la communication électronique », dans Service de la formation continue du Barreau du Québec, *Développements récents en déontologie, droit professionnel et disciplinaire*, Cowansville, Éditions Yvon Blais, 2011, p. 5, p. 38, en ligne : <http://edoctrine.caij.qc.ca/developpements-recents/335/368038435> ; Patrick GINGRAS et Nicolas W. VERMEYS, *Actes illicites sur Internet : qui et comment poursuivre*, Cowansville, Éditions Yvon Blais, 2011, 174 p., p. 58 et s. ; Susan WORTZMAN *et al.*, *E-Discovery in Canada*, Montréal, LexisNexis, 2011, p. 159 ;

nous croyons que certaines difficultés en amont accompagnent et expliquent cette paucité[13]), il nous semble opportun de plaider en leur faveur quant aux avantages qu'elles peuvent offrir en matière de preuve[14] – quand elles ne sont pas tout simplement nécessaires[15]. Ces métadonnées que nous considérons aux fins des

---

Pierre TRUDEL, *Introduction à la Loi concernant le cadre juridique des technologies de l'information*, Cowansville, Éditions Yvon Blais, 2012, 360 p., p. 36 et s. ; Gilles DE SAINT-EXUPÉRY, « Le document technologique original dans le droit de la preuve au Québec », Montréal, Faculté des études supérieures, Université de Montréal, 2012, 161 p., p. 96 et p. 120, en ligne : <http://lccjti.ca/doctrine/de-saint-exupery-g-le-document-technologique-original-dans-le-droit-de-la-preuve-au-quebec/> ; Vincent GAUTRAIS et Patrick GINGRAS, « La preuve des documents technologiques », *(2012) Congrès annuel du Barreau*, p. 29, en ligne : <http://edoctrine.caij.qc.ca/congres-du-barreau/20012/1755866973> ; Vincent GAUTRAIS, « TIC + TAQ et preuve technologique », vol. 363 – *Le TAQ d'hier, d'aujourd'hui et de demain – 15e anniversaire du TAQ* (2013), p. 123, en ligne : <http://edoctrine.caij.qc.ca/developpements-recents/363/368125890> ; François SÉNÉCAL et Gilles DE SAINT-EXUPÉRY, « Chronique – Démontrer l'authenticité des documents électroniques », dans *Preuve et Procédure civile en bref*, nº 14, Cowansville, Éditions Yvon Blais, octobre 2013, en ligne : <http://lccjti.ca/doctrine/senecal-f-et-de-saint-exupery-g-chronique-demontrer-lauthenticite-des-documents-electroniques> ; Nicolas VERMEYS, Julie M. GAUTHIER et Sarit MIZHARI, *Étude sur les incidences juridiques de l'utilisation de l'infonuagique par le gouvernement du Québec*, étude présentée au Conseil du Trésor du Québec, 2014, 191 p., p. 94, en ligne : <http://www.cyberjustice.ca/wordpress/wp-content/uploads/2014/08/%C3%89tude-sur-les-incidences-juridiques-de-lutilisation-de-linfonuagique-par-le-gouvernement-du-Qu%C3%A9bec.pdf> ; Patrick GINGRAS et Éloïse GRATTON, « Accéder ou ne pas accéder au matériel informatique de son employé, telle est la question », dans Service de la formation continue du Barreau du Québec, vol. 383, *Développements récents en droit du travail*, Cowansville, Éditions Yvon Blais, 2014, p. 35, p. 43, en ligne : <http://edoctrine.caij.qc.ca/developpements-recents/383/368185469> ; BARREAU DU QUÉBEC, *Guide des TI – Métadonnées*, 24 juillet 2014, en ligne : <http://guideti.barreau.qc.ca/documents/metadonnees/> ; et Vincent GAUTRAIS, *supra*, note 2, par. 162 et s.

13. Notamment la méconnaissance des métadonnées et de la technologie en général par les juristes. À ce sujet, voir notamment : Dominic JAAR et François SENÉCAL, *supra*, note 12, p. 83.
14. À cet égard, nous ne discuterons pas dans le présent article des questions afférentes aux métadonnées et au devoir de confidentialité, ainsi qu'au secret professionnel. Sur ces questions, voir notamment : Claude MARSEILLE, « L'utilisation du courrier électronique à la lumière de la Loi concernant le cadre juridique des technologies de l'information », (2002) 5 *Bulletin de prévention* 1, 2, en ligne : <http://lccjti.ca/doctrine/marseille-bulletin-prevention/> ; AMERICAN BAR ASSOCIATION, *Formal Opinion 06-442: Review and Use of Metadata*, August 5, 2006, en ligne : <http://www.americanbar.org/content/dam/aba/publications/YourABA/06_442.authcheckdam.pdf> ; Michel TÉTRAULT, *La preuve électronique en droit de la famille : ses effets sur le praticien*, Cowansville, Éditions Yvon Blais, 2012, 224 p., p. 28 et s. ; Dominic JAAR et François SENÉCAL, *supra*, note 13 ; ASSOCIATION DU BARREAU CANADIEN, *Lignes directrices pour un exercice du droit conforme à la déontologie dans le cadre des nouvelles technologies de l'information*, 2014, en ligne : <http://www.cba.org/abc/activities_f/pdf/guidelines-fr.pdf> ; et BARREAU DU QUÉBEC, s*upra*, note 12. Voir aussi : *R.* v. *A.B.*, 2014 NLCA 8.
15. *Sécurité des Deux-Rives ltée* c. *Groupe Meridian construction restauration inc.*, *supra*, note 8, par. 66.

présentes, comme des mal aimées et des incomprises, feront dans le présent article, tout comme ce fut le cas pour Goldorak[16], l'objet d'une certaine démystification.

Dans un premier temps, nous statuerons sur ce que nous entendons par les métadonnées (I.). Pour ce faire, nous les considérerons en tenant compte de la *Loi concernant le cadre juridique des technologies de l'information*[17], ci-après la « LCCJTI », et en les catégorisant comme étant internes ou externes au document technologique (I.A.). Par la suite, la question de la nécessité de conserver ces métadonnées, conséquence directe de l'obligation de maintenir l'intégrité d'un document technologique au cours de son cycle de vie, sera abordée[18] (I.B.).

Dans un second temps, nous démontrerons comment les métadonnées peuvent être utiles, voire nécessaires, à un juriste pour démontrer l'authenticité d'un document (II.), à savoir son intégrité (II. A.) et l'établissement d'un lien entre un document technologique et une personne, un évènement ou une activité (II. B.). Bien évidemment, cet exercice prendra place dans un esprit tant soit peu critique au regard de la jurisprudence disponible à ce jour.

I. Qui sont-elles ?

Beaucoup d'informations peuvent être regroupées sous le vocable des métadonnées. Afin de comprendre l'apport qu'elles peuvent avoir en matière de preuve, il importe, dans un premier temps, de définir concrètement ce que nous entendons par ces métadonnées (A.). Nous avons choisi, aux fins du présent article, de catégoriser les métadonnées en fonction d'un seul critère, à savoir si elles sont internes (A.1.) ou externes (A.2.) au document auquel elles se rattachent[19].

---

16. « *Il arrive du fond du temps, Comme un soleil éblouissant, Qui est-il ? D'où vient-il ?, Ce merveilleux génie, De l'infini* ». Extrait de la chanson thème de l'émission Goldorak, *Goldorak le Grand*, interprète : NOAM, auteur : Pierre DELANOË, compositeur : Pascal AURIAT, notamment disponible en ligne : <https ://www.youtube.com/watch?v=qK3hdIK3HKY>.
17. RLRQ, c. C-1.1, ci-après la « LCCJTI ».
18. Art. 6 (2) LCCJTI.
19. Cette classification fut notamment évoquée dans les décisions *Wenzel Downhole Tools Ltd.* c. *National-Oilwell Canada Ltd.*, 2011 CF 1323 ; *Sangha* v. *Reliance Investment Group Ltd.*, 2011 BCSC 1324, par. 325 ; de même que dans : Susan WORTZMAN *et al.*, *supra*, note 12, p. 159 ; François SENÉCAL et Gilles DE SAINT-EXUPÉRY, *supra*, note 12 ; et Vincent GAUTRAIS, *supra*, note 2,

Dans un second temps, considérant que l'intégrité d'un document doit être maintenue au cours de son cycle de vie[20], nous développerons sur la nécessité de les conserver puisque la perte de celles-ci, en tout ou en partie, lors de la reproduction du document technologique auquel elles sont rattachées aura potentiellement une incidence sur le maintien de l'intégrité de ce document et pourrait, de ce fait, affecter son admissibilité en preuve (B.). À cet égard, cette nécessité sera tout particulièrement étudiée en lien avec les métadonnées internes au document technologique ayant fait l'objet d'une reproduction par l'un des deux modes prévus à

---

par. 162. D'un point de vue plus technique, voir : Wikipedia, *File format*, en ligne : <http://en.wikipedia.org/wiki/File_format>.

Bien que nous sommes conscients qu'il existe d'autres façons de catégoriser les métadonnées et que la présente catégorisation puisse sembler simpliste, elle s'avère opportune et suffisante quant à l'objet du présent article.

Nous référerons toutefois, à quelques reprises, à d'autres classifications basées selon les fonctions des métadonnées. À cet égard, les auteures Françoise BANAT-BERGER et Anne CANTEAUT classent les métadonnées selon qu'elles sont descriptives, contextuelles, de gestion ou techniques. Les métadonnées descriptives, ou de contenu, sont celles qui permettent de comprendre, par exemple, la structure d'une base de données et des divers champs qui la composent. Les métadonnées contextuelles renseignent sur la provenance et l'historique du document. Les métadonnées de gestion identifient les dates de versement au système, le nom des personnes impliquées, etc., et enfin, les métadonnées techniques sont celles permettant d'identifier le formatage des données afin de pouvoir reprogrammer l'interpréteur. Françoise BANAT-BERGER et Anne CANTEAUT, « Intégrité, signature et processus d'archivage », dans Stéphanie LACOUR (dir.), *La Sécurité aujourd'hui dans la société de l'information*, Actes des séminaires de recherche du programme Asphales ACI Sécurité informatique 2004-2007, Paris, L'Harmattan, 2007, p. 213, p. 221.

Par ailleurs, BIBLIOTHÈQUE ET ARCHIVES CANADA, *Le gouvernement*, « Que sont les métadonnées ? », en ligne : <http://www.collectionscanada.gc.ca/gouvernement/002/007002-5001.2-f.html>, fait mention de trois catégories de fonctions : descriptives, structurelles et administratives. L'auteur Stephen MASON, dans *Electronic Evidence*, (3d ed.), LexisNexis, 2012, p. 34 et s., utilise ces mêmes catégories. Les métadonnées descriptives décrivent la ressource informationnelle en vue d'une finalité particulière, soit par exemple pour la production d'éléments de preuve, tels : titre, mots clés, nom prétendu de l'auteur, etc. Il précise par ailleurs que « [t]o understand the history of the document more fully, it would be necessary to obtain the underlying information about how and when the system recorded the name of the purported author », comme quoi les métadonnées ne font pas non plus preuve d'elles-mêmes. Les métadonnées structurelles décrivent comment divers éléments sont reliés entre eux. À cet égard, nous traiterons de ces métadonnées à la sous-section I.B.2. Enfin, les métadonnées administratives sont celles qui facilitent ou permettent la gestion des ressources informationnelles : gestion des droits (droits d'accès, etc.) ou gestion documentaire (cote attribuée en fonction du plan de classification, localisation, période de conservation, etc.).

Enfin, la norme ISO-15489 Information et documentation – « Records management » – Partie 1 : Principes directeurs définit les métadonnées de façon fonctionnelle comme des « données décrivant le contexte, le contenu et la structure des documents ainsi que leur gestion dans le temps ».

20. Art. 6(2) LCCJTI.

l'article 2841 al. 1 C.c.Q., à savoir la copie (B.1.) et le transfert (B.2.).[21]

A. Concrètement, de quoi parlons-nous ?

Le terme « métadonnée » signifie « donnée à propos d'une donnée ». Selon Le Grand dictionnaire terminologique de l'Office québécois de la langue française, les métadonnées sont des « donnée[s] qui renseigne[nt] sur la nature de certaines autres données et qui permet[tent] ainsi leur utilisation pertinente »[22]. Plus encore,

> [d]ans la perspective des entrepôts de données, les métadonnées sont un élément primordial et sont destinées à diverses catégories d'utilisateurs. Elles permettent notamment de connaître l'origine et la nature des données stockées dans l'entrepôt, de comprendre comment elles sont structurées, de savoir comment y avoir accès et comment les interpréter, de connaître les différents modèles de données en présence et les règles de gestion de ces données.[23]

Similairement, la norme américaine ANSI-ARMA, 19-2012, *Policy Design for Managing Electronic Messages* définit les métadonnées comme une :

> [s]tructured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource. [Nos soulignés]

Outre quelques mentions que l'on retrouve de façon parcimonieuse et applicables à des situations particulières[24], très peu de

21. Art. 2841 C.c.Q.
22. OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Grand dictionnaire terminologique*, en ligne : <http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=8869869>.
23. *Ibid.* Voir aussi : *Warman* v. *National Post Company*, 2010 ONSC 3670, par. 116 à 118.
24. Voir : *Loi sur les impôts*, RLRQ, c. I-3, Partie 7 (art. 1029.8.36.0.0.13), *Mineral Disposition Regulations*, 1986, Sask Reg 30/86, *The Mineral Tenure Registry Regulations*, RRS, c C-50.2 Reg 27, *Mineral Exploration Incentive Regulations*, RRS c. E-9.10001 Reg 1, *Normes de prestation relatives à l'exercice de la profession d'arpenteur-géomètre*, Règl de l'Ont 216/10, *Water Taking and Transfer*, O Reg 387/04, *Règlement sur le Programme d'aide à la prospection*, Règl du Man 165/92, *Règlement de 1992 sur les aliénations minières et les baux miniers*, Règl du Man 64/92, *Règlement de 1992 sur les minéraux de carrière*, Règl du Man 65/92. Par ailleurs, sans définir ce que l'on entend par métadonnées, le *Règlement sur les documents et informations électroniques*, DORS/2014-117, pris en vertu de la *Loi sur le ministère de l'emploi et du développement social*, LC 2005, c 34, énonce certaines règles quant à la transmission et la conservation des documents et informations électroniques.

lois et de règlements au Canada traitent expressément des métadonnées. À cet égard, soulignons que les règles de procédure de l'Ontario[25] réfèrent aux principes de Sedona Canada[26] et, par inférence, incluent la notion de métadonnées.

À notre connaissance, seule la Nouvelle-Écosse, dans ses règles de procédure civile, énonce dans la définition de « renseignements électroniques » des exemples, non limitatifs, de ce que l'on entend par les métadonnées :

> Enregistrement numérique qui est perçu à l'aide d'un ordinateur en tant que texte, tableau, image, son ou autre élément intelligible ; y sont assimilés les métadonnées associées à l'enregistrement et un enregistrement produit par un ordinateur traitant des données, tout ce qui suit constituant des exemples de renseignements électroniques :
>
> (i) un courriel, y compris une pièce jointe et les métadonnées dans les champs en-têtes indiquant des renseignements tels que l'historique du message et des renseignements concernant l'existence d'une copie muette,
>
> (ii) un fichier de traitement de textes, y compris ses métadonnées telles que les dates de création, de modification et d'accès ainsi que les renseignements concernant l'impression et les données relatives à la préédition de brouillons antérieurs,
>
> (iii) un fichier sonore, y compris ses métadonnées telles que la date de l'enregistrement,
>
> (iv) de nouveaux renseignements que produira une base de données apte à traiter ses données de sorte à produire ces renseignements. (electronic information). [Nos soulignés][27]

---

25. *Rules of Civil Procedure*, RRO 1990, Reg 194, art. 29.1.03(4).
26. SEDONA CANADA, *Les Principes de Sedona Canada : L'administration de la preuve électronique*, 2008, 60 p., en ligne : https://lexum.com/e-discovery/documents/LesPrincipesdeSedonaCanada200801.pdf>.
27. Art. 14.02 (1) des *Règles de procédure civile de la Nouvelle-Écosse*, Nova Scotia Civil Procedure Rules, Royal Gaz Nov 19, 2008. Voir aussi : *Laushway* v. *Messervey*, 2013 NSSC 47, par. 17 ; et *Laushway* v. *Messervey*, 2014 NSCA 7, par. 31 et s. Par ailleurs, sans employer le terme « métadonnée », la LCCJTI traite des « renseignements conservés avec le document lorsqu'ils garantissent les date, heure, minute, seconde de l'envoi ou de la réception et l'indication de sa provenance et sa destination » à son article 31 al. 3, la *Loi visant à promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation de certaines pratiques qui découragent l'exercice des activités commerciales par voie électronique et modifiant la loi sur le Conseil de la radiodiffusion et des télécommunications canadiennes, la loi sur la concurrence, la loi sur la protection des renseignements*

Considérant tout ce qui précède, il nous semble qu'une métadonnée peut être entendue d'une information qui explique le contexte d'un document[28], d'un évènement ou d'une activité[29]. Bref, c'est une information au sujet d'un document, d'un évènement ou d'une activité que l'on peut considérer de la nature d'un fait juridique qu'une partie à un litige pourrait, par hypothèse, souhaiter utiliser en preuve.

