Document generated on 04/18/2024 8:32 p.m.

Revue du notariat

LA SÉCURITÉ DES ACTES NOTARIÉS DÉMATÉRIALISÉS

Nicolas Vermeys and Dahlia Chalati

Volume 120, Number 3, 2018

URI: https://id.erudit.org/iderudit/1061829ar
DOI: https://doi.org/10.7202/1061829ar

See table of contents

Publisher(s)

Éditions Yvon Blais

ISSN

0035-2632 (print)
2369-6184 (digital)

Explore this journal

Cite this article

Vermeys, N. & Chalati, D. (2018). LA SÉCURITÉ DES ACTES NOTARIÉS DÉMATÉRIALISÉS. *Revue du notariat*, *120*(3), 479–555. https://doi.org/10.7202/1061829ar

Tous droits réservés © Nicolas Vermeys et Dahlia Chalati, 2019

This document is protected by copyright law. Use of the services of Érudit (including reproduction) is subject to its terms and conditions, which can be viewed online.

https://apropos.erudit.org/en/users/policy-on-use/

This article is disseminated and preserved by Érudit.

Érudit is a non-profit inter-university consortium of the Université de Montréal, Université Laval, and the Université du Québec à Montréal. Its mission is to promote and disseminate research.

https://www.erudit.org/en/

LA SÉCURITÉ DES ACTES NOTARIÉS DÉMATÉRIALISÉS

Nicolas VERMEYS* et Dahlia CHALATI**

INTRODUCTION 481

1. La sécurité des actes notariés – État des lieux 485

1.1 Les fondements de la sécurité de l'information. . . . 485

1.1.1 La disponibilité 487

1.1.2 L'intégrité 488

1.1.3 La confidentialité. 489

1.1.4 L'authentification 492

1.1.5 L'irrévocabilité 492

1.2 Analyse des mesures de sécurité actuellement mises en œuvre par les notaires 494

1.2.1 Le papier. 496

1.2.2 La minute 499

1.2.3 La signature manuscrite 502

1.2.4 L'encre 506

* Professeur à la Faculté de droit de l'Université de Montréal, chercheur au Centre de recherche en droit public (CRDP) et directeur adjoint du Laboratoire de cyberjustice. Le présent article reprend le contenu d'une étude produite par les auteurs grâce à une subvention obtenue de la Chambre des notaires.

** Notaire à Montréal.

1.2.5 Le sceau 510

1.2.6 Le greffe du notaire 512

1.2.7. Le répertoire et l'index du répertoire 514

2. La sécurité des actes notariés dématérialisés – projections 517

2.1 Les risques pour la sécurité des actes notariés dématérialisés 517

2.1.1 Les risques relatifs à la disponibilité des actes notariés dématérialisés 518

2.1.2 Les risques relatifs à l'intégrité des actes notariés dématérialisés 523

2.1.3 Les risques relatifs à la confidentialité des actes notariés dématérialisés 524

2.1.4 Les risques relatifs à l'authentification des actes notariés dématérialisés 528

2.1.5 Les risques relatifs à l'irrévocabilité des actes notariés dématérialisés 531

2.2 Les solutions technologiques assurant un niveau de sécurité fonctionnellement équivalent aux mesures de sécurité actuellement mises en œuvre par les notaires 533

2.2.1 Le PDF/A 539

2.2.2 La signature électronique 544

2.2.3 Le greffe technologique. 548

2.2.4 La chaîne de blocs 552

CONCLUSION 554

INTRODUCTION

En 1989, dans un article publié dans la *Revue du notariat*, Jean Martineau rappelait qu'un notaire n'a besoin que d'un cerveau, d'une machine à écrire, d'une plume et d'un sceau pour exercer sa profession[1]. Au sujet de la plume, il précisait : « [l]es notaires qui signent leurs actes, ou font signer leurs actes, avec un stylo à bille de dix-neuf cents doivent se graver dans la mémoire, qu'il n'est ni sage, ni prudent de procéder ainsi »[2]. Si cette affirmation peut surprendre un notaire ayant entrepris sa pratique au cours des dernières années, rappelons que, bien que l'usage d'un « stylo à dix-neuf cents » constitue aujourd'hui une pratique répandue, il était tout à fait légitime de se questionner sur la qualité de l'encre contenue dans un instrument aussi peu dispendieux vu l'effet fatal que pourrait avoir l'encre évanescente sur la conservation des actes notariés.

Comme le passage de la plume au « stylo à dix-neuf cents », le virage technologique que se propose de prendre la Chambre des notaires[3] implique le recours à une technologie « nouvelle » (tout au moins au sein de la profession) dont les effets à long terme sont nécessairement méconnus des membres. Il est donc tout à fait compréhensible que certains d'entre eux soient envahis par un sentiment d'angoisse et d'insécurité à l'idée de remplacer les actes notariés sur support papier par des « actes notariés dématérialisés »[4], c'est-à-dire de remplacer le papier chiffon par l'intangible, l'immatériel[5].

---

1. Jean MARTINEAU, « Sceau, stylo, dactylo et panonceau », (1989) 92-3-4 *R. du N.* 242.
2. *Ibid.*
3. CHAMBRE DES NOTAIRES DU QUÉBEC, « La profession notariale à l'ère du numérique », (2017) en ligne : <http://www.cnq.org/fr/60-0-salle-de-presse-la-profession-notariale-a-l-ere-du-numerique.html>.
4. Par l'expression « acte notarié dématérialisé » nous faisons référence à un acte notarié dont l'original est élaboré sur un support faisant appel aux technologies de l'information et « signé » par le notaire instrumentant, les parties, les témoins et (le cas échéant) les intervenants par le biais d'outils technologiques.
5. Sur la question de la dématérialisation, voir Dominique JAAR, « La valeur juridique du document numérisé », (2013) 22-1 *Entracte* 3 ; Didier FORGER, « Qu'avez-vous fait de mon contrat ? Je l'ai déposé au minutier central ! », (2013)

(à suivre...)