Les métadonnées peuvent être créées par une personne ou être automatiquement générées par un logiciel, une application ou un système. Elles peuvent se retrouver dans le document technologique lui-même et en faire partie intégrante – ce sont les métadonnées internes (A-1.). Elles peuvent également se retrouver dans un autre document technologique, tels une base de registre, un fichier de journalisation ou une base de données permettant de les rattacher aux documents qu'elles concernent – ce sont les métadonnées externes (A-2.). Une acception un peu plus large de la notion de métadonnée permet également d'y inclure les informations générées à la suite de l'utilisation d'une technologie par une personne, permettant ainsi de situer un évènement ou une activité (qui, quoi, où, quand et comment)[30]. Dans ce contexte, elles débordent alors du sens purement « documentaire » mais,

---

personnels et les documents électroniques et la loi sur les télécommunications, LC 2010, c 23, traite des données de transmission à son article 1, et la *Loi sur la protection des Canadiens contre la cybercriminalité*, LC 2014, c 31, traite aussi des données de transmission et de localisation à son article 20.

28. « [M]*etadata* [...] *describes certain properties of electronically stored documents that are automatically assigned to the document through the computer operating system and the application used to create the documents. Metadata can indicate properties such as the date a document was created or modified on a computer.* [...] ». *Cameco Corporation* v. *The Queen*, 2014 TCC 45, par. 60.
« [...] il arrive souvent que les logiciels de traitement de texte génèrent automatiquement des fichiers temporaires permettant aux analystes de reconstituer l'élaboration d'un fichier et d'avoir accès à des renseignements indiquant qui a créé le fichier et qui y a travaillé. [...] »
[Notre souligné] *R.* c. *Vu*, 2013 CSC 60, par. 42.
Voir aussi : *Imperial Tobacco Canada Limited* c. *La Reine*, 2013 CCI 144, par. 36 ; *Dosanjh* v. *Leblanc and St. Paul's Hospital*, 2011 BCSC 1660, par. 36 ; *R.* v. *Pan*, 2014 ONSC 6055, par. 82 et 83 ; et *Merpaw* v. *Hyde*, 2015 ONSC 1053, par. 44 et s.

29. « [...] *la plupart des navigateurs utilisés pour consulter Internet sont programmés pour conserver automatiquement des renseignements concernant les sites Web que l'utilisateur a visités dans les semaines précédentes, ainsi que les syntagmes de recherche qu'il a utilisés pour y accéder. Normalement, ces renseignements peuvent aider l'utilisateur à retracer ses démarches cybernétiques.* [...] » *R.* c. *Vu*, *supra*, note 28, par. 42.

30. COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Infographie : Qu'est-ce qu'une « métadonnée »*, mai 2014, en ligne : <https ://www.priv.gc.ca/resource/tool-outil/infographic/md_info_201410_f.asp>.

comme nous le verrons plus loin, elles n'en demeurent pas moins pertinentes en matière de preuve.

1. Les métadonnées internes au document technologique

En vertu de la LCCJTI, un document technologique est constitué d'information portée par un support faisant appel aux technologies de l'information[31]. Un document Word ou Excel, un courriel, un fichier de musique et une photographie numérique sont tous des documents technologiques.

En pratique, un document technologique est d'abord et avant tout un fichier informatique qui comprend en lui-même :

1- Différents renseignements permettant à un programme informatique de « l'ouvrir », instruisant le programme quant à l'encodage utilisé, la version du format utilisé pour le fichier, etc.[32] ;

2- L'information – le contenu informationnel à proprement parler – à afficher ; et

3- Les métadonnées, à afficher sur demande, qui sont des renseignements supplémentaires au sujet du document[33].

Ainsi, le fichier informatique, en plus de son contenu informationnel proprement dit, tels un texte ou une photographie, contient une multitude d'autres informations à même celui-ci.

Certaines métadonnées peuvent être définies et enregistrées automatiquement par un logiciel, une application ou le système

---

31. Art. 3 LCCJTI. Pour une analyse plus détaillée de la notion de document, voir notamment : Vincent GAUTRAIS et Patrick GINGRAS, *supra*, note 12, p. 29 ; Pierre TRUDEL, *supra*, note 12 ; LCCJTI.ca, « Document », 23 janvier 2013, en ligne : <http://lccjti.ca/definition/document/> ; et Vincent GAUTRAIS, *supra*, note 2.
32. Il s'agit de métadonnées structurelles, telles que définie à la note 19.
33. Il s'agit de métadonnées biographiques ou bibliographiques. Pour un aperçu général, voir notamment : SEDONA CANADA, *supra*, note 26, aux p. 3 et 4 ; et INFORMATION AND PRIVACY COMMISSIONER ONTARIO, *supra*, note 3. Par ailleurs, même un simple micromessage (« *tweet* ») comprend des métadonnées. Voir : Simon FODDEN, « The Anatomy of a Tweet: Metadata on Twitter », *Slaw*, 17 novembre 2011, en ligne : <http://www.slaw.ca/2011/11/17/the-anatomy-of-a-tweet-metadata-on-twitter>.

d'exploitation d'un ordinateur, alors que d'autres peuvent être ajoutées ou modifiées à même le document par un usager ou par des systèmes de gestion de l'information lors de sa création, son enregistrement ou sa reproduction[34,35].

À ce titre, un document technologique dans son format natif est un document qui est demeuré au format dans lequel il a été créé ou reçu. Le Grand dictionnaire terminologique de l'Office québécois de la langue française souligne que c'est le « [f]ormat d'origine, non émulé, conçu pour une plateforme donnée »[36]. On peut penser entre autres à un document Word enregistré en format « DOCX » au moment de sa création ou à un courriel reçu par son destinataire dans sa boîte de courriels Outlook en format « MSG »[37].

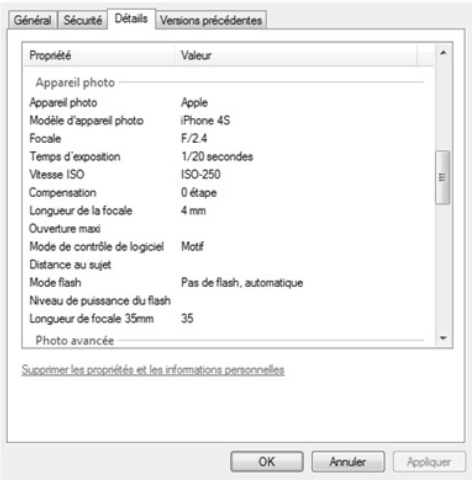
Voici des exemples de métadonnées internes à un document technologique dans son format natif puisqu'elles font partie intégrante de celui-ci.

- Une photographie numérique comprend généralement des métadonnées basées sur le standard EXIF[38]. Tout dépendant du type d'appareil utilisé pour prendre la photographie, il pourrait s'agir, à quelques exceptions près, des mêmes informations qu'aurait colligées, à l'époque de l'argentique, un photographe

34. À titre d'exemple, des métadonnées peuvent être utilisés pour documenter le transfert d'information d'un document vers un support faisant appel à une technologie différente conformément à l'article 17 LCCJTI. Voir notamment : LCCJTI.ca, « Article 17 », 23 janvier 2013, en ligne : 25 mai 2012, <http://lccjti.ca/article/article-17/> ; et BIBLIOTHÈQUE ET ARCHIVES NATIONALES DU QUÉBEC, « La numérisation des documents – Méthodes et recommandations », Direction générale des archives, Version revue et corrigée, Mai 2012, en ligne : <http://lccjti.ca/doctrine/bibliotheque-et-archives-nationales-du-quebec-la-numerisation-des-documents-methodes-et-recommandations/>.
35. BARREAU DU QUÉBEC, *supra*, note 12.
36. OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Grand dictionnaire terminologique*, en ligne : <http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=26508265>.
37. À cet égard, il semble y avoir un débat à savoir si le format MSG est considéré comme un format natif pour les courriels Outlook. En ce qui concerne la collecte de l'entièreté d'une boite de courriels Outlook, nous sommes d'avis qu'il est préférable d'utiliser le format PST. Toutefois, s'il s'agit uniquement d'un courriel, nous croyons que le format MSG peut être utilisé. Craig BALL, « What is Native Production for E-Mail? », 2 juillet 2012, en ligne : <https ://ballinyourcourt.wordpress.com/2013/07/02/what-is-native-production-for-e-mail/>. Sur cette question dans le cadre de la communication de la preuve, voir : *Camino Construction Inc.* v. *Matheson Constructors Limited*, 2015 ONSC 3614, par. 24.
38. WIKIPÉDIA, *Exchangeable image file format*, en ligne : <http://en.wikipedia.org/wiki/Exchangeable_image_file_format>.

consciencieux dans un calepin de notes. Ces métadonnées peuvent notamment être[39] :

- Le manufacturier de l'appareil ;
- Le modèle de l'appareil[40] ;
- La version du logiciel utilisé par l'appareil ;



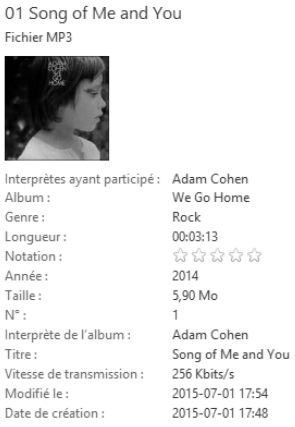
- Les date et heure auxquelles la photographie a été prise et, le cas échéant, modifiée[41] ;

---

39. « [...] Digital cameras typically record the time and date when the photograph was taken. Some cameras capture the camera's GPS co-ordinates as well. These data are known as metadata. These data are relevant to a matter in issue in this lawsuit because they may provide information from which the camera user's tolerance for physical activity from day to day or over several days may be inferred. More particularly, the metadata may be relevant to the plaintiff's ability to, for example, be active throughout a given day and then go walking on the beach in the evening, or it may be relevant to the plaintiff's ability to spend an evening at a nightclub until some given hour, and then tolerate swimming the next morning. [...] ». *Abougoush* v. *Sauve*, 2011 BCSC 885, par. 11. Voir aussi *R.* v. *Somel*, 2015 ONSC 2207, par. 117.
Par ailleurs, quant à l'impact sur les métadonnées de la modification d'une photographie, par exemple le rognage d'une partie de la photographie, ou son téléversement sur un réseau social, voir notamment : *R.* v. *Andalib-Goortani*, 2014 ONSC 4690, par. 9 et s.
40. Voir notamment : *Mejia* v. *LaSalle College International Vancouver Inc.*, 2014 BCSC 1559, par. 179 ; *R.* v. *Cockell*, 2013 ABCA 112, par. 20 et 21 (*R.* v. *Cockell*, 2012 ABQB 149, par. 72) ; *R.* v *SBS*, 2013 ABQB 322, par. 70 à 73 ; *R.* v. *Caza*, 2012 BCSC 627, par. 24 et 64 ; *R.* v. *Cater*, 2012 NSPC 18, par. 46 ; *R.* v. *Cater*, 2012 NSPC 2, par. 40 ; et *Scallon* c. *Desjardins Assurances générales*, *supra*, note 6, par. 19.
41. Voir notamment : *Mejia* v. *LaSalle College International Vancouver Inc.*, *supra*, note 40, par. 179 ; *R.* v. *Cockell*, *supra*, note 40, par. 20 et 21 (*R.* v. *Cockell*, *supra*, note 40, par.72) ; *R.* v. *SBS*, *supra*, note 40, par. 70 à 73 ; *R.* c. *Cole*, 2012 CSC 53, par. 131 ; *Glanzmann Tours Ltd.* v. *Yukon Wide Adventures*, 2012 YKSM 3, par. 11 ; *R.* v. *Caza*, *supra*, note 40, par. 24 et 64 ; *R.* v. *Cater*, *supra*, note 40, par. 46 ; *R.* v. *Cater*, *supra*, note 40, par. 40 ; *R.* c. *Therrien*, 2008 QCCQ 9175, par. 73 ; *R.* c. *Coupal*, 2013 QCCQ 859, par. 8 (incluant la date de dernière consultation) ; et *Scallon* c. *Desjardins Assurances générales*, *supra*, note 6, par. 19.

- Le format du fichier et l'algorithme de compression ;
- La résolution de la photographie ;
- Le temps d'exposition de la photographie ;
- Le type de lentille utilisée pour prendre la photographie[42] ;
- L'ouverture, la vitesse d'obturation et la sensibilité ISO quant à la photographie.
- Le mode de flash utilisé ;
- La géolocalisation de l'endroit où la photographie a été prise.

• Un fichier de musique en format MP3 comprend des métadonnées basées sur le standard ID3[43], tels :

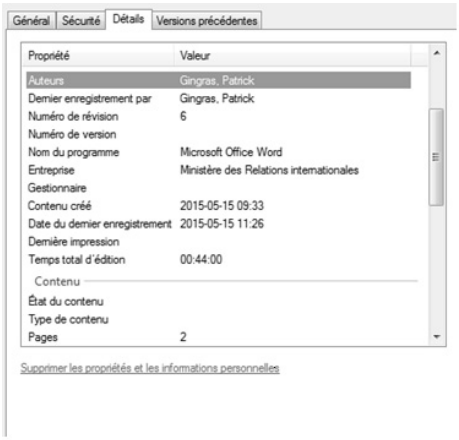


- L'auteur de l'œuvre ainsi que, le cas échéant, l'interprète, le compositeur ou tout autre collaborateur ;
- Le titre de l'œuvre musicale ;
- L'année de création de l'œuvre ;
- Le titre de l'album dans lequel se trouve l'œuvre ;
- Une image de la jaquette de l'album ;
- Le numéro de la pièce dans l'album ;
- Le genre selon une liste de choix prédéfini ;
- Un champ pour des commentaires.

42. *Bernier* c. *L'Écho de la Rive-Nord*, 2012 CanLII 18581 (QC CPQ), par. 4.
43. WIKIPÉDIA, *ID3*, en ligne : <http://en.wikipedia.org/wiki/ID3>. Concernant les métadonnées d'un fichier, à savoir un film, voir : *Voltage Picture LLC* v. *John Doe*, 2014 FC 161, par. 13.

- Un document créé avec un logiciel d'une suite bureautique comme Microsoft Office ou Apache OpenOffice, de même qu'un document enregistré en format PDF comprend également une multitude de métadonnées, les plus connues étant notamment[44] :

  - Le titre du document ;
  - L'auteur du document ;
  - L'organisation/entreprise de l'auteur ;
  - L'auteur de la dernière modification ;
  - La date de création ou de la dernière modification apportée[45] ;
  - La date de la dernière impression ;
  - Le modèle de document[46] ;
  - Le nombre de mots ;
  - Le temps total d'édition ;



44. « [...] In particular, metadata would include when each document was prepared, what changes were made to drafts of the document, when and by whom those changes were made. [...] ». *Berry* v. *Scotia Capital Inc.*, 2014 ONSC 5244, par. 36. Voir aussi : *Demaria* v. *Law Society of Saskatchewan*, 2013 SKQB 178, par. 72.
45. À titre d'exemple, c'est notamment à l'aide des métadonnées qu'il fut possible, dans le cadre de la Commission d'enquête sur le processus de nomination des juges du Québec, de déterminer avec précision la dernière date de modification d'un fichier emmagasiné sur un cédérom ainsi que la dernière date de consultation d'un agenda sauvegardé sur une disquette. Voir la pièce 88 P : *Rapport d'expertise*, en ligne : <http://www.cepnj.gouv.qc.ca/documents-deposes-devant-la-commission.html?eID=tx_rtgfiles_download&tx_rtgfiles_pi1%5Buid%5D= 157>. Voir aussi : *Animal Welfare International Inc.* v. *W3 International Media Ltd.*, 2014 BCSC 1839, par. 340 ; *Dhillon* v. *Virk*, 2014 BCSC 51, par. 34 ; *Law Society of Upper Canada* v. *Ali Amiri*, 2013 ONLSHP 124, par. 39 ; *Sangha* v. *Reliance Investment Group Ltd.*, *supra*, note 19, par. 325 ; *Ménard* c. *Société de transport de Montréal*, 2012 QCCRT 454, par. 129 ; *Wenzel Downhole Tools Ltd.* c. *National-Oilwell Canada Ltd.*, *supra*, note 19, par. 111 ; et *1483860 Ontario* v. *Beaudoin*, 2011 ONSC 5311.
46. Quant au fait qu'un document provenait d'une version antérieure, voir notamment : *Sangha* c. *Reliance Investment Group Ltd.*, *supra*, note 19.

- Des marques d'édition et des commentaires[47].

- Une page Web créée en langage HTML[48] comprend elle aussi des métadonnées. Il s'agit notamment :


http://www.lapresse.ca/ - Source originale

Fichier Edition Formater

```
 7
 8 <!doctype html>
 9 <!-- accueil et Rmon1 entete -->
10 <html lang="fr" xmlns:fb="http://ogp.me/ns/fb#">
11 <!-- / accueil et Rmon1  -->
12
13 <!-- Tout le site -->
14 <head>
15     <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
16 <title>LaPresse.ca | Actualités, Arts, International, Débats, Sports, Vivre, Voyage</title>
17 <meta name="description" content="Le site d'information francophone le plus complet en Amérique: Actualités régionales, provinciales,
   nationales et internationales" />
18 <meta name="keywords" content="Actualités, Arts, International, Débats, Sports, Vivre, Voyage" />
19 <meta property="og:type" content="article" />
20 <meta property="og:title" content="LaPresse.ca | Actualités, Arts, International, Débats, Sports, Vivre, Voyage" />
21 <meta property="og:description" content="Le site d'information francophone le plus complet en Amérique: Actualités régionales,
   provinciales, nationales et internationales" />
22 <meta property="og:site_name" content="La Presse" />
23 <meta property="og:locale" content="fr_CA" />
24 <meta property="og:url" content="http://www.lapresse.ca/" />
25 <meta name="twitter:card" content="summary_large_image">
26 <meta name="twitter:site" content="@LP_LaPresse">
27 <meta name="twitter:title" content="LaPresse.ca | Actualités, Arts, International, Débats, Sports, Vivre, Voyage">
28 <meta name="twitter:description" content="Le site d'information francophone le plus complet en Amérique: Actualités régionales,
   provinciales, nationales et internationales">
29
```

  - Du titre de la page Web (<*title*> en langage HTML) ;

  - De la description de la page Web (<*description*> en langage HTML) ;

  - Des mots clés de la page (divers éléments de la balise <*meta*> en langage HTML).

- Un courriel, incluant son en-tête, contient, outre la date d'envoi, l'expéditeur et son objet, une multitude de métadonnées[49]. Toutefois, certaines de ses métadonnées sont bien souvent complexes à interpréter et une attention particulière doit leur être apportée[50] – certaines connaissances techniques peu-

47. Bien que techniquement parlant, le suivi des modifications et les commentaires puissent ne pas être considérés comme faisant partie des métadonnées, nous inclurons ceux-ci dans la définition des métadonnées internes aux fins du présent article. Dominic JAAR et François SENÉCAL, *supra*, note 12, note 55.
48. WIKIPÉDIA, *Hypertext Markup Language*, en ligne : <http://fr.wikipedia.org/wiki/Hypertext_Markup_Language>.
49. Les champs « de », « à », « cc », « cci », « date d'envoi », « date de réception » et « objet » que l'on retrouve dans les courriels sont considérés comme étant des métadonnées. Par surcroît, tout courriel reçu contient généralement beaucoup d'informations retraçant, serveur par serveur, le chemin parcouru de l'expéditeur au destinataire. BARREAU DU QUÉBEC, *supra*, note 12. Voir aussi : Nicolas VERMEYS et Patrick GINGRAS, *supra*, note 12, p. 38.
50. « Certains avertissements s'imposent : D'abord, il est possible que les métadonnées d'un courriel soient mal interprétées. Par exemple, l'heure d'envoi d'un courriel devrait être examinée minutieusement si l'émetteur et le récipiendaire sont des fuseaux horaires différents, puisque le fuseau horaire ne fait pas partie des

vent être nécessaires[51]. Ces métadonnées peuvent notamment être :

```
Received: from GOATLEXC903.kworld.kpmg.com (10.196.2.107) by
 CATOREXC900.ca.kworld.kpmg.com (10.132.30.85) with Microsoft SMTP Server
 (TLS) id 14.3.224.2; Sun, 28 Jun 2015 10:50:34 -0400
Received: from kpmg.com (10.196.6.206) by GOATLEXC903.kworld.kpmg.com
 (10.196.2.44) with Microsoft SMTP Server id 14.3.224.2; Sun, 28 Jun 2015
 10:50:33 -0400
Received: from courrier.mri.gouv.qc.ca (courrier.mri.gouv.qc.ca
 [205.151.51.5])    by m0004873.ppops.net with ESMTP id 1va8svkb6g-1
          (version=TLSv1/SSLv3 cipher=ECDHE-RSA-AES256-GCM-SHA384 bits=256 verify=NOT)
          for <fsenecal@kpmg.ca>; Sun, 28 Jun 2015 14:50:32 +0000
Received: from PARVATI.inter.reseau (parvati.inter.reseau [172.30.32.210]) by
 courrier.mri.gouv.qc.ca with ESMTP id 2ErUgRdi0HwKkBBI (version=TLSv1
 cipher=AES128-SHA bits=128 verify=NO); Sun, 28 Jun 2015 10:50:30 -0400 (EDT)
Received: from BRAHMA.inter.reseau ([169.254.1.198]) by PARVATI.inter.reseau
 ([fe80::381f:b007:d19f:5801%16]) with mapi id 14.03.0224.002; Sun, 28 Jun
 2015 10:49:54 -0400
From: "Gingras, Patrick" <Patrick.Gingras@mri.gouv.qc.ca>
To: =?iso-8859-1?Q?Fran=E7ois_Sen=E9cal?= <fsenecal@kpmg.ca>,
Subject: Lexique
X-ASG-Orig-Subj: Lexique
Thread-Index: AQHQsbGxj5wOGxmSg06KDJkPtOj05Q==
Date: Sun, 28 Jun 2015 14:49:53 +0000
Message-ID: <A7BAFE92-E6D6-4626-86A6-FD40F7319FCD@mri.gouv.qc.ca>
```

En-tête d'un courriel entre les deux auteurs (extrait) :

- Des informations sur le programme informatique utilisé par l'expéditeur ;
- L'adresse IP de l'expéditeur[52] ;
- L'heure et la date de sa transmission[53] ;

---

métadonnées. Un courriel transmis à 11 h à Vancouver, c.-à-d. 14 h à Montréal, pourrait être interprété comme ayant été reçu à 14 h, heure de Vancouver. De plus, la date et l'heure d'envoi et de réception d'un courriel sont basées sur le réglage des dates et heures des ordinateurs des émetteurs et récipiendaires ; Ainsi, si ces réglages sont inexacts, les métadonnées afférentes seront affectées. Pour terminer, mentionnons que certaines métadonnées peuvent être réinitialisées par l'utilisateur. » SEDONA CANADA, *supra*, note 26, note 10.

51. Il importe de souligner que selon le mode d'envoi d'un courriel, par exemple via une messagerie Web en HTTP, via un serveur SMTP, ou via un serveur Exchange, le courriel que l'on retrouve dans la boite « Éléments envoyés » peut contenir une quantité variable de métadonnées.
52. Voir : *A* c. *B*, 2009 QCCQ 14676, par. 28.
53. Voir : *Bustros* c. *César*, 2010 QCCQ 8099, par. 13 ; *Section locale 145 du Syndicat canadien des communications, de l'énergie et du papier (Section locale 145, SCEP)* c. *Roy*, 2011 QCCRT 234, par. 41 et s. ; et *GLP Paysagiste inc.* c. *Thibodeau*, *supra*, note 10. Voir aussi : Patrick GINGRAS et Jean-François De RICO, « La transmission des documents technologiques », *XX^e Conférence des juristes de l'État 2013 – XX^e Conférence*, Cowansville, Éditions Yvon Blais, 2013, 694 p., p. 435, en ligne : <http://lccjti.ca/doctrine/gingras- patrick-et-de-rico-jean-francois-la-transmission-des-documents-technologi ques/>.

- Des identifiants uniques ;
- Une valeur de hachage
- Des informations sur les dates et nombreux systèmes empruntés par le courriel entre le serveur courriel de l'expéditeur et le serveur entrant du destinataire[54].

Ainsi, la grande majorité des documents technologiques comporte des métadonnées[55]. Plus que la photographie numérique, le fichier de musique, le document ou le courriel, la grande majorité des fichiers informatiques qui les comprennent comportent des métadonnées faisant partie intégrante de ceux-ci.

Plusieurs formats de documents sont néanmoins plus complexes dans leur nature que les exemples présentés précédemment. En effet, qu'en est-il des documents technologiques générés à partir d'un tableur permettant la création de feuilles de calcul, tel Microsoft Excel, ou d'un logiciel de gestion de projet, tel Microsoft Project ? Ces documents sont quelque peu différents considérant que l'information qu'ils affichent est, en tout ou en partie, fonction de l'information qui y a été enregistrée.

---

54. Celles-ci sont particulièrement utiles dans les cas où l'intégrité ou l'expéditeur d'un courriel est contesté, par exemple dans les cas d'usurpation d'adresse IP (« *IP spoofing* »), soit une « [t]echnique qui consiste à usurper l'identité d'un autre utilisateur du réseau en utilisant son adresse IP, ce qui permet de faire croire que la connexion provient d'un compte d'utilisateur autorisé. ». Voir : OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Grand dictionnaire terminologique*, en ligne : <http:// www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=8370637>. Dans le cas d'un courriel où plusieurs informations (expéditeur, date et autres métadonnées) auront été forgées, il sera question de « email spoofing » – voir WIKIPÉDIA, « Email spoofing », en ligne : <http://en.wikipedia.org/wiki/Email_spoofing>. Pour des exemples, voir notamment : *Vaquero Energy* v. *Weir*, 2004 ABQB 68, par. 10 et 12 et *R.* v. *Moss*, 2011 ONSC 51436, par. 37 à 41, 63 et 76.

55. Eu égard aux messages textes, voir notamment : *R.* v. *A.B.*, *supra*, note 14, par 43, aux sites Web, voir notamment : *WCAT-2012-02876 (Re)*, 2012 CanLII 88303 (BC WCAT), par. 102 ; à un compte ou profil Facebook, un blogue et un service de clavardage ou de messagerie instantanée : *Frangione* v. *Vandongen et al.*, 2010 ONSC 2823, par. 65 ; Nicolas VERMEYS, « Facebook et la relation employeur-employé : quand amitié et surveillance vont de pair », dans Service de la formation continue du Barreau du Québec, *Développements récents en droit de la santé et sécurité au travail*, Cowansville, Éditions Yvon Blais, 2014, p. 169, p. 173, en ligne : <http://edoctrine.caij.qc.ca/developpements-recents/379/368161447/> ; Nicolas VERMEYS et Patrick GINGRAS, *supra*, note 12, p. 38 ; et Patrick GINGRAS et Nicolas W. VERMEYS, *supra*, note 12, p. 58 et s.

À titre d'exemple, si un utilisateur inscrit les chiffres 6 (cellule A1 de l'illustration 1) et 8 (cellule B1 de l'illustration 1) dans deux cellules d'une feuille de calcul d'un tableur et qu'il demande à l'aide d'une formule à la troisième cellule d'afficher le produit de ces deux cellules, celle-ci affichera le nombre 48 (cellule C1 de l'illustration 1). Par ailleurs, sans modifier la formule inscrite, la cellule affichera le nombre 60 (cellule C1 de l'illustration 2) si le chiffre 8 est changé pour le nombre 10 (cellule B1 de l'illustration 2). Dans ce contexte, le document est-il ce qui est affiché et directement visible, ou est-ce que les informations et les formules entrées par l'utilisateur sont partie intégrante du document ? Dans cet exemple, nous sommes d'avis que tant l'information affichée que la formule sont essentielles à la compréhension du document[56] – à son intelligibilité – et qu'à ce titre, la réponse est positive[57].

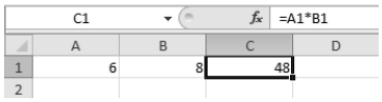


Illustration 1

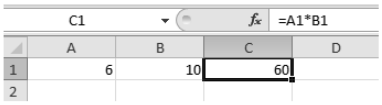


Illustration 2

Nous croyons qu'il faut alors voir le document comme un programme qui contient de l'information et des instructions, comme

56. Bien que le présent exemple soit simpliste, il est facile d'extrapoler la nécessité de connaitre les formules d'un document comptable s'il est nécessaire d'en faire l'expertise.

57. Au soutien de cette prétention, voir : Dominic JAAR, Élise LACOSTE et François SENÉCAL, « Investir dans les renseignements personnels et leur protection », dans Service de la formation permanente du Barreau du Québec, *Développements récents en droit de l'accès à l'information et de la protection des renseignements personnels – les 30 ans de la Commission d'accès à l'information*, vol. 328, Cowansville, Éditions Yvon Blais, 2012, p. 358, p. 195, en ligne : <http://edoctrine.caij.qc.ca/developpements-recents/358/368100906> ; et SEDONA CANADA, *supra*, note 26, à la note 11.
Par ailleurs et avec déférence pour le tribunal, il en découle que nous sommes en désaccord avec la décision *Stadacona, s.e.c. / Papier White Birch* c. *KSH Solutions inc.*, *supra*, note 7, laquelle confirma la communication à la demanderesse *Stadacona, s.e.c. / Papier White Birch* d'un document technologique format PDF, soit un format différent de celui d'origine, lequel ne permettait pas de prendre connaissance des formules permettant à l'expert de la demanderesse *Stadacona, s.e.c. / Papier White Birch* de comprendre le fonctionnement de l'échéancier des travaux. « Dans un format PDF, l'expert ne peut examiner les effets d'un changement à l'échéancier des travaux qu'induit sur les autres éléments de l'échéancier tel changement. L'expert ne pourra ainsi identifier « le chemin critique » dont fait référence [l'expert de la défenderesse KSH Solutions inc.] » Sur cette question, voir notamment : Vincent GAUTRAIS et Patrick GINGRAS, *supra*, note 12, p. 29.

par exemple des formules[58]. Ainsi, une façon encore plus simple de le concevoir est par l'entremise du jumelage de l'information et de sa mise en forme, à savoir :

Information :	« texte en gras »
Mise en forme (formule) :	texte en gras
Résultat affiché :	**texte en gras**.[59]

Même le simple fichier d'un éditeur de texte peut être vu comme un document programme. Ceci étant, la différence notable entre ce fichier et une feuille de calcul d'un tableur est que c'est généralement l'affichage final à l'utilisateur qui est important pour un document textuel, alors que c'est dans le processus intellectuel menant aux résultats affichés dans la feuille de calcul d'un tableur que se retrouve toute la valeur de ce type de documents[60]. L'imprimé sur une feuille de papier ou la version statique, en format PDF par exemple, d'un fichier texte reproduira en principe fidèlement le contenu informationnel du document – à distinguer de ses métadonnées, tel que vu en début de la présente sous-section, alors que pareille version d'un document créé à l'aide d'un tableur occultera toute la structure intellectuelle du document pour n'afficher que les résultats.

La pertinence de ces informations ne fait aucun doute dans les litiges. Ainsi, les métadonnées incluses à des photographies numériques ont été centrales dans deux autres décisions. Dans la première, il était question de déterminer si une personne a consenti à la prise de sa photographie par un journaliste. Les métadonnées de la photographie ont permis de déterminer le type de lentille utilisé, permettant ainsi au journaliste de démontrer que la photographie avait été prise à une distance de quelques mètres et qu'en conséquence, la personne photographiée ne pouvait pas ne pas savoir faire l'objet de ladite photographie[61]. Dans la seconde décision, il a été possible de déterminer la date de la prise des photographies soumises à un assureur au soutien d'une

58. R.T. PÉDAUQUE, « Document : forme, signe et médium, les re-formulations du numérique », dans R. T. PÉDAUQUE, *Le document à la lumière du numérique*, Caen, C&F Éditions, 2006.
59. LCCJTI.ca, « Document », 23 janvier 2013, en ligne : <http://lccjti.ca/definition/document/>.
60. À ce sujet, voir notamment François SENÉCAL, *L'écrit électronique*, Cowansville, Éditions Yvon Blais, 2012, 202 p., p. 122 et s., version précédente en ligne : <http://lccjti.ca/doctrine/senecal/>.
61. Voir notamment : *Bernier* c. *L'Écho de la Rive-Nord*, *supra,* note 42.

demande d'indemnisation – les photographies avaient été prises très peu de temps avant le sinistre allégué[62]. Ces deux décisions soulignent l'importance de s'assurer de la conservation des métadonnées EXIF[63] lors de la reproduction d'une photographie numérique. Leur pertinence est telle qu'elles font partie intégrante de la photographie et qu'elles peuvent être utiles pour établir des faits distincts, tels le consentement du sujet, leur authenticité, ou la date de la photographie.

2. Les métadonnées externes au document technologique

Les métadonnées externes à un document technologique sont des informations qui, à la différence des métadonnées internes, ne font pas partie intégrante du document technologique auquel elles se rattachent. Ces métadonnées se retrouvent dans un autre document et constituent, en elles-mêmes, un autre document technologique. À ce titre, les métadonnées utilisées par un système de gestion documentaire sont souvent externes aux documents qu'elles concernent, et sont généralement comprises dans une base de données distincte des documents.