Afin d'atténuer ces craintes, il importe donc de procéder à une analyse des risques associés au virage technologique proposé, notamment quant à la sécurité des actes notariés dématérialisés. Bien qu'ils soient souvent exagérés, les risques découlant d'une migration vers le numérique sont bien réels. Il importe donc de les définir, de les mesurer et d'identifier le ou les outils technologiques susceptibles de les limiter à un niveau jugé acceptable. En effet, le risque zéro étant impossible à atteindre[6], il importe d'identifier le niveau de risque avec lequel les notaires et leurs clients sont à l'aise. Pour ce faire, il nous semble pertinent de qualifier les risques associés au processus existant puisque les technologies présentement utilisées telles que le papier, la minute, le sceau, l'encre, le greffe, le répertoire et l'index au répertoire comportent leur propre niveau de risque. Une analyse tripartie visant à identifier les objectifs sécuritaires de ces technologies, leur fonction et leur histoire s'avère donc pertinente. Dans un second temps, nous proposerons des solutions de rechange contemporaines à ces outils et procédés, en prenant soin d'identifier des technologies de l'information offrant un niveau de sécurité jugé soit « fonctionnellement équivalent », soit supérieur aux pratiques actuelles.

Ce principe d'équivalence fonctionnelle et son concept voisin de « neutralité technologique »[7] – lesquels sont au cœur de la *Loi concernant le cadre juridique des technologies de l'information*[8] – constituent, à notre avis, la pierre angulaire de toute migration numérique. En effet, comme nous venons de l'évoquer, une tendance se dessine suivant laquelle un environnement numérique exigerait plus de sécurité que son équivalent papier[9]. Pourtant, rappelons que « [l]a valeur juridique d'un document [...] n'est ni aug-

(...suite)
22-2 *Entracte* 3 et Jeffrey A. TALPIS, « Les actes notariés électroniques dans les États membres de l'Union internationale du notariat latin (UINL) : État de la question », (2010) 2 *C.P. du N.* 247.

6. À ce sujet, voir Nicolas W. VERMEYS, *Responsabilité civile et sécurité informationnelle*, Montréal, Éditions Yvon Blais, 2010, p. 14.
7. Sur ces notions, voir Vincent GAUTRAIS, *Neutralité technologique*, Montréal, Éditions Thémis, 2012.
8. RLRQ, c. C-1.1.
9. Par exemple, Alain Roy fait valoir que, « [a]vant qu'on ne puisse valablement remplacer le papier, il faudra disposer de moyens technologiques présentant des garanties à toute épreuve contre toute forme d'altération volontaire ou involontaire des données contenues à l'acte notarié ». Voir : Alain ROY, *Déontologie et procédure notariale*, coll. Répertoire de droit/Nouvelle série, Montréal, Chambre des notaires du Québec, 2002, p. 95. Pourtant, comme nous le verrons ci-après, les outils et procédés actuellement en place ne présentent pas de telles garanties.

mentée ni diminuée pour la seule raison qu'un support ou une technologie spécifique a été choisi » et que « [l]e document dont l'intégrité est assurée a la même valeur juridique, qu'il soit sur support papier ou sur un autre support, dans la mesure où, s'il s'agit d'un document technologique, il respecte par ailleurs les mêmes règles de droit »[10].

La dématérialisation des actes notariés est une idée qui accable les notaires depuis des décennies. En 1992, Jean Martineau posait déjà la question : « [l]a révolution informatique qui entraîne l'abandon de la feuille de papier et la signature électronique à distance, hors la présence du notaire, finira-t-elle par nous tuer » ? Il y répond succinctement : « Je le crois »[11]. À notre avis, toutefois, ce n'est pas la dématérialisation qui *tuera* la profession notariale, mais bien l'inertie quant aux changements technologiques. Comme le souligne William Dross, « le développement des nouvelles technologies de l'information a confronté le droit à de nouveaux défis, défis qui ont provoqué en retour une modification de ses règles »[12]. Toutefois, la simple adaptation directe et technique de la règle de droit n'est pas suffisante. Il importe en effet de se questionner sur les objectifs poursuivis avant de « forger des concepts nouveaux à même de saisir un phénomène nouveau »[13]. Dans le cas de l'acte notarié dématérialisé, l'adaptation technique de la règle de droit a été effectuée lors de la réforme de 2000[14], réforme par laquelle le législateur a reconnu que les actes notariés peuvent être reçus et conservés sur tout support permettant d'en assurer l'intégrité[15]. Près de 20 ans plus tard, on constate toutefois que cette réforme a entraîné peu d'adaptations pratiques et méthodologiques.

Notons que l'inhibition du cycle d'adoption n'est pas due aux exigences de la transposition du droit aux nouvelles technologies, mais plutôt à un certain immobilisme au sein des professions juridiques. Pourtant, nous sommes d'avis que le notaire ne peut promouvoir l'indispensabilité de son service et la prééminence des actes

---

10. Art. 5 de la *Loi concernant le cadre juridique des technologies de l'information*, préc., note 8.
11. Jean MARTINEAU, « Au fil des minutes », (1992) 95-3-4 *R. du N.* 211.
12. William DROSS, « L'encadrement des technologies par le droit : nécessité et source de changement », (2004) 106 *R. du N.* 341, 343.
13. *Ibid.*
14. *Loi sur le notariat*, RLRQ, c. N-3.
15. *Ibid.*, art. 35 et 39.

notariés lorsque son client se méfie de la désuétude des méthodes employées : des documents facilement reproductibles et falsifiables.

Cela étant, le notaire ne peut pas – non plus – migrer aveuglément vers le numérique sans prendre en compte les risques sécuritaires associés à un tel virage. La présente contribution vise donc à identifier ces risques dans l'absolu et à identifier les contre-mesures pouvant y répondre dans le respect des règles de droit propres à la profession notariale en général et aux actes notariés en particulier. En ce sens, elle vise à aiguiller la Chambre des notaires dans son rôle d'« établir des normes de sécurité relatives à l'utilisation des technologies de l'information pour la réception des actes notariés, y compris l'apposition des signatures en présence ou non du notaire instrumentant »[16].

Avant de procéder à l'analyse proposée, une dernière observation s'impose. Le virage numérique devrait être non seulement perçu comme une nécessité afin de permettre à la profession notariale de se moderniser[17], mais également comme une occasion de revoir les us et coutumes associées à la pratique ou, plutôt, à certains des outils autour desquels elle s'est développée (en l'occurrence, le papier)[18]. Par exemple, certains notaires remettent en question la pertinence de conserver divers actes, notamment les actes hypothécaires, après leur durée de vie utile. En effet, on s'interroge si « cela [vaut] la peine de traîner ces cadavres d'acte une carrière durant »[19] ? Évidemment, aucun notaire n'oserait détruire un acte d'hypothèque périmé ou un prêt quittancé, mais il demeure que la conservation matérielle de milliers d'actes nonobstant leur utilité est un fardeau très lourd pour un notaire, surtout lorsque

16. *Ibid.*, art. 98(5).
17. Comme l'explique Rémy Charras, « une profession ne doit pas s'affirmer moderne simplement parce qu'elle propose une signature des actes sur tablette électronique, ou investit dans la visioconférence afin de faciliter les rendez-vous longue distance. Une profession peut s'affirmer moderne après avoir mené une réflexion globale sur la connaissance, la recherche, l'innovation et après avoir accepté d'évoluer au gré du progrès, et de s'adapter ». Voir : Rémy CHARRAS, « Notaire VS. Blockchain », (2016) en ligne : <http://jurischain.com/notaire-vs-blockchain/>.
18. Sur cette question, voir : Nicolas VERMEYS et Karim BENYEKHLEF, « Premiers éléments d'une méthodologie de réformation des processus judiciaires par la technologie », dans Daniel LE MÉTAYER (dir.), *Les technologies de l'information au service des droits : opportunités, défis, limites*, Bruxelles, Bruylant, 2010, p. 209.
19. André DUVAL, « Considérations objectives sur l'avenir de la profession », (1972) 75 *R. du N.* 45.

celui-ci n'est pas rémunéré ou indemnisé pour son archivage. Ainsi, comme l'espace disque demeure peu coûteux, il est envisageable de simplement poursuivre cette pratique et d'en assumer les coûts puisque la technologie nous offre ici une solution bien plus économique que la construction d'une voute ignifuge. Toutefois, cette approche ne règle pas la problématique sous-jacente ; comme nous le verrons, elle créera même de nouveaux risques sécuritaires liés à la génération des mégadonnées[20] notariales. Il importe donc de ne pas simplement recréer l'existant en format numérique, mais bien de s'attarder à la pertinence de faire migrer certaines pratiques.

1. La sécurité des actes notariés – État des lieux

1.1 Les fondements de la sécurité de l'information

Avant de nous pencher sur la sécurité des actes notariés pour ensuite envisager l'équivalent fonctionnel technologique des mesures de sécurité présentement mises en œuvre par les membres de la profession notariale, encore faut-il nous entendre sur la notion même de sécurité, concept polysémique s'il en est un[21]. Or, pour définir ce terme, il importe d'identifier la qualification juridique de l'objet de cette obligation de sécurité, à savoir : l'acte notarié. Rappelons que l'acte notarié peut être décrit comme étant un « [a]cte authentique reçu ou attesté par un notaire compétent, selon les formalités requises par la loi »[22]. Il s'agit donc d'un écrit[23], soit un document[24] composé d'informations portées par un support[25]. Bref,

20. « L'ensemble des données produites en temps réel et en continu, structurées ou non, et dont la croissance est exponentielle ». OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Le grand dictionnaire terminologique*, 2017, « Mégadonnées », en ligne : <http://granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=26507313>.
21. Sur ce point, voir l'introduction à l'ouvrage de Karim BENYEKHLEF et Nicolas W. VERMEYS, *Le droit à la sécurité… La sécurité par le droit*, Montréal, Éditions Thémis, 2011.
22. Hubert REID, *JuriBistro eDictionnaire*, 2016, « acte notarié », en ligne : <https://dictionnaire reid.caij.qc.ca/recherche#q=acte%20notari%C3%A9&t=edictionnaire&sort=relevancy&m=search>.
23. En effet, l'acte authentique est défini comme étant un « [é]crit qui a été reçu ou attesté par un officier public compétent selon les lois du pays, avec les formalités requises par la loi ». Voir : H. REID, *ibid.*, « acte authentique », en ligne : <https://dictionnairereid.caij.qc.ca/recherche#q=acte%20authentique&t=edictionnaire&sort=relevancy&m=search>.
24. *Loi concernant le cadre juridique des technologies de l'information*, préc., note 8, art. 71.
25. *Ibid.*, art. 3.

l'acte notarié est constitué d'informations et ce sont ces informations dont la sécurité doit être assurée.

Selon l'Office québécois de la langue française, la sécurité de l'information se résume à la « [p]rotection des ressources informationnelles d'une organisation, face à des risques définis, qui résulte d'un ensemble de mesures de sécurité prises pour assurer la confidentialité, l'intégrité et la disponibilité de l'information traitée »[26] [nos soulignements]. Ces trois critères, lesquels sont notamment repris à l'article 26 de la *Loi concernant le cadre juridique des technologies de l'information*, constituent, selon une majorité d'experts[27], les piliers de l'obligation de sécurité de l'information. Toutefois, certains auteurs voient en cette triade une liste trop limitative[28]. Par exemple, selon la *Directive sur la sécurité de l'information gouvernementale*[29], les notions d'authentification et d'irrévocabilité devraient également être prises en compte[30], position qui, tout au moins en matière d'actes notariés, est validée par le législateur[31].