Au sujet des métadonnées externes, l'auteure Susan Wortzman énonce :

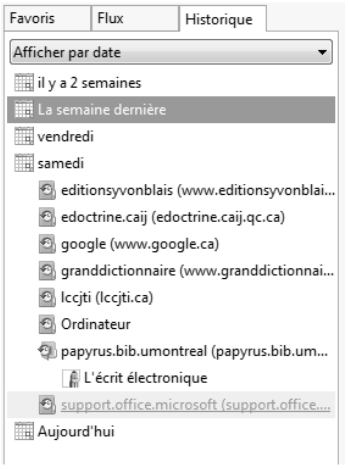
> Metadata may also exist elsewhere in the computer, in the form of log files, entries to the Windows Registry, history files, and so on. Metadata may also exist elsewhere on the network, and, in terms of Internet use, may also exist, along with the files and records, somewhere outside the organization, whether on the systems of any [Internet services provider], or on third party Web sites or servers.[64] [nos soulignés]

Les métadonnées externes peuvent être toutes aussi importantes que les métadonnées internes. Elles regroupent sous leur vocable les informations afférentes aux systèmes, telles les dates de création, d'accès et de dernière modification, mais aussi, pour

62. Voir : *Scallon* c. *Desjardins Assurances générales*, *supra*, note 6. Voir aussi Belinda GRANT GEARY, *supra*, note 6
63. Voir la note 38.
64. Susan WORTZMAN *et al.*, *supra*, note 12, p. 159.

certains systèmes, les informations relatives à l'utilisateur, aux droits d'accès, etc.[65]. Ainsi, nous considérons, par exemple, un fichier de journalisation, soit l'« enregistrement [dans un document] d'événements se produisant dans un système informatique »[66] comme étant des métadonnées externes relatives à un autre document, un évènement ou une activité effectuée sur Internet, tels un historique de navigation[67] ou un fichier de témoins (« *cookies* »)[68], ou relié à l'utilisation ou l'accès à un logiciel[69], une application ou un système d'exploitation, ou à un médium technologique[70].

À titre d'exemple, dans la décision *Durocher-Lalonde* c. *9096-0469 Québec inc.*, un historique de navigation semble avoir été utilisé afin de démontrer les sites Web visités par une employée à partir de l'ordinateur de son employeur, incluant les recherches qu'elle a effectuées sur Internet par celle-ci :



> Madame Côté se rend ensuite à la réception de l'hôtel et vérifie l'historique des utilisations faites sur l'ordinateur du centre de santé depuis la veille. Elle constate qu'il y a eu successivement des visites sur le site d'Emploi-Québec (10 h 5), sur Facebook (10 h 46, 10 h 48, 10 h 53 et 11 h 38), sur le site enceinte.com

65. François SÉNÉCAL et Gilles DE SAINT-EXUPÉRY, *supra*, note 12.
66. OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Grand dictionnaire terminologique,* en ligne : <http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=8383642>.
67. Voir notamment : *Desgagne* v. *Yuen et al.*, 2006 BCSC 955, par. 43 à 45 ; *R.* c. *Morelli*, 2010 CSC 8, par. 105 et *R.* c. *Vu*, *supra*, note 28, par. 42 et 46 ; *Perreault* c. *R.*, 2015 QCCA 694, par. 77 et Patrick GINGRAS et Éloïse GRATTON, *supra*, note 12, p. 45.
68. « Fichier créé dans l'ordinateur de l'internaute par le navigateur et rassemblant les témoins persistants issus de la visite de sites Web. » OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Grand dictionnaire terminologique*, en ligne : <http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=2075187>.
Voir notamment : *R.* c. *Vu*, *supra*, note 28, par. 46 et SEDONA CANADA, *supra*, note 26, p. 3 et p. 4.
69. Voir notamment : *Voltage Pictures LLC* c. *M. Untel et M^me^ Unetelle*, 2014 CF 161, par. 13.
70. Quant à la détermination de la date à laquelle de nombreux fichiers ont été copiés ou consultés, voir notamment : *IMS Health Canada Inc.* c. *Th !Nk Business*

(10 h 59) et des recherches sur les petites annonces pour une table à langer (11 h 19).[71]

B. Faut-il nécessairement les conserver ?

L'article 3 LCCJTI définit le document comme étant constitué d'information portée par un support. Il sera considéré comme un document technologique lorsqu'il sera un support faisant appel aux technologies de l'information.

La LCCJTI ne fait, à cet égard, aucune distinction quant à une quelconque catégorisation ou nature de l'information portée par le support. Elle ne traite pas non plus explicitement des métadonnées[72]. Elle précise uniquement que l'information que comporte un document doit :

> [...] y [être] délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et [être] intelligible sous forme de mots, de sons ou d'images.[73]

Dans la décision *R.* c. *Nde Soh*[74], laquelle traitait notamment de l'interprétation de l'article 31.8 de la *Loi sur la preuve au Canada*[75] qui définit les termes « document électronique »[76] et « données »[77], le tribunal souligne :

> À mon avis selon la définition [...] « document électronique » inclut tout ce qui se présente sous forme électronique, c'est-à-dire les courriels, tous les fichiers informatiques, les métadonnées concernant ces fichiers, l'historique de navigation, le contenu mis en ligne dans les forums Web tels que Twitter et Facebook, les messages textes,

---

Insights Ltd., 2013 QCCA 1303, par. 16 et *Maax Bath inc.* c. *Agostino*, 2013 QCCS 3646, par. 7. Voir également : *R.* c. *A.M.*, 2013 ONSC 6174, par. 7 à 16.

71. *Durocher-Lalonde* c *9096-0469 Québec inc.*, 2011 QCCRT 490, par. 16.
72. Nous reviendrons sur les articles 10 et 11 LCJTI dans les sous-sections B.1. et B.2.
73. Art. 3 LCCJTI. La loi souligne de plus que « [l]'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcriptibles sous l'une de ces formes ou en un autre système de symboles. »
74. 2014 NBBR 20, par. 21.
75. L.R.C. (1985), ch. C-5.
76. « Ensemble de données enregistrées ou mises en mémoire sur quelque support que ce soit par un système informatique ou un dispositif semblable et qui peuvent être lues ou perçues par une personne ou par un tel système ou dispositif. Sont également visés tout affichage et toute sortie imprimée ou autre de ces données. »
77. « Toute forme de représentation d'informations ou de notions. »

les clavardages en ligne, etc. ainsi que toute sortie imprimée de ces données. [...]. [Notre souligné][78]

Bien que cette décision traite de l'application d'une loi fédérale, force est d'admettre que la définition de « données »[79] comporte des similitudes avec celle d'« information » que l'on retrouve dans la LCCJTI. De ce fait, nous croyons que la notion d'information définie à l'article 3 LCCJTI comme, d'une part, étant délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et, d'autre part, étant intelligible sous forme de mots, de sons ou d'images, ne limite pas celle-ci qu'à l'information visible *de facto* au lecteur. Toute information, qu'elle soit visible ou non aux yeux du lecteur, respectant ces exigences doit être considérée comme faisant partie intégrante du document technologique[80].

Dans ce contexte, les métadonnées internes à un document technologique doivent, à notre avis, être considérées comme de l'information faisant partie intégrante du document auquel elles se rattachent[81], alors que les métadonnées externes à un docu-

78. Nous pouvons même être portés à croire que, selon l'énumération, notre souligné réfère aux métadonnées externes.
79. *Supra*, note 77.
80. Voir notamment : *Règles de procédure civile de la Nouvelle-Écosse*, Nova Scotia Civil Procedure Rules, Royal Gaz Nov 19, 2008 ; *Règlement sur les documents et informations électroniques*, DORS/2014-117. Voir aussi : *Desgagne* v. *Yuen et al.*, 2006, BCSC 955 et *Bishop* v. *Minichiello*, 2009 BCSC 358.
81. Au soutien de notre prétention, voir notamment Pierre TRUDEL, *supra*, note 12, p. 37. « Dans la mesure où les métadonnées sont générées du seul fonctionnement des outils logiciels ou autres qui permettent de générer un document, il est difficile d'imaginer au nom de quel principe elles devraient être considérées comme ne faisant pas partie du document. Cela paraît d'autant plus vrai que la Loi reconnaît, à l'article 4, qu'un document peut comporter de l'information fragmentée et répartie. » [Notre souligné]. Voir également : François SENÉCAL, *supra*, note 60, p. 123 et s. ; et François SENÉCAL et Gilles DE SAINT-EXUPÉRY, *supra*, note 12. L'auteur Éric DUNBERRY, *supra*, note 12, p. 20, est toutefois d'avis, en discutant des éléments qui distinguent le document technologique du document papier, que celles-ci ne font pas partie intégrante du document, ce avec quoi nous sommes respectueusement en désaccord. « Le quatrième élément distinctif concerne l'existence de données secondaires connues sous le vocable de métadonnées du fait qu'elles sont nécessaires à la définition du contexte ou de la structure du document électronique, au-delà de son contenu. Elles procurent des renseignements relatifs aux données d'un document électronique qui permettent leur utilisation pertinente sans pour autant faire partie intégrante de ce document, même si elles en sont extraites en partie. Les métadonnées lient le document à l'activité dont il émane et l'environnement qui l'a vu naître. Elles servent à l'identification, à la description et à l'administration du document électronique. [références omises]. » Il mentionne néanmoins, à la p. 110, que « [l]es messages de données, comprenant les métadonnées, doivent être archivés sans modification et pouvoir être récupérés, imprimés et lus, parfois suivant un format prédéterminé. [références omises] »

ment technologique forment en elles-mêmes un autre document technologique. Une altération ou une perte, intentionnelle ou non, des métadonnées internes pourra avoir un impact sur l'intégrité du document technologique et pourra affecter sa valeur juridique[82]. Toutefois, certaines nuances doivent être apportées eu égard à ces altérations ou pertes des métadonnées, notamment quant aux métadonnées structurelles[83]. Ces nuances font l'objet des prochaines sous-sections. Il convient néanmoins de souligner que tout comme l'information d'un document peut être modifiée, les métadonnées peuvent également l'être[84].

Basant notre réflexion sur la prémisse que les métadonnées internes font partie intégrante du document technologique auxquelles elles se rattachent et que les métadonnées externes constituent elles-mêmes un document technologique, il convient de se pencher sur la nécessité de les conserver dès lors que le document technologique auquel elles se rattachent fait l'objet d'une reproduction par l'un des deux modes prévus à l'article 2841 al. 1 C.c.Q., à savoir la copie (B.1.) et le transfert (B.2).[85]

---

82. Art. 5 LCCJTI.
83. Voir la note 19.
84. Quant à des métadonnées internes, voir notamment : *Order P2005-001*, 2006 CanLII 80853, par.15 ; *Richard* c. *Gougoux*, *supra*, note 9, par. 77 ; *Sécurité des Deux-Rives ltée.* c. *Groupe Meridian construction restauration inc.*, *supra*, note 8, par. 84 et 85 et *Ménard* c. *Société de transport de Montréal*, 2012, QCCRT 454, par. 129.
Quant à des métadonnées externes, voir notamment : *R.* c. *Plamondon*, 2006 QCCQ 14171, par. 27 ; et *R.* c. *Morelli*, 2010 CSC 8, par. 68.
Il importe par ailleurs de rappeler que l'article 21 LCCJTI énonce que « [l]orsqu'une modification est apportée à un document technologique durant la période où il doit être conservé, la personne qui a l'autorité pour faire la modification doit, pour en préserver l'intégrité, noter les renseignements qui permettent de déterminer qui a fait la demande de modification, quand, par qui et pourquoi la modification a été faite. Celle-ci fait partie intégrante du document, même si elle se trouve sur un document distinct. »
85. Sur la distinction entre les modes de copie et de transfert, voir notamment : Vincent GAUTRAIS et Patrick GINGRAS, *supra*, note 12, p. 29 ; Pierre TRUDEL, *supra*, note 12 et Vincent GAUTRAIS, *supra*, note 2.
Il importe de souligner que l'article 15 (4) LCCJTI offre une présomption d'intégrité à l'égard de toute copie effectuée par une entreprise ou l'État. Une telle présomption exempte donc un tiers de démontrer l'intégrité de la copie qu'il souhaite déposer en preuve à l'égard de l'entreprise ou de l'État. Toutefois, elle est seulement applicable à la copie et non au document résultant du transfert. La LCCJTI offre aussi une autre présomption à son article 33, laquelle s'applique tant à la copie qu'au, à notre avis, document résultant du transfert bien que la loi utilise le terme « exemplaire ». Ainsi, toute personne jouit d'une présomption d'intégrité à l'égard de tout exemplaire ou copie d'un document d'une entreprise ou de l'État qu'elle génère à partir d'un système, y compris un logiciel, mis à sa disposition par l'un d'eux. Enfin, quant à ces deux présomptions, tant l'entreprise que l'État pourraient les contester.

Comme nous le constaterons, bien que le législateur ait basé la valeur juridique des documents sur leur intégrité et qu'il ait prévu deux modes de reproduction, le transfert s'avère celui qui, de par sa nature, risque le plus d'apporter des changements à l'information. L'éclaircissement des limites, forcément grises, de ce qui constitue un changement permissif des métadonnées apporte certains questionnements, lesquels devront assurément faire l'objet de développements par la jurisprudence.

1. Le document technologique résultant d'une copie

En vertu de l'article 2841 al. 1 C.c.Q., la copie se définit comme étant la reproduction d'un document sur un support, à savoir le même ou un différent, qui ne fait pas appel à une technologie différente, c'est-à-dire un format technologique différent[86]. La copie se veut la « [r]eproduction d'un document source qui en conserve l'information et la forme »[87].

Outre la reproduction de l'information visible au lecteur et de ses métadonnées internes, c'est-à-dire de toute l'information du document, elle reproduit aussi intégralement sa forme, soit l'agencement de l'information du document technologique source – bref, il s'agit d'une copie à l'identique.

La copie se veut une duplication du document technologique source dans son format technologique natif sans aucun changement ni modification. Étant donné que le format technologique du document technologique source et du document technologique copié est le même, l'information s'avère elle aussi la même et ne subit aucune modification. En conséquence, une quelconque altération du contenu informationnel ou des métadonnées internes devra ainsi être considérée comme une atteinte à l'intégrité du document technologique résultant de la copie[88]. Rappelons qu'en

---

86. À cet égard, la notion de « format » nous paraît devoir être vue comme un sous-ensemble de la technologie. Sur cette question, voir : Vincent GAUTRAIS et Patrick GINGRAS, *supra*, note 12, p. 7.
87. SECRÉTARIAT DU CONSEIL DU TRÉSOR, *Glossaire*, en ligne : <http://www.tresor.gouv.qc.ca/en/information-resources/gouvernance-et-gestion-des-ressources-informationnelles/loi-concernant-le-cadre-juridique-des-technologies-de-linformation/glossaire/c/>.
88. Voir l'article 11 LCCJTI qui énonce « [qu'e]n cas de divergence entre l'information de documents qui sont sur des supports différents ou faisant appel à des technologies différentes et qui sont censés porter la même information, le document qui prévaut est, à moins d'une preuve contraire, celui dont il est possible de vérifier

vertu de l'article 2841 C.c.Q. al. 2, la copie doit être certifiée conformément à l'article 2842 C.c.Q.[89] pour pouvoir « légalement tenir lieu du document reproduit » qui remplit l'une des fonctions d'un original aux termes de l'article 12 LCCJTI.

Voici des exemples qui peuvent être considérés comme des copies en vertu de l'article 2841 C.c.Q. :

- Une photographie numérique en format JPEG enregistrée sur une carte mémoire amovible est reproduite et enregistrée dans le même format sur un disque dur ou un cédérom ;

- Un fichier de musique en format MP3 disponible sur un site Web est reproduit et enregistré dans le même format sur le disque dur d'un téléphone intelligent ;

- Un fichier en format XLS (Excel) enregistré sur une clé USB est reproduit et enregistré dans le même format sur une clé USB semblable ou un autre support ;

- Un courriel en format MSG reçu et enregistré dans une boite de courriels Outlook sur un disque dur est reproduit et enregistré dans le même format dans un répertoire du même disque dur ou sur une clé USB.

Afin d'être considéré comme une copie, le document technologique reproduit doit utiliser la même technologie, soit conserver le même format du document technologique source, et comporter la même information. Le contenu informationnel ainsi que toutes les métadonnées internes sont donc maintenus dans leur entièreté et ne sont pas altérés.

À la différence du document reproduit par l'entremise d'un procédé de transfert, la reproduction par un procédé de copie équivaut à une duplication complète et intégrale, tant de l'information

---

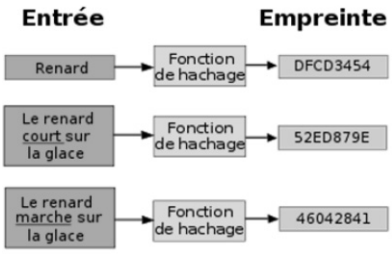
que l'information n'a pas été altérée et qu'elle a été maintenue dans son intégralité. » Par ailleurs, soulignons qu'en vertu de l'article 5 (3) LCCJTI « [l]e document dont le support ou la technologie ne permettent ni d'affirmer, ni de dénier que l'intégrité en est assurée peut, selon les circonstances, être admis à titre de témoignage ou d'élément matériel de preuve et servir de commencement de preuve, comme prévu à l'article 2865 du Code civil. »

89. Voir aussi l'article 16 LCCJTI.

que de la forme, du document technologique source. À cette fin, comme l'exige l'article 15 LCCJTI :

> [...] le procédé employé [pour réaliser la copie] doit présenter des garanties suffisamment sérieuses pour établir le fait qu'elle comporte la même information que le document source.

Rares sont les décisions qui ont traité de la nature des garanties suffisamment sérieuses que doit présenter un procédé permettant de réaliser une copie. Outre le témoignage de la personne ayant réalisé la copie d'un enregistrement audio du disque dur d'un ordinateur vers le disque dur d'un autre ordinateur[90], les tribunaux n'ont jamais eu, à notre connaissance, à porter leur attention sur ce que constituaient de telles garanties. Toutefois, eu égard aux pratiques utilisées dans le domaine, nous croyons que ces garanties peuvent être aisément rencontrées. Si l'utilisation d'outils spécialisés permet de documenter de façon claire l'exactitude et l'intégrité d'une



Source : <https ://fr.wikipedia.org/wiki/Fonction_de_hachage>

90. *B.L.* c. *Maison sous les arbres*, 2013 QCCAI 150. Il est intéressant de constater dans cette décision de la Commission d'accès à l'information que malgré une métadonnée erronée dans l'enregistrement audio copié, soit la date de création de l'enregistrement, la Commission admet celui-ci. Elle énonce notamment : « [...] Le problème de datation du document n'est pas suffisant en soi pour remettre en question l'intégrité du document qui a été copié de manière systématique avec les autres fichiers contenus sur l'ancien ordinateur portable du demandeur. Au surplus, les deux interlocuteurs ayant participé à cette conversation téléphonique étaient présents à l'audience et n'ont pas mis en doute que l'extrait entendu correspond à leur conversation originale. » De même, « [...] tenant compte de la souplesse de mise dans la conduite de l'audience devant la Commission, de l'utilisation circonscrite que souhaite faire le demandeur de cet élément de preuve et de la présence des deux interlocuteurs qui ont confirmé tant leur identité que leurs propos, la Commission admet en preuve l'extrait de la conversation téléphonique entendu lors de l'audience. ». Selon notre compréhension des faits, nous présumons que le problème de datation en question résulte plus précisément du fait que, à la suite de la copie de l'enregistrement audio sauvegardé sur un ancien ordinateur vers un nouvel ordinateur, l'enregistrement a été daté de l'année 1969. Il convient ici de préciser que le 1er janvier 1970 à 0h00:00 +0000 est le moment zéro de la computation des dates dans les systèmes UNIX – notre fuseau horaire -0500 nous ramenant la veille, soit en 1969. Il est probable que les métadonnées systèmes associées à l'enregistrement audio n'aient pas été copiées lors de la reproduction et ainsi que la date « par défaut », soit l'année 1969, ait été attribuée. À ce sujet, voir notamment : WIKIPÉDIA, « Heure Unix », en ligne : <http://fr.wikipedia.org/wiki/Heure_Unix>.

copie[91], de nombreux autres outils[92], souvent gratuits, peuvent procéder à pareille vérification en calculant puis en comparant la valeur de hachage du document source puis du document résultant de la copie[93]. Par ailleurs, les mécanismes de copie de fichiers intégrés aux systèmes d'opération comportent des mécanismes visant à prévenir les erreurs de copie[94].

Ainsi, la reproduction par le mode de la copie, c'est-à-dire en conservant le format du document source, s'avère, à notre avis, la façon la plus sûre pour recueillir et conserver les éléments de preuve technologiques et démontrer le maintien de leur intégrité[95].

---

91. Tels EnCase Forensic (https://www.guidancesoftware.com/products/Pages/encase-forensic/overview.aspx) et Forensic Toolkit (FTK) (http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk), dont l'utilisation a été étudiée dans plusieurs décisions américaines.
92. Pour des exemples de logiciels, voir notamment : WIKIPÉDIA, « List of file copying software », en ligne : <http://en.wikipedia.org/wiki/List_of_file_copying_software>.
93. « Le calcul d'une valeur de hachage permet par exemple de prendre l'« empreinte digitale » d'un document électronique. La valeur de hachage est constituée d'une suite de caractères alphanumériques obtenue par l'application d'une fonction mathématique. Chaque document a une valeur de hachage unique, et tout changement, aussi minime soit-il, dans le document modifie du tout au tout la valeur de hachage : « A given file will always have the same hash value ; it is the digital DNA of the file and cannot be altered. » [*R.* v. *Burke*, 2013 ONCA 424, par. 11]. En générant cette valeur de hachage en début de processus, il devient possible de démontrer l'intégrité des documents depuis le moment de la collecte. » François SÉNÉCAL et Gilles DE SAINT-EXUPÉRY, *supra*, note 12.
Au sujet de la fonction de hachage, voir notamment : WIKIPÉDIA, « Fonction de hachage », en ligne : <http://fr.wikipedia.org/wiki/Fonction_de_hachage>.
La valeur de hachage est fréquemment utilisée dans le cadre de poursuites judiciaires en matière de pornographie juvénile, et ce, afin d'identifier les fichiers contenant une telle pornographie. Voir notamment : *Baldwin Janzen Insurance Services (2004) Ltd.* v. *Janzen*, 2006 BCSC 554, par. 19 ; *R.* v. *Braudy*, 2009 CanLII 2491 (ON SC), par. 21 et 23 ; *R.* v. *Ahmad*, 2009 CanLII 84777 (ON SC), par. 92 ; *R.* v. *Carswell*, 2009 ONCJ 297, par. 200 ; *R.* v. *Beauchamp*, 2009 CanLII 64185 (ON SC), par. 398 et 399 ; *R.* v. *Wonitowy*, 2010 SKQB 346, par. 11 ; *R.* v. *Wainwright*, 2012 BCPC 123, par. 37 à 40 ; *R.* v. *Lorenz*, 2012 SKQB 293, par. 7 et *Kelly* v. *R.*, 2014 CanLII 67963. Dans cette dernière décision, l'expert de la défense souligne, au par. 49 : « [...] The purpose of these "hash values" is to ensure a secure chain of custody for digital media and that the image, as captured, has not been modified. Since digital media is a volatile medium and can easily be modified, MD5 or SHA 1 is used because the slightest change to that media, no matter how small, will result in these "hash" values being different. »
94. Un contrôle de redondance cyclique ou CRC (« *Cyclic Redundancy Check* ») est une fonction logicielle qui détecte les changements dans les blocs de données lors de la copie ou de la transmission. Voir notamment : WIKIPEDIA, *Cyclic Redundancy Check*, en ligne : <http://en.wikipedia.org/wiki/Cyclic_redundancy_check>.
95. Les processus de collecte juridico-technologique comprennent généralement la copie miroir, c'est-à-dire une copie exacte (identique) de l'ensemble des informations, de tous les supports collectés, afin de pouvoir recréer le système

2. Le document technologique résultant d'un transfert

En vertu de l'article 2841 C.c.Q., le transfert se définit comme étant la reproduction d'un document sur un support faisant appel à une technologie différente. Ce mode de reproduction se veut une opération qui permet d'associer une valeur juridique à un document lors de son passage d'une technologie à une autre, soit d'un format à un autre. Dans ce contexte, il appert que le transfert est beaucoup plus attaché à l'information elle-même, et semble, de ce fait, permettre des modifications de forme[96].

En vertu de l'article 2841 al. 2 C.c.Q., le document résultant du transfert de l'information doit être documenté conformément à l'article 2842 C.c.Q.[97] pour pouvoir « légalement tenir lieu du document reproduit » qui remplit l'une des fonctions d'un original aux termes de l'article 12 LCCJTI.

Voici des exemples qui peuvent être considérés comme des transferts en vertu de l'article 2841 C.c.Q. :

- Une photographie numérique en format JPEG enregistrée sur une carte mémoire amovible est reproduite et enregistrée dans le format BMP sur un disque dur ou un cédérom ;

- Une page Web en format HTML d'un site Web est imprimée sur une feuille de papier ou reproduite et enregistrée en format PDF sur un disque dur ;

---

informatique dans son ensemble. L'avantage est alors double : premièrement, les outils technologiques utilisés permettent de vérifier l'exactitude de la copie, permettant de documenter et d'établir le maintien de l'intégrité entre le moment de la collecte et la présentation de la preuve devant le tribunal et deuxièmement, toutes les métadonnées systèmes, soit celles externes aux documents, sont également préservées et permettent de reconstituer « l'histoire » du document. Les outils d'administration de la preuve électronique pourront alors associer ces métadonnées aux documents qu'elles concernent et les rendre directement disponibles aux personnes impliquées dans ces processus. Les outils technologiques de collecte, tels EnCase Forensic ou Forensic Toolkit (FTK), sont couramment utilisés à cette fin. À ce sujet, voir notamment : Dominic JAAR et François SENÉCAL, « L'administration de la preuve électronique au Québec ? » dans Service de la formation permanente du Barreau du Québec, *Développements récents et tendances en procédure civile*, Cowansville, Éditions Yvon Blais, 2010, vol. 320, p. 129, p. 158, en ligne : <http://edoctrine.caij.qc.ca/developpements-recents/320/368003842>.

96. Art. 10 LCCJTI. Voir notamment : *Lefebvre Frères ltée* c. *Giraldeau*, *supra*, note 9.
97. Voir aussi l'article 17 LCCJTI.

- Un fichier en format XLS (Excel) enregistré sur une clé USB est reproduit et enregistré en format PDF sur une clé USB semblable ;

- Un courriel en format MSG reçu et enregistré dans une boite de courriels Outlook sur un disque dur est imprimé sur une feuille de papier ou reproduit et enregistré en format DOC dans un répertoire du même disque dur ou sur une clé USB.

Le transfert permet la confection d'un nouveau document qui pourra remplacer le document source et même permettre sa destruction[98]. Toutefois, pour en autoriser sa destruction, le transfert devra être documenté. Cette documentation comprendra conformément à l'article 17 al. 2 LCCJTI, au minimum :

> [...] la mention du format d'origine du document dont l'information fait l'objet du transfert, du procédé de transfert utilisé ainsi que des garanties qu'il est censé offrir, selon les indications fournies avec le produit, quant à la préservation de l'intégrité, tant du document devant être transféré, s'il n'est pas détruit, que du document résultant du transfert.[99]

La documentation du transfert s'avère importante, car à défaut de la détenir, le document résultant du transfert n'aura pas la même valeur juridique que le document source advenant la

98. Art. 20 LCCJTI : « Les documents dont la loi exige la conservation et qui ont fait l'objet d'un transfert peuvent être détruits et remplacés par les documents résultant du transfert. [...] » ; et art. 18 : « Lorsque le document source est détruit, aucune règle de preuve ne peut être invoquée contre l'admissibilité d'un document résultant d'un transfert effectué et documenté conformément à l'article 17 et auquel est jointe la documentation qui y est prévue, pour le seul motif que le document n'est pas dans sa forme originale. » « Cela dit, au regard des articles 17 et 20, et même si cette condition est fortement à conseiller, il semble qu'elle ne soit obligatoire que lorsque le document transféré est par la suite détruit. Une documentation qui n'a pas nécessairement besoin d'être très élaborée, et ce, même si plusieurs standards techniques qui peuvent prévaloir dans certains cas le sont passablement plus. [Notes omises] » Vincent GAUTRAIS, *supra*, note 12, p. 145.

99. Le standard canadien en matière de numérisation, qui a surtout vocation à encadrer l'ensemble des étapes d'un programme de numérisation au sein d'une organisation, recommande la captation de nombreuses métadonnées : date et heure de la numérisation, nom de la personne effectuant la numérisation, identification ou localisation de l'appareil de numérisation et mention de toute modification apportée à l'image : Office des normes générales du Canada, *Microfilm et images électroniques – Preuve documentaire*, CAN/CGSB-72.11-93, 1993 (mieux connu sous son titre anglais « Microfilm and Electronic Images as Documentary Evidence »), partie I, art. 3.6 et partie III, art. 3.10.2.

destruction de ce dernier[100]. Ainsi, sous réserve des règles de preuve applicables, une partie pourrait donc s'opposer au dépôt en preuve d'un tel document[101]. Rappelons par ailleurs qu'en vertu de l'article 5 al. 3 LCCJTI :

> [Un] document dont le support ou la technologie ne permettent ni d'affirmer, ni de dénier que l'intégrité en est assurée peut, selon les circonstances, être admis à titre de témoignage ou d'élément matériel de preuve et servir de commencement de preuve, comme prévu à l'article 2865 du Code civil.[102]

Force est de reconnaître que, jusqu'à ce jour, les tribunaux ont généralement et aisément tendance à admettre en preuve un document technologique ayant été imprimé, et ce, bien qu'il s'agisse d'un transfert et qu'aucune documentation au soutien de celui-ci ne l'accompagne comme le veut l'article 2841 al. 2 C.c.Q. Certains admettent par ailleurs ces documents lorsque la preuve de la réalisation du transfert est apportée par témoignage[103]. Toutefois, il importe de souligner que, dans la majorité des situations, il n'y a aucune opposition au dépôt en preuve du document ayant fait l'objet d'une reproduction par le procédé de transfert. Cela ne saurait cependant justifier ou pallier le manque de documentation d'un transfert.

---

100. La documentation est obligatoire lorsque le document source est détruit et fortement utile dans tout autre contexte, puisque celle-ci pourra permettre de démontrer, conformément à l'article 11 LCCJTI, « [qu'e]n cas de divergence entre l'information de documents qui sont sur des supports différents ou faisant appel à des technologies différentes et qui sont censés porter la même information, le document qui prévaut est, à moins d'une preuve contraire, celui dont il est possible de vérifier que l'information n'a pas été altérée et qu'elle a été maintenue dans son intégralité. »

101. Cette obligation de documenter le transfert est l'évolution normale de l'obligation de documenter (déclarations assermentées) que l'on retrouvait autrefois dans le régime de la preuve par documents microfilmés de la *Loi concernant la preuve de certains documents de banque*, 12 Georges VI, c. 44 à la *Loi sur la preuve photographique de documents*, RLRQ, c. P-22. Voir François SENÉCAL, *supra*, note 60, note 147 : dans la décision *Banque Nationale du Canada* c. *Simard*, J.E. 96-1172 (C.Q.), des documents microfilmés ont été déclarés irrecevables car ils « ne port[aient] aucune mention de la nature du document et des lieux et date de leur reproduction et ce tel que prescrit à l'article 2842 ». Outre le défaut de documentation, les reproductions étaient de mauvaise qualité et illisibles.

102. Sur l'interprétation de cet alinéa, voir notamment : Claude FABIEN, « La preuve par document technologique », (2004) 38 *R.J.T.* 533, 578 ; et LCCJTI.ca « Article 5 – Développements sur l'alinéa 3 », en ligne : <http://lccjti.ca/article/article-5/>.

103. Voir notamment : *Commission des droits de la personne et des droits de la jeunesse* c. *Société de l'assurance automobile du Québec*, 2008 QCTDP 20, par. 54 à 56 et *Deslauriers Jeansonne, s.e.n.c.* c. *Panther Publications inc.*, *supra*, note 11, par. 4.

À la lumière des exemples de transfert présentés précédemment, on comprend que le transfert se veut une duplication du document technologique source vers un format technologique différent[104].

Quelles sont alors ces métadonnées qui peuvent être modifiées ou perdues, et ce, sans atténuer l'obligation juridique de maintenir l'intégrité d'un document technologique tout au long de son cycle de vie, tel que requis par l'article 6 al. 2 LCCJTI, et incidemment sa valeur juridique[105] ? Pouvons-nous limiter celles-ci qu'à certaines métadonnées spécifiques ?

L'article 10 LCCJTI visant notamment à permettre de pallier aux modifications susceptibles d'être apportées aux documents ayant été reproduits. Il crée ainsi une brèche à l'égard de la notion d'intégrité en permettant à des documents sur des supports différents[106] qui « présentent des différences en ce qui a trait à l'emmagasinage ou à la présentation de l'information » ou qui « comporte[nt] de façon apparente ou sous-jacente de l'information différente relativement au support ou à la sécurité de chacun des documents » d'avoir la même valeur juridique. Dans les faits, ces différences ne doivent pas être considérées comme portant atteinte à l'intégrité du document. Il en est par ailleurs de même eu égard aux différences « quant à la pagination du document, au caractère tangible ou intangible des pages, à leur format, à leur présentation recto ou verso, à leur accessibilité en tout ou en partie ou aux possibilités de repérage séquentiel ou thématique de l'information. »

L'objectif de cet article est de confirmer l'intégrité d'un document lorsque l'information qu'il porte est intacte, malgré le fait que celle-ci puisse être disposée autrement ou que les particulari-

104. Art. 10 LCCJTI.

105. Vincent GAUTRAIS souligne « [qu']un changement relatif aux métadonnées n'a pas pour conséquence systématique d'altérer l'information du document ; entendons l'information qui est l'objet même du document.. » Vincent GAUTRAIS, *supra*, note 2, par. 164. Voir aussi LCCJTI.ca, « Article 11 », 9 avril 2014, en ligne : <http://lccjti.ca/article/article-11/>.