Ce sont donc ces cinq obligations : disponibilité (1.1.1), intégrité (1.1.2), confidentialité (1.1.3), authentification (1.1.4) et irrévocabilité (1.1.5), mieux connues collectivement sous l'acronyme DICAI, qu'il nous faut maintenant définir afin de mieux circonscrire l'obligation de sécurité relative à l'acte notarié « depuis sa création, en passant par son transfert, sa consultation et sa transmission, jusqu'à sa conservation, y compris son archivage ou sa destruction », soit durant son cycle de vie[32].

---

26. OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Le grand dictionnaire terminologique*, 2005, « Sécurité de l'information », en ligne : <http://granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=8358572>.
27. Pour un résumé des positions de ces experts, voir N.W. VERMEYS, préc., note 6, p. 23.
28. *Ibid.*, p. 31.
29. GOUVERNEMENT DU QUÉBEC, *Directive sur la sécurité de l'information gouvernementale*, Décret 7-2014 du 15 janvier 2014.
30. Notons que la définition d'« assurance de l'information », concept synonymique à celui de « sécurité de l'information » utilisé par le législateur fédéral dans la *Loi sur les systèmes de télédétection spatiale* (L.C. 2005, ch. 45), inclut également ces éléments : « 2. [...] assurance de l'information : Protection de l'information et des systèmes d'information au moyen de mesures en garantissant l'accessibilité, l'intégrité, l'authentification, la confidentialité et la non-répudiation ».
31. Voir notamment les articles 10, 11 et 43 de la *Loi sur le notariat*, préc., note 14.
32. *Loi concernant le cadre juridique des technologies de l'information*, préc., note 8, art. 6.

Avant de ce faire, il importe toutefois de préciser que ces obligations demeurent des obligations de moyens[33]. En effet, nous devons rappeler au lecteur que la sécurité parfaite demeure une utopie. Le notaire, tant dans la conservation de l'acte « papier » que de sa version technologique, devra donc mettre en œuvre les mesures de sécurité qu'un notaire « raisonnable » placé dans la même situation adopterait[34], sans quoi les coûts associés à la mise sur pied d'un greffe technologique deviendraient prohibitifs[35].

1.1.1 La disponibilité

Le principe de la disponibilité de l'information implique que les documents détenus par un notaire doivent être « accessibles dans les délais convenables pour les personnes autorisées à en disposer dès qu'elles le désirent »[36]. Pour le notaire, cette obligation est prévue à l'article 42 du *Code de déontologie des notaires* :

> Le notaire doit permettre à son client de prendre connaissance des documents qui le concernent dans tout dossier et, sous réserve de dispositions législatives incompatibles, d'obtenir copie de ces documents. Toutefois, le notaire doit refuser l'accès aux renseignements qui y sont contenus lorsque leur divulgation entraînerait vraisemblablement un préjudice grave pour le client ou pour un tiers.

Notons que si, comme le démontre la disposition ci-dessus, la disponibilité est conceptuellement liée à la notion d'accès, elle ne se limite pas à assurer le « droit d'accès » au sens de l'article 9 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*[37]. En effet, cette obligation vise plus largement à permettre la consultation d'un document à « toute personne habilitée à en prendre connaissance »[38] et non aux seules

33. Gabriel-Arnaud BERTHOLD, *La responsabilité civile du notaire*, Montréal, Wilson & Lafleur, 2017, p. 15.
34. Voir N.W. VERMEYS, préc., note 6, p. 118. Voir également *Roberge* c. *Bolduc*, [1991] 1 R.C.S. 374 : « La personne qui exerce une profession n'encourra donc pas de responsabilité à moins qu'elle n'ait agi d'une manière incompatible avec la conduite d'un professionnel raisonnable ».
35. Voir Nicolas W. VERMEYS, « Un modèle économique pour baliser l'obligation de sécurité informationnelle », dans Stéphane ROUSSEAU (dir.), *Juriste sans frontières – Mélanges Ejan Mackaay*, Montréal, Éditions Thémis, 2015, p. 471.
36. Joël HUBIN et Yves POULLET, *La sécurité informatique, entre technique et droit*, Namur, CRID, 1998, p. 7.
37. RLRQ, c. A-2.1, art. 9 : « Toute personne qui en fait la demande a droit d'accès aux documents d'un organisme public ».
38. *Loi concernant le cadre juridique des technologies de l'information*, préc., note 8, art. 26.

personnes qui en font la demande selon la méthode prescrite. Comme nous le verrons en deuxième partie, cette obligation impliquera, pour l'acte notarié technologique, celle de « voir à la disponibilité du matériel qui permet de le rendre accessible et intelligible et de l'utiliser aux fins auxquelles il est destiné »[39].

1.1.2 L'intégrité

L'intégrité est une « [p]ropriété associée aux données qui, lors de leur traitement ou de leur transmission, ne subissent aucune altération ou destruction volontaire ou accidentelle, et conservent un format permettant leur utilisation »[40]. L'article 6 de la *Loi concernant le cadre juridique des technologies de l'information* définit ce concept de la façon suivante :

> 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.[41]

Un document dont l'intégrité est compromise deviendra, dans bien des cas, inutilisable lors d'un litige[42] ou à des fins transactionnelles. C'est pourquoi l'article 19 de la *Loi concernant le cadre juridique des technologies de l'information* précise que « [t]oute personne doit, pendant la période où elle est tenue de conserver un document, assurer le maintien de son intégrité », obligation qui se situe d'ailleurs au cœur même de la *Loi sur le notariat* :