106. Bien que le législateur utilise l'expression « sur des supports différents », nous sommes d'avis que l'article devrait plutôt s'appliquer à tout document ayant fait l'objet d'un transfert, soit d'un changement technologique, qu'il soit ou non sur un même support, tel un fichier en format DOC enregistré sur un disque dur qui est reproduit et enregistré en format PDF sur le même disque dur. Considérant que la copie ne nécessite pas de changement de technologie, il nous semble difficile, comme énoncé précédemment, de justifier une quelconque modification d'un document ayant fait l'objet d'une copie.

tés de son support varient. À ce titre, la présentation d'un courriel variera selon que celui-ci sera sauvegardé en format HTML, MSG, PDF ou PST. En deux mots et pour faire une analogie qu'apprécierait George Orwell, comme pour l'individu dans une société totalitaire, chaque document a droit à son style et à sa forme tant que l'information qu'il contient demeure la même[107].

Transposée aux métadonnées, nous croyons que cette disposition ne devrait viser que les métadonnées structurelles définies précédemment[108], soit des métadonnées intrinsèquement liées à la technologie du support, physique ou logiciel, du document et qui instruisent le logiciel, l'application ou le système quant à la façon d'interpréter le contenu du fichier pour le rendre intelligible au lecteur. Pensons par exemple au format PDF dont les spécifications techniques font l'objet d'un standard ISO[109]. La structure interne de l'information d'un tel fichier s'y trouve détaillée aux fins de son interprétation par un logiciel, une application ou un système. Les structures d'autres formats sont dites propriétaires et ne sont généralement pas connues, d'où la pertinence d'évaluer et d'utiliser, à des fins de pérennité, des formats documentés, ouverts, voire libres.

Il est effectivement dans la nature du transfert que de changer la structure logicielle du document ou, dans le cas de la numérisation, de détacher – de désencrer – l'information du papier qui la porte. La condition de ce changement de structure étant que le document résultant du transfert doit porter la même information. La documentation afférente au procédé de transfert utilisé doit justement venir établir comment ledit procédé de transfert main-

---

107. Jean-François DE RICO et Dominic JAAR, *supra*, note 12.

108. Voir la note 19. *Données de recherche du Canada* propose une définition similaire des métadonnées techniques, à savoir : « Les métadonnées techniques comprennent le titre des tableaux et des colonnes des bases de données physiques, les propriétés des colonnes et les propriétés des autres objets de la base de données, notamment la façon dont les données sont stockées. », *Termes et définitions*, 2015, en ligne : <http://www.rdc-drc.ca/fr/glossaire/>. Stephen MASON (éd.), *Electronic Evidence* (3d ed.), Butterworths, LexisNexis, 2012, p. 34 et s., propose d'autres exemples de métadonnées structurelles, soit des métadonnées relatives à l'encodage du fichier (type de fichier, méthode de compression et de chiffrement...), à l'interprétation du fichier (dépendances matérielles et logicielles...), à la structure du contenu (définition des sets de données, dictionnaire de données...) et à la source (les circonstances ayant mené à la saisie des données). Nous émettons cependant une certaine réserve quant à l'inclusion de cette dernière sous-catégorie parmi un ensemble résolument axé sur la technologie utilisée.

109. ISO 32000-1 :2008, *Document management – Portable document format*.

tient l'information du document source, quoiqu'elle fût, d'un point de vue du logiciel, organisée différemment.

Toute information autre que les métadonnées structurelles, directement visible ou masquée, doit être maintenue. En conséquence, les formules d'une feuille de calcul d'un tableur ou d'un fichier de gestion de projet, les métadonnées d'un courriel, les commentaires dans le code source d'un logiciel ou les balises méta[110] que l'on retrouve dans le code en langage HTML d'une page Web dépassent, à notre avis, le seuil de ce que l'article 10 LCCJTI définit comme des changements de forme[111].

Ainsi, si un document créé à partir d'un logiciel de gestion de projet comprend les informations afférentes au déroulement du projet et toutes les contraintes relatives aux délais, à la disponibilité des ressources, aux sous-tâches préalables, etc., il devient évident que ce document n'est pas qu'une représentation graphique du déroulement du projet, mais bien toutes les formules et la structure du projet qui y sont consignées. Ainsi, lorsque l'on veut expertiser une feuille de calcul d'un tableur ou un fichier de gestion de projet, c'est sa programmation qui est importante pour comprendre la structure du document ainsi que les divers liens entre les données. La complexité est telle que, contrairement à un fichier Word, il devient rapidement impossible d'en faire une rétro-ingénierie[112]. C'est donc cet outil que l'on souhaitera exper-

---

110. « Balise HTML insérée dans l'en-tête d'une page Web, après le titre, qui permet de décrire le contenu de la page afin de la référencer correctement et plus facilement dans les moteurs de recherche. » OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Grand dictionnaire terminologique*, en ligne : <http://www.grand dictionnaire.com/ficheOqlf.aspx?Id_Fiche=8373849>.

111. « Quelqu'un qui irait au-delà de ça, qu'un document qui serait modifié non plus dans sa forme ou dans ses différences de présentation, on pourrait à ce moment-là plaider qu'il y a atteinte à l'intégrité du document. » : Journal des débats de la Commission de l'économie et du travail, 36e législature, 1re session, 13 décembre 2000, en ligne : <http://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/cet-36-1/journal-debats/CET-001213.html>.

112. « Ensemble des opérations d'analyse d'un logiciel ou d'un matériel destinées à retrouver le processus de sa conception et de sa fabrication, ainsi que les modalités de son fonctionnement. » OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Grand dictionnaire terminologique,* en ligne : <http://www.grand dictionnaire.com/ ficheOqlf.aspx?Id_Fiche=26528543>.
Pour reprendre l'exemple présenté précédemment dans la sous-section I.A.1., est-ce que la cellule C1 de la feuille de calcul du tableur de l'illustration 1 affichant le chiffre 48, est le produit des cellules A1 et B1 (6 x 8), ou est-ce plutôt la cellule B1 affichant le chiffre 8 qui est le quotient de la cellule C1 divisée par la cellule A1 (48 ÷ 6) ?

tiser, car en pratique on ne peut expertiser le fonctionnement d'un moteur à l'aide d'une photographie de ce moteur !

Certaines décisions permettent de présenter ces raisonnements quant à la reproduction par transfert. Prenons par exemple la décision *Convectair NMT* c. *Ouellet Canada*[113] où il était question d'une concurrence déloyale par l'utilisation sans autorisation de la marque de commerce de la demanderesse dans les balises méta du site Web du défendeur[114]. Le litige est né lorsque la demanderesse Convectair constata que le site Web de la défenderesse apparaissait systématiquement dans les résultats des recherches Internet pour le mot « Convectair ». Or, « le texte du site www.ouellet.com ne faisait pas référence au mot « Convectair », mais seulement aux produits semblables à ceux de la demanderesse »[115].

La raison en est que le terme « Convectair NMT » apparaissait 44 fois dans le code source (en langage HMTL) de la page Web de Ouellet Canada, soit dans les balises méta. Cette information n'est pas affichée directement au lecteur sur la page Web, mais est facilement accessible dans le code source de la page[116]. Ainsi, si la page Web avait été imprimée sans ses métadonnées, celles-ci auraient été impossibles à retracer – bien que leur importance soit centrale dans le litige. Leur suppression aurait été bien plus qu'une simple atteinte à la forme du document, soit le seuil de l'article 10 LCCJTI, mais bien une atteinte au contenu informationnel du document à notre avis.

La pertinence des métadonnées, voire du format natif du document, a également été l'objet de la décision *Stadacona, s.e.c.* / *Papier White Birch* c. *KSH Solutions inc.*[117]. Dans cette décision, les formules, les ressources et les contraintes du fichier de gestion de projet ont été omises lors du transfert du fichier en format PDF. Dans cette décision, une requête afin d'obtenir les documents dans leur format natif a été rejetée au motif que la partie requérante avait accepté le document en format PDF, rendant ainsi impossible son expertise. L'absence de plaidoyer ou d'expertise

113. C.S. : 300-05-000018-997.
114. La décision est cependant interlocutoire et ne portait que sur le district où devait se dérouler le procès.
115. *Supra*, note 113, par. 4
116. Dans le fureteur Internet Explorer, on peut afficher le code en langage HTML d'une page Web en choisissant l'option « source » du menu « affichage ».
117. *Supra*, note 7. Voir la trame factuelle à la note 57.

relativement à la nature des documents technologiques est toutefois à noter.

Dans la décision *Lefebvre Frères ltée* c. *Giraldeau*[118], il était question de la récupération d'informations provenant de vieux agendas électroniques, dont les précédentes tentatives d'extraction par des techniciens s'étaient avérées infructueuses[119]. Bien que la fiabilité de ces informations fut mise en cause, le tribunal arriva à la conclusion que :

> [d]e la preuve examinée et entendue, le Tribunal est satisfait que les copies de relevés d'agendas électroniques produits sous la pièce D-27 sont complètes et reflètent fidèlement le contenu desdits agendas sur support électronique. Leur transfert sur papier reflète de façon adéquate les informations qui y ont été insérées.[120]

Malgré tout, et avec déférence pour le Tribunal, nous considérons que le transfert des relevés d'agenda n'a pas fait l'objet de la documentation prévue à l'article 17 LCCJTI ou alors la décision n'en fait pas mention expressément.

II. À quoi peuvent-elles servir : exemples d'application

Les métadonnées, qu'elles soient internes ou externes, peuvent être très utiles pour démontrer l'authenticité du document auquel elles se rattachent. Aux fins de la présente section et dans l'objectif de démontrer l'utilité des métadonnées, nous utilisons la conception classique de l'authenticité, décrite comme la preuve, à la fois, de l'intégrité de l'élément de preuve (II-A.) et le lien avec l'auteur (II-B.)[121].

---

118. *Supra*, note 9.
119. *Ibid.*, par. 75.
120. *Ibid.*, par. 83.
121. « L'authenticité implique [...] à la fois 1) un lien avec son auteur et 2) l'intégrité du document. » : Vincent GAUTRAIS, *supra*, note 2, partie 2, chapitre 2, section 1 : « De l'intégrité ». Cette conception est largement reconnue par la doctrine. Voir aussi : Léo DUCHARME, *Précis de la preuve*, 6e éd., Montréal, Wilson & Lafleur, 2005, nº 477 ; Jean-Claude ROYER et Sophie LAVALLÉE, *Droit de la preuve*, 4e éd., Cowansville, Éditions Yvon Blais, 2008, nº 357 ; C. FABIEN, « La preuve par document technologique », (2004) 38 *R.J.T.* 533, 571 ; Pierre TESSIER et Monique DUPUIS, « Les qualités et les moyens de preuve – L'écrit », dans École du Barreau du Québec, Collection de droit 2009-2010, vol. 2, *Preuve et procédure*, Cowansville, Éditions Yvon Blais, 2009, p. 257 ; Claude MARSEILLE et Raphaël LESCOP, « Règle de nécessité de l'original », dans *Preuve et prescription*, JurisClasseur Québec, Montréal, LexisNexis, 2008,

A. La démonstration de l'intégrité du document technologique

L'intégrité du document technologique est définie au premier alinéa de l'article 6 LCCJTI, lequel se lit comme suit :

> L'intégrité du document est assurée, lorsqu'il est possible de vérifier que l'information n'en est pas altérée et qu'elle est maintenue dans son intégralité, et que le support qui porte cette information lui procure la stabilité et la pérennité voulue.

L'intégrité d'un document est tributaire de la capacité du support de procurer à l'information une stabilité et une pérennité, ainsi que du caractère inaltéré et intégral de l'information qu'il porte. Si la condition relative au support s'avère présumée[122], la condition relative à l'information doit, quant à elle, nécessairement faire l'objet d'une preuve – preuve qui pourra le plus souvent, et le plus efficacement, être étayée par des métadonnées.

L'intégrité se prouve dans le temps. Tout au long du cycle de vie du document, il doit être possible de démontrer le maintien de l'intégrité de document[123]. Cette démonstration se fait par un faisceau d'indices, notamment des présomptions de fait, car il s'avère bien souvent difficile de remonter le temps jusqu'à la création du document, voire de déterminer avec précision les circonstances de sa confection. Ainsi, puisque les métadonnées sont bien souvent générées automatiquement et de façon contemporaine à la création du document, elles peuvent apporter un éclairage.

---

p. 21 ; Marie-Ève BÉLANGER, « Documents technologiques, copies et documents résultant d'un transfert », Fascicule 5, JurisClasseur Québec – *Preuve et prescription*, Montréal, LexisNexis Canada, 2008, par. 41. Dans le même sens : « Reconnaître la véracité ou l'exactitude d'un écrit dans son aspect matériel, c'est en reconnaître l'authenticité, c'est reconnaître que l'écrit émane bien de la personne qui en est apparemment l'auteur », *Desgagné-Bolduc* c. *Provigo Distribution inc.*, 2007 QCCS 3224, par. 106. Ces références sont citées dans François SENÉCAL et Gilles DE SAINT-EXUPÉRY, *supra*, note 12.

122. Art. 7 LCCJTI : « Il n'y a pas lieu de prouver que le support du document ou que les procédés, systèmes ou technologies utilisés pour communiquer au moyen d'un document permettent d'assurer son intégrité, à moins que celui qui conteste l'admission du document n'établisse, par prépondérance de preuve, qu'il y a eu atteinte à l'intégrité du document. » Ainsi, « [e]n aucun cas l'article 7 ne saurait constituer une présomption d'intégrité à l'égard d'un document technologique. » Voir aussi : Vincent GAUTRAIS et Patrick GINGRAS, *supra*, note 13.

123. Art. 6, al. 2 LCCJTI : « L'intégrité du document doit être maintenue au cours de son cycle de vie, soit depuis sa création, en passant par son transfert, sa consultation et sa transmission, jusqu'à sa conservation, y compris son archivage ou sa destruction. »

À titre d'exemple, certaines métadonnées que l'on retrouve dans certains formats de fichiers (ex : un document en format Word comprend des dates de modifications, de commentaires, etc.) peuvent être utiles. Certes, l'heure et la date sont celles de l'ordinateur (et, sauf en présence d'une mesure de sécurité mise en place par un administrateur système, un utilisateur peut la changer), ce qui n'est pas aussi fiable qu'une signature électronique horodatée par un tiers de confiance[124], mais ce risque n'amoindrit pas leur pertinence.

Certains cas sont également plus difficiles. Ainsi, puisqu'un courriel s'enrichit de métadonnées lors de sa transmission, le courriel que l'on trouve dans la boite « Éléments envoyés » de l'expéditeur ne comporte pas toutes ces métadonnées relatives à la transmission[125]. C'est possiblement dans les fichiers de journalisation des connexions des serveurs sortants qu'il faudrait aller vérifier les métadonnées afférentes à l'envoi d'un courriel – tout dépendra alors de la configuration dudit serveur et de la période de conservation des fichiers de journalisation. La situation probatoire idéale serait de retrouver à la fois dans le courriel et dans le fichier de journalisation d'un serveur, une métadonnée identifiant ledit courriel de façon unique. L'intervention d'un tiers de confiance (par exemple pour l'hébergement d'une pièce jointe, voire du message) pourrait aussi faciliter la démonstration de l'intégrité du courriel, voire même de l'authentification de l'expéditeur[126].

La décision *Sécurité des Deux-Rives ltée* c. *Groupe Meridian construction restauration inc*.[127] relate une action sur compte où la

---

124. « Opération qui consiste à dater un document électronique de façon fiable ». *Grand dictionnaire terminologique*, en ligne : <http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=8355557>.
125. Voir la note 51.
126. En effet, les protocoles de communication par courriel n'ont pas été conçus avec des préoccupations d'identification et d'authentification du message et de l'expéditeur. Voir notamment : *Hamilton* v. *Jackson*, 2009 BCSC 538, par. 17 : « Neither party tendered the electronic version of the email or any metadata relating to it. As this was not done in this case, I am left with conflicting versions as to what Ms. Galloway emailed to Mr. Jackson. It is possible to alter the text of an email. Ordinarily such alteration can be detected by a forensic review or simply by viewing the metadata of the email. Given the way in which emails are created and sent, I must exercise great caution in considering what they purport to contain. » De même, « [An] IP address does not identify the sender of the message. It identifies only a connection to a network, such as the internet. » *R.* v. *Moss*, *supra*, note 54, par. 41. Enfin, sur la question du « *email spoofing* », voir la note 54.
127. *Supra*, note 8.

question était de savoir si un avis de résiliation devant mettre fin aux services de la demanderesse avait effectivement été envoyé par la défenderesse. Le courriel que la défenderesse voulait faire admettre en preuve était une impression de celui-ci sur une feuille de papier du courriel, soit un transfert. Citant les articles 2839 C.c.Q. et 6 LCCJTI, le tribunal affirma que « [l]a preuve de l'intégrité du « document » se fera donc par la divulgation des métadonnées qui doivent être révélées sur le document et ce, indépendamment du type de support employé »[128]. Une preuve testimoniale par l'auteur présumé du courriel a néanmoins été présentée pour tenter de l'authentifier. Toutefois, nous croyons que :

> [...] ne disposant que de l'imprimé, d'une preuve testimoniale peu convaincante de la part de la défenderesse et du témoignage du directeur général de la demanderesse indiquant qu'il n'avait pas trouvé trace du courriel sur ses serveurs et soulignant les différences visuelles entre l'imprimé et les autres courriels envoyés par la défenderesse, c'est, à notre avis, à bon droit que le juge Massol a déterminé que la preuve de l'intégrité (et, partant, de l'authenticité) du courriel n'avait pas été faite.[129]

Dans l'hypothèse où l'admissibilité en preuve d'un courriel reçu était contestée, l'analyse des métadonnées contenues dans son en-tête serait, à notre avis cruciale[130], dans la détermination de son authenticité et de ce fait, le recours à la preuve testimoniale aurait été secondaire[131].