> **35.** [...] Les actes notariés en minute doivent être reçus et conservés sur tout support qui permet d'en assurer l'intégrité et qui est approuvé par règlement du Conseil d'administration. Ce support peut être différent selon qu'il s'agisse d'un projet d'acte ou d'un acte clos. Les ins-

39. *Ibid.*, art. 19.
40. OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Le grand dictionnaire terminologique*, « Intégrité des données », en ligne : <http://www.granddictionnaire.com/index.aspx> (consulté le 15 novembre 2015).
41. *Loi concernant le cadre juridique des technologies de l'information*, préc., note 8, art. 6. Cette définition est par ailleurs pratiquement identique à celle proposée au premier alinéa de l'article 2839 du *Code civil du Québec*, RLRQ, c. CCQ-1991 (ci-après « C.c.Q. ») : « L'intégrité d'un 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 ».
42. *Code de procédure civile*, RLRQ, c. C-25.01, art. 262.

criptions des actes doivent, au moment de la clôture de l'acte, être permanentes, sans lacune et être protégées contre les altérations.[43] [Nos soulignements]

1.1.3 La confidentialité

La confidentialité peut être définie comme étant la « [p]ropriété d'une information ou de renseignements personnels qui ne doivent pas être divulgués à des personnes ou à des entités non autorisées »[44]. En droit, l'obligation de confidentialité est prévue par divers textes législatifs[45] (notamment les articles 39[46] et 40[47] du *Code de déontologie des notaires*) et, lorsque le document visé est un document technologique, par l'article 25 de la *Loi concernant le cadre juridique des technologies de l'information*. Nous y reviendrons.

Il importe de souligner que les dispositions prévoyant une obligation de confidentialité limitent toutefois cette obligation à la protection des seuls renseignements « confidentiels », notion n'ayant à ce jour pas encore été définie en droit québécois ou canadien[48]. En

43. Notons que l'article 39 de la *Loi sur le notariat* (préc., note 14) est au même effet en ce qui concerne les actes notariés en brevet : « Les actes notariés en brevet peuvent être reçus sur tout support qui permet d'en assurer l'intégrité et qui est approuvé par règlement du Conseil d'administration. Les inscriptions des actes doivent, au moment de la clôture de l'acte, être permanentes, sans lacune et être protégées contre les altérations ».
44. OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Le grand dictionnaire terminologique*, « Confidentialité », en ligne : <http://www.granddictionnaire.com/index.aspx> (consulté le 15 novembre 2015).
45. Voir notamment les articles 67.2 et 125 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, préc., note 37 ; la *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ, c. P-39.1, art. 10 ; la *Loi sur les services de santé et les services sociaux*, RLRQ, c. S-4.2, art. 19 et s., etc. En fait, une recherche rapide sur le site du Canadian Legal Information Institute (www.canlii.org) nous permet de constater que la notion de confidentialité est prévue dans plus de 200 textes législatifs québécois, alors que le terme « confidentiel » se retrouve dans plus de 300 lois.
46. *Code de déontologie des notaires*, RLRQ, c. N-3, r. 2, art. 39 : « Le notaire ne doit pas faire usage de renseignements de nature confidentielle au préjudice d'un client ou en vue d'obtenir directement ou indirectement un avantage pour lui-même ou pour autrui ».
47. *Ibid.*, art. 40 : « Le notaire doit veiller à ce que toute personne dont il a la responsabilité dans l'exercice de sa profession ne communique à un tiers des renseignements confidentiels dont elle a pu avoir connaissance ».
48. *R.* c. *Stewart*, [1988] 1 R.C.S. 963, par. 33.

effet, outre certaines dispositions telles que l'article 23 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (lequel énumère une série de types de renseignements qui pourraient être considérés comme confidentiels dans certains cas[49]), ou l'article 39 de la *Loi sur les télécommunications*[50], les textes législatifs demeurent quelque peu nébuleux quant à la portée à accorder à cette notion. Sans nous plonger dans une analyse exhaustive des types d'informations qui peuvent, selon le contexte, constituer des renseignements confidentiels[51], nous nous limiterons à en énoncer les trois principales catégories, à savoir :

- Les renseignements personnels[52].

---

49. *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, préc., note 37, art. 23 : « Un organisme public ne peut communiquer le secret industriel d'un tiers ou un renseignement industriel, financier, commercial, scientifique, technique ou syndical de nature confidentielle fourni par un tiers et habituellement traité par un tiers de façon confidentielle, sans son consentement ». Notons que ce type de disposition se retrouve dans diverses autres lois québécoises. Par exemple, l'article 25 de la *Loi sur l'aquaculture commerciale*, RLRQ, c. A-20.2, traite de « renseignements industriels, financiers, commerciaux, scientifiques ou techniques de nature confidentielle ».
50. L.C. 1993, ch. 38. Cette disposition prévoit que peuvent être désignés comme des renseignements confidentiels les secrets industriels, les renseignements financiers, commerciaux, scientifiques ou techniques qui sont de nature confidentielle et qui sont traités comme tels de façon constante par la personne qui les fournit, ou les renseignements dont la communication risquerait vraisemblablement soit de causer à une autre personne ou elle-même des pertes ou profits financiers appréciables ou de nuire à sa compétitivité, soit d'entraver des négociations menées par cette autre personne ou elle-même en vue de contrats ou à d'autres fins. Une énumération quasi identique se retrouve également à l'article 20(1) de la *Loi sur l'accès à l'information* (L.R.C. (1985), ch. A-1).
51. Nous référons le lecteur à notre étude sur l'infonuagique pour une telle analyse. Nicolas VERMEYS, Julie M. GAUTHIER et Sarit MIZRAHI, *Étude sur les incidences juridiques de l'utilisation de l'infonuagique par le gouvernement du Québec*, Document de travail, Laboratoire de cyberjustice, 2014, en ligne : <http://www.cyberjustice.ca/publications/etude-sur-les-incidences-juridiques-de-lutilisation-de-linfonuagique-par-le-gouvernement-du-quebec/>.
52. Voir l'article 53 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, préc., note 37, lequel prévoit expressément que « [l]es renseignements personnels sont confidentiels ». Rappelons par ailleurs qu'un renseignement personnel peut être défini comme étant « tout renseignement qui concerne une personne physique et permet de l'identifier » ; voir aussi la *Loi sur la protection des renseignements personnels dans le secteur privé*, préc., note 45, art. 2.

- Les secrets industriels[53] ou commerciaux[54] et autres renseignements connexes[55].

- D'autres types de renseignements qui, selon l'individu auquel ils auront été communiqués (par exemple un notaire[56]), selon le contexte de cette communication (une séance de médiation[57]) ou selon le contexte de leur conservation (un dossier du tribunal de la jeunesse[58]), devront être protégés.

Bref, comme nous l'avons proposé ailleurs[59], peut être qualifié de « confidentiel » tout renseignement dont la loi interdit la divulgation volontaire ou involontaire à un tiers (à l'exception, dans certains cas, de la personne concernée) ou autorise la non-divulgation (notamment à des fins de sécurité nationale).

---

53. La notion de secret industriel n'est pas définie en droit québécois (voir *Merck Frosst Canada Ltée* c. *Canada (Santé)*, 2012 CSC 3, par. 105). Selon une publication de Santé Canada intitulée *Loi sur l'accès à l'information – Renseignements de tiers – Lignes directrices opérationnelles* (qui interprète donc la portée de cette notion au sens de la *Loi sur l'accès à l'information*, préc., note 50), pour être qualifiée de secret industriel, une information « doit être secrète dans un sens absolu ou relatif (c'est-à-dire qu'elle est connue seulement d'une ou de quelques personnes) ; le détenteur de l'information doit démontrer qu'il a agi avec l'intention de traiter l'information comme si elle était secrète ; l'information doit avoir une application pratique dans le secteur industriel ou commercial ; le détenteur doit avoir un intérêt (par exemple, un intérêt économique) digne d'être protégé par la loi ». Voir *Astrazeneca Canada Inc.* c. *Canada (Ministre de la Santé)*, 2005 CF 189, par. 64 et 65. Voir également *Société Gamma Inc.* c. *Canada (Secrétariat d'État)*, [1994] A.C.F. nº 589, par. 7 et 8 et *Merck Frosst Canada Ltée* c. *Canada (Santé)*, *ibid.*, par. 109.
54. « Information concernant des procédés de fabrication ou d'exploitation d'un produit que son bénéficiaire cherche à tenir confidentielle afin qu'elle ne soit pas divulguée à ses concurrents ». Hubert REID, *Dictionnaire de droit québécois et canadien*, 4e éd., Montréal, Wilson & Lafleur, 2010, p. 551. Pour une analyse jurisprudentielle de cette notion, voir : *R.L. Crain Limited* v. *R.W. Ashton & Ashton Press Mfg. Co. Ltd.*, [1949] 2 D.L.R. 481, par. 22 et s. (confirmée en appel : [1950] 1 D.L.R. 601).
55. Sont notamment visés certains renseignements financiers, commerciaux, scientifiques ou techniques. Voir, par exemple, l'article 23 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, préc., note 37. Pour une analyse exhaustive de ces différents types de renseignements, voir Raymond DORAY et François CHARETTE, *Accès à l'information : loi annotée, jurisprudence, analyse et commentaires*, Montréal, Éditions Yvon Blais, 2001, p. II/23 1 et s.
56. *Loi sur le notariat*, préc., note 14, art. 14.1.
57. *Loi sur les chemins de fer*, RLRQ, c. C-14.1, art. 19.
58. *Loi sur la protection de la jeunesse*, RLRQ, c. P-34.1, art. 96.
59. N. VERMEYS, J.M. GAUTHIER et S. MIZRAHI, préc., note 51.

1.1.4 L'authentification

La notion d'authentification peut se définir comme étant une « [p]rocédure consistant à vérifier ou à valider l'identité d'une personne ou l'identification de toute autre entité »[60]. En matière technologique, elle sera notamment utile « lors d'un échange électronique, pour contrôler l'accès à un réseau, à un système informatique ou à un logiciel »[61]. Ici encore, il s'agit d'une obligation intrinsèquement liée à la fonction même du notaire, dont le rôle est notamment d'« attester l'identité [...] d'une personne pour accomplir ou passer un acte juridique »[62].

En sécurité de l'information, on prévoit normalement que l'identification d'une personne pourra être établie à l'aide d'une ou de plusieurs catégories de facteurs : ce qu'une personne sait (mot de passe, combinaison, etc.), ce qu'elle possède (clé, carte d'accès, etc.) ou ce qu'elle est (biométrie[63])[64].

Ces mêmes catégories sont d'ailleurs reprises par le législateur à l'article 40 de la *Loi concernant le cadre juridique des technologies de l'information*, où il est prévu que « [l]a vérification de l'identité d'une personne peut aussi être effectuée à partir de caractéristiques, connaissances ou objets qu'elle présente ou possède ». Cela étant, la catégorie dans laquelle est inscrit un facteur d'authentification importe peu tant que le facteur permet « la vérification de l'identité ou de l'identification »[65] et que cette vérification soit faite « dans le respect des lois »[66].