À cet égard, cette question a notamment été abordée dans la décision *Richard* c. *Gougoux*. Dans cette décision en matière de diffamation, des courriels litigieux ont fait l'objet d'une expertise à la suite de laquelle le Tribunal souligna :

---

128. *Ibid.*, par. 51.
129. François SENÉCAL, « Commentaire sur la décision *Sécurité des Deux-Rives ltée* c. *Groupe Meridian construction restauration inc.* – La contestation de la mise en preuve d'un courriel », *Repères*, décembre 2013, EYB2013REP1449, en ligne : <http://lccjti.ca/wp-content/uploads/2014/11/EYB2013REP1449.pdf>. Voir aussi : *GLP Paysagiste inc.* c. *Thibodeau*, *supra*, note 10.
130. Voir l'article 89(4) C.p.c. Par ailleurs, il importe de noter que cette disposition n'a pas été reprise dans le la *Loi instituant le nouveau Code de procédure civile*, 2014, chapitre 1. Voir aussi : François SENÉCAL, *supra*, note 2, p. 183 et s.
131. Voir par exemple : *Commission scolaire de la Beauce-Etchemin* c. *Syndicat du personnel de soutien de la commission scolaire de la Beauce-Etchemin*, *supra*, note 9 ; et *GLP Paysagiste inc.* c. *Thibodeau*, *supra*, note 10.

> À cet égard, le Tribunal a pris connaissance d'une preuve d'expertise exhaustive qui lui permet de conclure qu'il est scientifiquement difficile de retracer l'auteur réel d'un courriel. L'auteur peut facilement modifier, altérer et falsifier un courriel et on ne peut simplement pas se fier aux informations qui apparaissent à la face du document.[132]

Jugeant impossible la détermination de la paternité du courriel, le tribunal poursuivit son analyse des courriels litigieux selon d'autres moyens disponibles. « [P]uisqu'il est impossible d'établir la paternité desdits courriels sur une base purement scientifique, le Tribunal doit déterminer s'il existe des présomptions graves, précises et concordantes qui lui permettent de conclure par prépondérance de preuve sur l'origine et l'auteur des écrits en question. » Dans ce contexte, il devint ainsi pertinent à l'analyse que M. Richard avait accès aux serveurs d'une autre personne impliquée et qu'il aurait affirmé à un témoin « qu'il peut transmettre des courriels au nom d'autrui sans que quiconque puisse déceler qu'il s'agit d'un faux »[133].

Outre le risque de faux, la décision *Richard* c. *Gougoux* révèle, de façon bien plus importante, que l'obligation qui incombe à toute organisation de maintenir l'intégrité des documents qu'elle est tenue de conserver s'accompagne de l'obligation de maintenir l'intégrité des métadonnées relatives à ces documents[134]. Ainsi, « [s]i les métadonnées ne sont pas intègres, il deviendra difficile d'établir l'intégrité des documents eux-mêmes et, donc, de prendre une décision éclairée en se basant sur ceux-ci »[135].

---

132. *Supra*, note 9, par. 75.
133. *Ibid.*, par. 82 et 73.
134. Pour l'état du droit au Québec à ce sujet, voir : *Jacques* c. *Ultramar ltée*, 2011 QCCS 6020, par. 26 et Dominic JAAR et François SENÉCAL, *supra*, note 95. Soulignons par ailleurs que l'article 20 (1) de la *Loi instituant le nouveau Code de procédure civile*, 2014, chapitre 1, énonce que « Les parties se doivent de coopérer notamment en s'informant mutuellement, en tout temps, des faits et des éléments susceptibles de favoriser un débat loyal et en s'assurant de préserver les éléments de preuve pertinents. »
135. Nicolas VERMEYS, Julie M. GAUTHIER et Sarit MIZHARI, *supra*, note 12. Voir également : Mark PHILLIPS, « L'obligation de conservation des documents électroniques », dans Service de la formation permanente du Barreau du Québec, *Congrès annuel du Barreau 2007*, Cowansville, Éditions Yvon Blais, 2007, p. 27, en ligne : <http://edoctrine.caij.qc.ca/congres-du-barreau/2007/1731853504>.

Quoi qu'il en soit, la préservation de la valeur juridique d'un document nécessite que celui-ci soit conservé dans son format natif. À l'égard des courriels, l'utilisation des fonctions *Répondre* ou *Faire suivre* « entraîne généralement une perte ou une modification de l'en-tête message, ainsi que de la date et de l'heure de transmission. Un tel changement risque donc d'affecter directement la qualité de la preuve, voire son admissibilité »[136].

Les métadonnées des courriels sont donc d'une grande importance, si ce n'est parce qu'une forte proportion des documents technologiques mis en preuve à ce jour sont des courriels ayant fait l'objet d'un transfert sur une feuille de papier. Si elles semblent de prime abord

> inintelligibles, elles recèlent beaucoup d'informations qu'une expertise juridico-technologique permettra d'apprécier, si besoin est. Dans tous les cas, l'impression d'un courriel a pour effet d'atteindre son intégrité en détruisant ces métadonnées, qui (1) font partie intégrante du document technologique et (2) sont essentielles à la démonstration de son authenticité (puisque des informations relatives à l'auteur du courriel s'y trouvent également[137].

Relativement aux autres documents technologiques, les métadonnées permettent notamment d'identifier la date de création ou de dernière modification. Encore ici, s'il est possible que cette date soit altérée sans altération du document auquel elle est associée (ou l'inverse), il s'agit néanmoins d'informations éminemment pertinentes dans le cadre d'un litige[138]. Les métadonnées, à l'instar de certains éléments de preuve, ne créent pas de certitude absolue. Il s'agit d'informations venant établir un fait, pouvant à ce titre être contestées par tout moyen, notamment le témoignage[139]. Par exemple, une partie à un litige pourrait invoquer que les informations pertinentes se trouvent dans les systèmes de la partie adverse, mais ce n'est pas dans toutes les circonstances que le recours à des expertises juridico-technologi-

---

136. Patrick GINGRAS et Jean-François De RICO, *supra*, note 53, p. 435.
137. François SENÉCAL et Gilles DE SAINT-EXUPÉRY, *supra*, note 12.
138. « Cpl. Gallagher was able to determine from the metadata in the Samsung that the images of the handguns were created on October 9 and October 13, 2008 ». *R.* v. *Cater*, *supra*, note 40, par. 50.
139. Voir par exemple : *Bo* c. *Yuan*, 2014 QCCA 2259 ; et l'authentification par le décideur dans *Lemire et Garderie petits génies de Duvernay inc.*, 2014 QCCSST 277 (soulignons en tout respect la portée, à notre avis trop large, conférée par le tribunal à la présomption retrouvée à l'article 7 LCCJTI, dont nous avons traité précédemment).

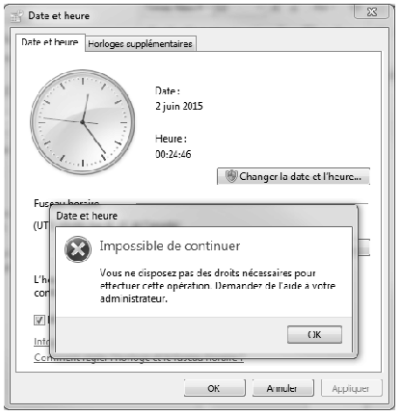
ques se justifie – la gestion d'instance et le principe de proportionnalité guideront alors les décisions à prendre[140].

Ainsi, dans le cadre de la Commission d'enquête sur le processus de nomination des juges, l'agenda d'un ancien ministre de la Justice retrouvé sur une disquette a fait l'objet d'une expertise juridico-technologique afin d'évaluer la fiabilité des documents qui y étaient enregistrés. Le rapport d'expert :

> [...] conclu[a] que les fichiers d'intérêt particulier « ont été modifiés pour la dernière fois respectivement le 2 octobre 2003 à 18 :08, et le 5 février 2004 à 17 :06 ». On a accédé à ces fichiers le 26 septembre 2010, mais ils n'ont pas été modifiés.[141]

En effet, en l'absence de mesures de sécurité propres visant à empêcher la modification de la date du système, ou en l'absence de sécurisation par un tiers, les métadonnées systèmes peuvent être contestables :

> La question de la fiabilité et de l'intégrité des dessins du palier 3103 réalisés à l'aide du logiciel AutoCAD a été abordée par M. Finnie, l'un des experts des défendeurs. Monsieur Finnie était d'avis que les métadonnées du dessin du palier 3103 révélaient que le fichier avait été créé le 27 septembre 1989. Monsieur Finnie a examiné aussi bien les métadonnées internes que les



140. Ces questions sont fréquentes dans les juridictions de Common Law, plus habituées au *discovery* que le Québec. Bien que les métadonnées internes soient reconnues comme faisant partie intégrante des documents technologiques au sein de ces provinces, les décisions traitent majoritairement de la pertinence de les communiquer ou non à l'autre partie dans le cadre d'un litige. Voir notamment sur la notion de pertinence et la règle de proportionnalité quant à la communication des métadonnées : *Park* v. *Mullin*, 2005 BCSC 1813 ; *483860 Ontario Inc.* c. *James Beaudoin*, 2010 ONSC 6294, par. 73 et s. ; *Frangione* v. *Vandongen et al.*, *supra*, note 55, par. 64 et s. ; *Warman* v. *National Post Company*, *supra*, note 23, par. 121 et 122 ; *Ravenda Homes Ltd*. c. *1372708 Ontario Inc.*, 2011 ONSC 4277 ; *Abougoush* v. *Sauve*, *supra*, note 39 ; *Fric* v. *Gershman*, 2012, BCSC 614 ; *Laushway* v. *Messervey*, *supra*, note 27, par 19 et s. ; *Laushway* v. *Messervey*, *supra*, note 27, par.31 et s. et *Conrod* v. *Caverley*, 2014, NSSC 35.

141. COMMISSION D'ENQUÊTE SUR LE PROCESSUS DE NOMINATION DES JUGES, *Rapport*, 19 janvier 2011, p. 137 (références omises), en ligne : <http://www.cepnj.gouv.qc.ca/rapport.html>.

> métadonnées externes correspondant aux fichiers pour en arriver à cette conclusion. Il a expliqué que la date créée qui apparaît dans les métadonnées correspond en fait à l'horloge de l'ordinateur. Monsieur Finnie a reconnu que, au début des années 1990, il aurait été facile de changer les réglages de l'horloge interne d'un ordinateur, mais les demandeurs n'ont renvoyé à aucun élément de preuve démontrant que les dessins avaient été falsifiés (outre la simple affirmation de Bill Wenzel). Il est par conséquent plus probable que le palier 3103 ait été conçu au cours de l'automne 1989, à savoir avant la date de revendication du 1er octobre 1990.[142]

Cependant, comme dans toute situation, il convient de faire preuve de discernement. Certaines métadonnées captées automatiquement peuvent être erronées. Les circonstances de la captation des métadonnées pourraient alors devoir être éclaircies :

> [...] il peut arriver que l'information enregistrée par l'ordinateur soit inexacte. Par exemple, lorsqu'un nouvel employé utilise un programme de traitement de texte afin de créer un mémorandum en utilisant un modèle créé par un ancien employé, les métadonnées peuvent indiquer erronément l'ancien employé comme l'auteur du nouveau mémorandum.[143]

B. L'établissement d'un lien entre un document technologique et une personne, un évènement ou une activité

À l'instar de l'intégrité, les métadonnées peuvent bien évidemment participer à la démonstration de la seconde composante de l'authenticité d'un élément de preuve – c'est-à-dire le rattachement à sa source et aux circonstances de sa confection ou de son utilisation. De ce fait, elles peuvent servir à l'établissement d'un lien entre un document technologique et une personne, un évènement ou une activité. À ce titre, les nombreux fichiers de journalisation générés automatiquement par un système d'exploitation peuvent se révéler fort utiles dans les enquêtes et dans l'établissement de faits importants dans un litige[144].

L'article 38 de la LCCJTI prévoit cette situation où un lien doit être fait entre un document et une personne.

---

142. *Wenzel Downhole Tools Ltd.* c. *National-Oilwell Canada Ltd.*, *supra*, note 19.
143. SEDONA CANADA, *supra*, note 26, p. 3 et p. 4.
144. Voir notamment les notes 66 à 70.

> Le lien entre une personne et un document technologique, ou le lien entre un tel document et une association, une société ou l'État, peut être établi par tout procédé ou par une combinaison de moyens dans la mesure où ceux-ci permettent :
>
> > 1° de confirmer l'identité de la personne qui effectue la communication ou l'identification de l'association, de la société ou de l'État et, le cas échéant, de sa localisation, ainsi que la confirmation de leur lien avec le document ;
> >
> > 2° d'identifier le document et, au besoin, sa provenance et sa destination à un moment déterminé.

En effet, « [c]'est souvent en établissant un lien entre une personne et un document qu'il devient possible d'attribuer les droits et responsabilités relatifs à ce document »[145].

À cet égard, les métadonnées, tel que nous l'avons mentionné précédemment, agissent alors comme un faisceau d'indices pouvant baser les prétentions d'une partie quant à ce lien entre un document. Ces métadonnées, souvent générées par les procédés ou moyens utilisés, prennent notamment la forme de traces laissées dans les logiciels, applications ou systèmes (par exemple des serveurs enregistrant des transactions), voire dans les documents (par exemple les en-têtes de courriels comportant des informations générées par les systèmes de messagerie).

La décision *Claro* c. *Lizarazo*[146] illustre bien une situation où ce type d'information aurait pu être utile. Dans cette affaire, la partie demanderesse a mis en preuve des courriels devant servir de commencement de preuve afin de pouvoir présenter une preuve testimoniale dans un litige de plus de 1500 $. Le commencement de preuve devant émaner de la partie envers qui on entend l'opposer[147], la partie défenderesse a émis une objection selon laquelle il n'avait pas été démontré que les messages en question émanaient bien d'elle citant à cet égard l'article 38 LCCJTI à son appui. C'est sur la foi de témoignages que le tribunal conclut que le défendeur était probablement l'expéditeur des messages et que

145. SECRÉTARIAT DU CONSEIL DU TRÉSOR, *LCCJTI annotée – article 38,* en ligne : <http://www.tresor.gouv.qc.ca/fr/ressources-informationnelles/gouvernance-et-gestion-des-ressources-informationnelles/loi-concernant-le-cadre-juridique-des-technologies-de-linformation/loi-annotee-par-article/loi-annotee-par-article-article-38/>.
146. 2012 QCCQ 710.
147. Art. 2865 C.c.Q.

ceux-ci ont admis en preuve[148]. Notons au passage que les métadonnées de ces messages électroniques auraient bien mieux convenu à la preuve relative à l'article 38 LCCJTI, par ailleurs cité par l'une des parties.

Un autre exemple d'application de cet article est présenté sur le site Web du Secrétariat du Conseil du trésor :

> Dans le monde bancaire, les contrats stipulent souvent que la présentation d'une carte et l'usage d'un numéro d'identification personnel pourront permettre d'établir le lien entre un individu et une transaction effectuée à un guichet automatique.[149]

En soi, l'article 38 LCCJTI ne prescrit pas quels éléments de preuve doivent être mis de l'avant (ni la façon de le faire) afin de former la base factuelle d'une conclusion quant à la provenance d'un document. Il comporte toutefois une finalité pédagogique visant à souligner que le recours à tout procédé ou moyen dans ce qui n'est ni plus ni moins que l'authentification des éléments de preuve, doit permettre les deux finalités que sont l'identification dudit document et l'identification de la personne, physique ou morale, dont il est prétendu qu'elle a un lien avec le document en question. Il y a toutefois une liberté dans le choix des moyens pour atteindre ces finalités. Il va sans dire que le niveau de certitude variera selon les moyens utilisés. À ce titre, l'identification d'une personne est plus certaine dans le cas de l'utilisation d'une signature faisant appel à une infrastructure à clé publique que dans le cas d'une enquête n'ayant pour indices qu'une adresse IP associée à une période de temps[150].

Ainsi, dans un premier temps, l'établissement d'un lien entre un document technologique et une personne relève entre autres de la question de la signature[151]. Si la signature peut prendre plu-

---

148. *Supra*, note 146, par. 21.
149. *Supra*, note 145.
150. À titre d'exemple, voir aussi : *Fafard* c. *Poirier*, 2010 QCCQ 11280, par. 16 et 17. Dans cette décision, en l'absence d'une adresse IP, une preuve circonstancielle, soit l'adresse de courriel elle-même, a notamment permis d'identifier l'auteur d'un acte illicite.
151. Art. 39 LCCJTI. « Quel que soit le support du document, la signature d'une personne peut servir à l'établissement d'un lien entre elle et un document. La signature peut être apposée au document au moyen de tout procédé qui permet de satisfaire aux exigences de l'article 2827 du Code civil.
La signature d'une personne apposée à un document technologique lui est opposable lorsqu'il s'agit d'un document dont l'intégrité est assurée et qu'au moment de la signature et depuis, le lien entre la signature et le document est

sieurs aspects, avec un degré de sécurité variable[152], la signature électronique avec certificat renferme de nombreuses informations supplémentaires au sein de celui-ci : date, autorité de certification, révocation du certificat, fonctions de la signature et limitations de l'autorisation de signer, valeurs de hachage, etc.[153].