1.1.5 L'irrévocabilité

L'irrévocabilité peut être définie comme la « [p]ropriété d'une action ou d'un document d'être indéniable et clairement attribué à

---

60. OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Le grand dictionnaire terminologique*, « Authentification », en ligne : <http://www.granddictionnaire.com/index.aspx>.
61. *Ibid.*
62. *Loi sur le notariat*, préc., note 14, art. 17. Voir également les articles 23 et 43 de la Loi.
63. Sur cette notion, voir Julie M. GAUTHIER, *Le droit de la biométrie au Québec : Sécurité et vie privée*, Montréal, Éditions Yvon Blais, 2015.
64. Shon HARRIS, *CISSP All-in-One Exam Guide*, 6e éd., New York, McGraw-Hill Education, 2012, p. 129.
65. *Loi concernant le cadre juridique des technologies de l'information*, préc., note 8, art. 40.
66. *Ibid.*

son auteur ou au dispositif qui l'a généré »[67]. Ce principe est donc lié à celui de la non-répudiation, soit l'idée de « [s]e prémunir contre le refus d'une personne de reconnaître sa responsabilité à l'égard d'un document ou d'un autre objet, dont un dispositif d'identification avec lequel elle est en lien »[68]. Notons que, bien que le législateur québécois ait notamment considéré la non-répudiation comme étant une propriété essentielle à protéger dans le cadre de la mise en œuvre du RDPRM[69], celle-ci n'est pas expressément prévue comme étant l'une des composantes de la sécurité de l'information selon la *Loi concernant le cadre juridique des technologies de l'information*[70]. Cette loi prévoit néanmoins :

> **38.** 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.

Qui plus est, si la *Loi concernant le cadre juridique des technologies de l'information* ne fait pas expressément référence à cette obligation, elle demeure au centre du rôle du notaire. En effet, les exigences prévues par les articles 52 et suivants de la *Loi sur le notariat* visent notamment à assurer l'irrévocabilité des actes.

---

67. GOUVERNEMENT DU QUÉBEC et SOUS-SECRÉTARIAT À L'INFOROUTE GOUVERNEMENTALE ET AUX RESSOURCES INFORMATIONNELLES, *Guide pour l'élaboration d'une politique de sécurité de l'information numérique et des échanges électroniques (pratique recommandée)*, version 1.0, Québec, SSIGRI, 2003, p. 36.
68. GOUVERNEMENT DU QUÉBEC, préc., note 29.
69. *Règlement sur le registre des droits personnels et réels mobiliers*, RLRQ, c. CCQ, r. 8, art. 15.1.
70. En effet, tel que nous l'avons déjà souligné, l'article 26 de la *Loi concernant le cadre juridique des technologies de l'information*, préc., note 8, semble limiter l'obligation de sécurité à ses trois principales composantes : intégrité, disponibilité et confidentialité.

1.2 Analyse des mesures de sécurité actuellement mises en œuvre par les notaires

Notre objectif étant d'identifier les mesures à mettre en œuvre afin d'assurer un niveau de sécurité raisonnable aux actes notariés dématérialisés, une question s'impose : que constitue un niveau de sécurité raisonnable en matière d'actes notariés ? Pour paraphraser les propos de la Cour suprême dans l'affaire *Roberge* c. *Bolduc*[71], il serait permis, afin de répondre à cette question, de se référer au niveau de sécurité assuré par une majorité de membres de la Chambre (bien que cela ne soit pas nécessairement déterminant)[72]. Or, comme la gestion des actes notariés dématérialisés en est encore au stade embryonnaire, peu de notaires ont mis en place une infrastructure technologique visant à assurer la sécurité de ces documents. Il est donc difficilement envisageable pour un notaire de s'inspirer des précautions prises par ses pairs. Comme nous le verrons dans la seconde partie du présent texte, il pourrait s'avérer utile de prendre en compte les choix effectués par les notaires d'autres pays ayant procédé à une certaine numérisation de leurs pratiques (en l'occurrence la France et l'Italie). Toutefois, certaines distinctions législatives limiteront nécessairement la portée d'une telle comparaison.

La question demeure donc entière : comment établir si les mesures de sécurité mises de l'avant par un notaire sont ou non « [compatibles] avec la conduite d'un professionnel raisonnable »[73] lorsqu'il n'existe aucune balise quant auxdites mesures ? Une réponse instinctive à cette question réside dans la création de ces balises par la Chambre. Cela implique toutefois une analyse de l'ensemble des solutions offertes par l'industrie. Une telle analyse étant difficile à effectuer, notamment puisque certains joueurs sont peu transparents quant aux limites de leurs outils, il est possible que de mauvais choix soient effectués. De plus, certaines technolo-

---

71. Préc., note 34.
72. « Il se peut fort bien que la pratique professionnelle soit le reflet d'une conduite prudente et diligente. On peut, en effet, espérer qu'une pratique qui s'est développée parmi les professionnels relativement à un acte professionnel donné témoigne d'une façon d'agir prudente. Le fait qu'un professionnel ait suivi la pratique de ses pairs peut constituer une forte preuve d'une conduite raisonnable et diligente, mais ce n'est pas déterminant. Si cette pratique n'est pas conforme aux normes générales de responsabilité, savoir qu'on doit agir de façon raisonnable, le professionnel qui y adhère peut alors, suivant les faits de l'espèce, engager sa responsabilité ». *Roberge* c. *Bolduc*, *ibid.*
73. *Ibid.*

gies pourraient être retenues non pas parce qu'elles correspondent aux besoins sécuritaires identifiés, mais parce qu'elles répondent à un sentiment d'insécurité ou à une mauvaise conception de la problématique.