Le certificat d'une signature électronique est un document technologique délivré par une autorité certifiant l'identité de la personne, physique ou morale, qui l'utilise. La confiance en l'autorité de certification viendra directement affecter la confiance quant à l'identité véritable du signataire[154]. Ainsi, un certificat créé par le signataire lui-même (un certificat dit autosigné) ne confère aucune confiance supplémentaire quant à l'identité du signataire, alors qu'un certificat émanant d'une autorité reconnue, telles l'infrastructure à clés publiques gouvernementale du gouvernement du Québec[155] ou Notarius[156], confère une plus grande confiance dans l'identité du signataire.

À ce titre, c'est la raison pour laquelle l'utilisation d'une signature électronique s'accompagne de mesures de sécurité pour protéger le certificat[157]. Cela a été souligné dans la décision *Notaires (Ordre professionnel des)* c. *Kanou*[158], où une notaire s'est vue

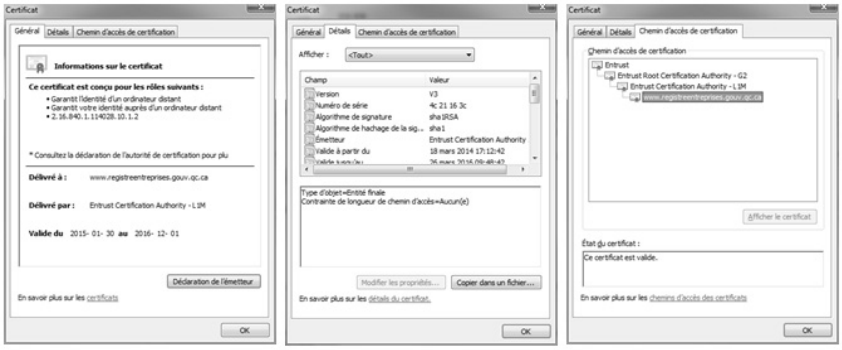
---

maintenu. », mentionné dans *Montréal (Ville de)* c. *Bolduc*, 2009 QCCM 185, confirmée par *Bolduc* c. *Montréal (Ville de)*, 2011 QCCA 1827. Sur la question de la signature, voir aussi : François SENÉCAL, « Chronique – La signature électronique en trois propositions », *Repères*, Septembre 2012, EYB2012REP1249, en ligne : <http://lccjti.ca/doctrine/senecal-f-chronique-la-signature-electronique-en-trois-propositions/>.

152. Pour une étude détaillée de la question, voir : CENTRE CANADIEN DE TECHNOLOGIE JUDICIAIRE, *Signatures numériques : recensement international sélectif des modèles déficients et performants*, août 2013, 24 p., en ligne : <http://wiki.modern-courts.ca/images/0/01/Signatures_num%C3%A9riques_-_Recensement_international_s%C3%A9lectif.pdf>.
153. Voir l'article 48 LCCJTI qui précise le contenu minimal d'un tel certificat. Voir les sections II et III du chapitre III de la LCCJTI portant respectivement sur les modes d'identification et de localisation et la certification.
154. Pour plus d'informations, voir : MINISTÈRE DE LA JUSTICE, Définitions et principes de base, en ligne : <https ://www.infocles.justice.gouv.qc.ca/?nav=rubrique[@nom=%27public%27]/rubrique[@nom=%27principes%27].
155. <https ://www.infocles.justice.gouv.qc.ca/>.
156. <https ://www.notarius.com/>.
157. Voir notamment les articles 41 et 58 LCCJTI.
158. 2014 CanLII 16662 (QC CDNQ). Voir par ailleurs, eu égard à la signature d'un avocat sur un acte de procédure*, Roussel* c. *Desjardins Sécurité financière, compagnie d'assurance-vie*, 2012 QCCQ 3835, où le tribunal énonce : « De plus, l'utilisation de la signature électronique ne dispense pas l'avocat de respecter ses obligations professionnelles à l'égard des procédures qu'il rédige. Le fait qu'un employé puisse apposer la signature plutôt que l'avocat lui-même ne modifie pas sa responsabilité professionnelle. »

radiée[159] pour une période de trois mois pour avoir partagé le mot de passe de sa signature électronique avec son adjointe.

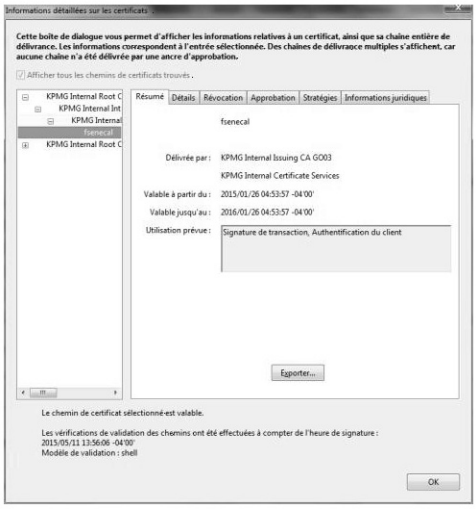
Ces informations quant au certificat de signature électronique sont aisément accessibles dans les documents en format natif. Par exemple, lorsque l'on visite le site Web du Registraire des entreprises du Québec (REQ), il est possible de s'assurer de l'identité du site en vérifiant son certificat. Cela permet de s'assurer que les documents affichés émanent véritablement du REQ.



Suivant ces mêmes informations, il est possible de créer des signatures électroniques dont l'apparence visuelle serait rigoureusement identique, mais dont les informations du certificat révèleraient la différence : il sera alors aisé de distinguer un certificat autosigné créé par le signataire d'un certificat émanant d'une autorité de certification réputée. Le premier revient à dire : « Faites-moi confiance pour vous dire qui je suis » et le second à dire « Vous faites confiance à un tiers réputé pour avoir validé mon identité préalablement à l'émission de mon certificat de signature électronique ». À titre d'exemple, dans un document au format PDF, cette information est accessible en cliquant sur une signature puis en affichant le certificat du signataire. Il devient

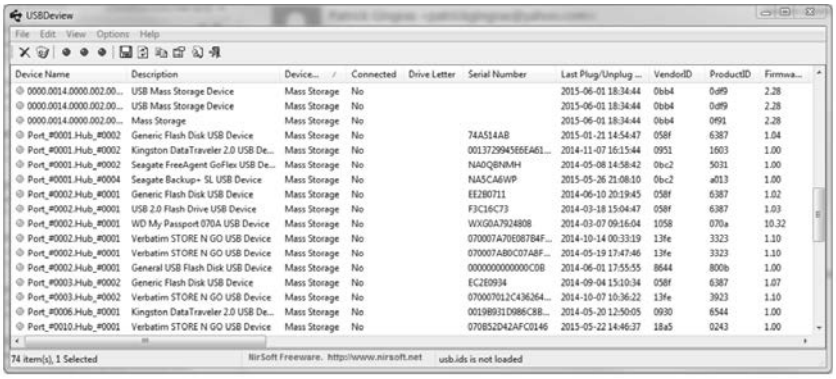
159. Le *Code de déontologie des notaires*, RLRQ, c. N-3, r. 2, énonce d'ailleurs que : « 41. Le notaire ne peut divulguer à quiconque tout code ou marque spécifique pouvant permettre l'utilisation de sa signature numérique ou, plus généralement, de tout autre moyen équivalent permettant de l'identifier et d'agir en son nom ».

ainsi possible de voir qui a délivré la signature électronique du signataire – une autorité de certification ou le signataire lui-même.



Dans un second temps, les métadonnées peuvent également documenter des événements ou activités rattachés à un logiciel, une application ou un système (d'autres éléments de preuve pourront rattacher ces événements à une personne). Ainsi, le système journalise les dates d'accès des différents utilisateurs, mais documente également certaines actions, par exemple le branchement d'un support amovible telle une clé USB. Des outils simples d'utilisation permettent de récupérer ces données où elles se trouvent sur le système, et une personne bien informée pourra les interpréter convenablement. L'illustration suivante présente un tel outil, listant les diverses clés USB et autres disques durs externes ayant été branchés dans un ordinateur, la date de branchement, leur nom et numéro de série et bien d'autres. La pertinence de ces informations ne ferait aucun doute dans des situations où un vol de documents confidentiels est allégué[160].

160. *IMS Health Canada Inc.* c. *Th !Nk Business Insights Ltd.*, *supra*, note 70 ; *Maax Bath inc.* c. *Agostino*, *supra*, note 70.



Les métadonnées deviennent alors de puissantes alliées lors d'enquêtes portant sur des actes illicites impliquant l'utilisation de systèmes informatiques, quels qu'ils soient. Elles orienteront l'enquête et leur recoupement pourrait permettre de faire le lien entre un document, telle une photographie publiée en ligne et l'adresse IP de la personne responsable de cette publication. Les données de connexion sur le serveur Web où se retrouve la photographie litigieuse comprendront peut-être l'adresse IP et le moment de la connexion. Ces informations pourraient permettre de retracer, auprès du fournisseur de services Internet propriétaire de l'adresse IP en question, le responsable de l'abonnement utilisant cette adresse IP au moment de la publication de l'image. L'enquête devra par la suite être complétée, puisque :

> [ces informations] déterminent uniquement qui est la personne responsable de l'abonnement auprès de cet intervenant[161]. Par conséquent, si le détenteur du compte est un père de famille, mais que celui-ci réside avec sa conjointe et ses trois enfants, l'auteur de l'acte illicite n'est pas nécessairement le père[162]. À l'opposé, si le détenteur du compte réside seul, les doutes pourront peut-être être plus fondés envers celui-ci.[163],[164]

De nombreuses informations pourront également être retrouvées sur l'ordinateur de l'auteur lui-même[165]. Pensons

161. *Pelchat* c. *Duchesneau*, 2006 QCCQ 5569 ; et *M.M.* c. *Société de l'assurance automobile du Québec*, 2011 QCCAI 112 (citées dans le texte).
162. Voir, par exemple, *R.* c. *Tremblay*, 2011 QCCQ 2146 (citée dans le texte).
163. *A* c. *B*, *supra*, note 52 (citée dans le texte).
164. Patrick GINGRAS et Nicolas W. VERMEYS, *supra*, note 12.
165. Voir par exemple *R.* c. *Girard Lévesque*, 2015 QCCQ 4509, par. 113 : « Pourtant, la perquisition survenue le 18 décembre 2012, de son téléphone dit intelligent, de sa tablette électronique, et de son ordinateur ont permis de retrouver

notamment à la mémoire cache et aux fichiers de journalisation de consultation des sites Web :

> ces informations, lorsqu'elles sont disponibles, peuvent être utilisées afin de retracer les activités effectuées par l'utilisateur d'un ordinateur sur Internet, et ce, à partir d'un dossier généré automatiquement par le navigateur, bien souvent à l'insu de l'utilisateur.[166]

Ces informations sont usuellement fort utiles dans le cadre d'enquêtes et ont été centrales à plusieurs poursuites, notamment en droit du travail[167].

CONCLUSION

Souvent subrepticement enregistrées et obscures, mais ô combien révélatrices et nombreuses, les métadonnées font partie du médium technologique, lequel est toujours plus présent dans notre quotidien. D'informations supplémentaires à fragments d'indices laissés sur notre passage, elles prennent plusieurs formes. Comme point de départ quant à l'étude de nombreux aspects juridiques qui y sont reliés – que ce soit la preuve civile ou le droit au respect de la vie privée – le juriste doit prendre acte de leur existence, s'enquérir de leur portée et de l'information qu'elles véhiculent, puis saisir l'opportunité d'en enrichir son travail dans l'objectif de toujours mieux conseiller son client. Ainsi, tout juriste pourra alors dire à la métadonnée qui elle est réellement, et celle-ci ne pourra plus jamais dire qu'elle est une incomprise ni une mal aimée.

---

notamment l'utilisation des courriels [...]@hotmail.com, [...123]@hotmail.com et de retracer notamment des preuves d'accès au profil sur réseau social électronique non seulement de X, mais aussi de A et de Z. »
Cette information peut également être retrouvée chez des tiers. Dans le même paragraphe de cette même décision : « De la même façon, l'extraction des données de réseau social électronique de J démontre que l'accusé a eu de longues conversations avec celle-ci. ». Sur les méthodes procédurales pour l'obtention de la preuve dans ces cas, voir Patrick GINGRAS et Nicolas W. VERMEYS, *supra*, note 12, p. 77 et s.

166. Patrick GINGRAS et Éloïse GRATTON, *supra*, note 12. L'article note en outre que le juriste doit se méfier des analogies quant à ces informations : « comme le souligne la Cour suprême, "les renseignements de ce genre ne possèdent pas d'équivalents dans le monde concret qui est celui des autres types de contenants." *R.* c. *Vu*, 2013 CSC 60. »

167. *Ibid.*, p. 42 à 47.

GLOSSAIRE

Les définitions qui suivent sont issues du Grand dictionnaire terminologique de l'Office québécois de la langue française*.

Adresse IP : Adresse numérique qui identifie de façon unique un ordinateur connecté au réseau Internet et en permet la localisation.

Balise méta : Balise HTML insérée dans l'en-tête d'une page Web, après le titre, qui permet de décrire le contenu de la page afin de la référencer correctement et plus facilement dans les moteurs de recherche.

Base de registre : Base de données qui répertorie l'ensemble des paramètres de configuration du système d'exploitation, sur les ordinateurs équipés de Windows.

Cache (mémoire) : Mémoire ou partie de mémoire dans laquelle sont stockés de façon temporaire les données ou les programmes les plus fréquemment ou les plus récemment utilisés, que l'ordinateur peut interroger afin de réduire les temps de réponse.

En-tête de message (de courriel) : Partie d'un courriel où sont notamment consignés les renseignements spécifiant l'identité du destinataire, celle de l'expéditeur ainsi que l'objet du message et la date de rédaction.

Fichier de journalisation (journal informatique) : Relevé chronologique des opérations informatiques, constituant un historique de l'utilisation des programmes et des systèmes sur une période donnée.

* Disponible en ligne : <http://www.granddictionnaire.com/>.

Fichier de journalisation (fichier journal) : Fichier texte dans lequel est emmagasinée, par le serveur gérant un site Web, chacune des requêtes qui lui ont été adressées, qui permet de mesurer ainsi le volume de transactions informatiques sur le serveur.

Fichier de témoins (« *cookies* ») : Fichier créé dans l'ordinateur de l'internaute par le navigateur et rassemblant les témoins persistants issus de la visite de sites Web.

Format natif : Format d'origine, non émulé, conçu pour une plateforme donnée.

Fournisseur de services Internet : Entreprise reliée en permanence au réseau Internet, et qui met à la disposition de particuliers ou d'entreprises des connexions leur permettant d'accéder aux différents services disponibles dans Internet.

Hachage : Opération qui consiste à appliquer une fonction mathématique permettant de créer l'empreinte numérique d'un message, en transformant un message de taille variable en un code de taille fixe, en vue de son authentification ou de son stockage

Historique de navigation (histoire) : Fonction d'un navigateur, qui conserve automatiquement et pour une période de temps paramétrable, la liste complète des adresses Web des sites visités durant les sessions de navigation.

Horodatage : Opération qui consiste à dater un document technologique de façon fiable.

Infrastructure à clé publique (ICP) : Système de gestion des clés de chiffrement et des certificats numériques, permettant de sécuriser les transactions électroniques et les échanges d'information confidentiels effectués, à l'aide de clés publiques, sur les réseaux ouverts comme Internet.

Langage HTML : Langage de balisage de texte qui permet la création de documents hypertextes affichables par un navigateur Web.

Nom de domaine : Libellé alphabétique associé à une adresse IP et identifiant un ordinateur ou un groupe d'ordinateurs reliés à Internet.

Protocole SMTP : Protocole de communication TCP-IP utilisé pour les échanges de courrier électronique dans Internet.

Rétro-ingénierie : Ensemble des opérations d'analyse d'un logiciel ou d'un matériel destinées à retrouver le processus de sa conception et de sa fabrication, ainsi que les modalités de son fonctionnement.

Serveur de courrier électronique : Serveur qui a pour fonction de recevoir et de délivrer les messages électroniques que s'envoient les différents utilisateurs d'un réseau.

Service de messagerie électronique : Service de transmission de messages géré par ordinateur, fournissant aux utilisateurs autorisés les fonctions de saisie, de distribution et de consultation de messages.

Système de localisation GPS : Système de localisation qui permet, à un moment précis, de déterminer une position géographique en se servant de signaux émis par des satellites, placés en orbite autour de la Terre, vers un appareil récepteur situé sur le site à localiser.

Usurpation d'adresse IP (« *IP spoofing* ») : Technique qui consiste à usurper l'identité d'un autre utilisateur du réseau en utilisant son adresse IP, ce qui permet de faire croire que la connexion provient d'un compte d'utilisateur autorisé.