Dans la même veine, l'une des principales erreurs commises par ceux et celles qui choisissent de prendre le virage numérique est d'envisager l'élaboration d'un cadre sécuritaire idéal[74], sans prendre en compte le cadre sécuritaire mis en œuvre pour le papier. En d'autres mots, il existe une tendance à la « sursécurisation » du numérique par rapport à son équivalent papier. L'exemple le plus éloquent de cette incohérence est fort probablement celui de la signature. En effet, la signature manuscrite est reconnue par divers experts comme étant l'une des méthodes d'identification et d'authentification les moins sécuritaires[75]. Pourtant, son « équivalent technologique » tel que perçu par les notaires, soit la signature numérique[76], constitue l'un des mécanismes les plus sécuritaires. Il existe donc une divergence majeure entre les niveaux de sécurité requis du papier et de l'électronique. Étant donné le changement de paradigme, une telle divergence peut s'avérer souhaitable. Il importe toutefois de s'assurer qu'elle est justifiée par les faits ou par un réel désir de profiter du changement technologique pour revoir des processus dépassés ou désuets[77], et non le fruit du phénomène de « sécuritisation »[78], soit l'adoption de mécanismes et de mesures

---

74. Voir par exemple A. ROY, préc., note 9, p. 95 : « le cadre technologique devra présenter une étanchéité totale. Comme nous l'avons déjà souligné, les stipulations de l'acte notarié bénéficient du secret professionnel. Or, on ne saurait permettre la rédaction et la conservation d'un acte notarié sur support informatique, s'il existe un risque d'intrusion ou d'infiltration du système informatique, si minime soit-il » [nos soulignements].
75. Robert SICILIANO, « Handwritten Signature Is Stupid Authorization », (2010) *Huffington Post*, en ligne : <http://www.huffingtonpost.com/robert-siciliano/handwritten-signature-is_b_379602.html>. Notons toutefois qu'il existe une exception à cette règle lorsque, comme c'est le cas pour les notaires, il existe un répertoire de signatures pour comparaison. Voir l'article 8(1) de la *Loi sur le notariat*, préc., note 14.
76. « Procédé d'identification du signataire d'un document électronique, basé sur l'utilisation d'un algorithme de chiffrement, qui permet de vérifier l'intégrité du document et d'en assurer la non-répudiation ». Voir : OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Le grand dictionnaire terminologique*, « Signature numérique », en ligne : <http://granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=8384641>.
77. Sur cette question, voir N. VERMEYS et K. BENYEKHLEF, préc., note 18.
78. Voir Barry BUZAN, Ole WAEVER et Jaap DE WILDE, *Security : A New Framework for Analysis*, Colorado, Lynne Rienner, 1998.

de sécurité visant à protéger contre une menace inexistante ou exagérée.

Ainsi, avant de proposer des mesures de sécurité à mettre en œuvre afin d'assurer la sécurité d'actes notariés dématérialisés, il importe d'identifier :

- Les mécanismes mis en œuvre pour assure la protection d'actes « papier ».
- L'objectif visé par la mise en œuvre de ces mécanismes.
- Le niveau de sécurité assuré par de tels mécanismes.
- Les outils ou procédés technologiques qui sauraient offrir un niveau de sécurité fonctionnellement équivalent à ces mécanismes.
- L'acceptabilité du niveau de sécurité actuel dans un environnement numérique.

Cette analyse sera donc effectuée pour les principaux outils et mécanismes présentement mis en œuvre par les notaires, à savoir : 1.2.1) le papier ; 1.2.2) la minute ; 1.2.3) la signature manuscrite ; 1.2.4) l'encre ; 1.2.5) le sceau ; 1.2.6) le greffe du notaire et 1.2.7) le répertoire et l'index du répertoire.

1.2.1 Le papier

Comme le prévoit l'article 30 du *Règlement sur la tenue des dossiers et des études des notaires*[79], « [l]e notaire doit employer, pour ses originaux, du papier chiffon mesurant 216 mm sur 356 mm et dont le grammage ou la masse doit être au moins de 75 g par mètre carré ». Cette dépendance historique au papier[80] comme support permettant d'assurer l'intégrité et la disponibilité des actes notariés[81] s'explique par le fait que, pendant des siècles, le papier a été le support le plus accessible (tant au sens propre qu'au sens financier). Pourtant, sa capacité d'assurer le respect des exigences énon-

79. RLRQ, c. N-3, r. 17.
80. Voir Julien S. MACKAY, « La loi sur le notariat, son évolution et son histoire », (1989) 91-9-10 *R. du N.* 573.
81. Art. 35 et 39 de la *Loi sur le notariat*, préc., note 14.

cées aux articles 35 et 39 de la *Loi sur le notariat* demeure discutable.

Concrètement, le papier est normalement constitué d'une pâte à base de fibres végétales que l'on étale et fait sécher en feuilles minces[82]. La confection du papier, peu importe la nature de sa base, fait foi de sa fragilité : il peut être déchiré, déchiqueté, mouillé, brûlé, etc.[83] ; il peut se dégrader ou se perdre[84]. Il peut également être remplacé par un autre papier identique, ou légèrement altéré. Bref, il s'agit d'un bien meuble léger, tangible et matériel qui demeure assujetti à tout phénomène naturel terrestre[85]. Qui plus est, un document notarié sur support papier est presque nécessairement composé de plusieurs feuilles attachées par une agrafe qui, ensemble, forment un tout. Ces feuilles sont toutefois nécessairement dissociables et, surtout, l'agrafe détachable.

Bref, le papier constitue un support fragile et précaire[86], qualités difficilement réconciliables avec l'obligation d'intégrité associée aux actes notariés originaux.

Notons par ailleurs que les exigences concernant l'intégrité des actes notariés originaux s'étendent aussi aux copies des actes notariés que le notaire est tenu de livrer[87]. Évidemment, avec les logiciels de traitement de textes et les photocopieurs, la production d'une copie est aujourd'hui chose facile et sa conformité à l'original beau-

82. OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Le grand dictionnaire terminologique,* 1983, « Papier », en ligne : <http://granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=2093118>.
83. Voir : CHAMBRE DES NOTAIRES, « Mémoire portant sur le projet de loi nº 65 *Loi concernant le remplacement et la reconstitution des actes notariés en minute détruits lors du sinistre ferroviaire du 6 juillet 2013 dans la ville de Lac-Mégantic* », (2013) en ligne : <http://www.cnq.org/DATA/PUBLICATION/152_fr~v~memoire-projet-de-loi-n65.pdf>, p. 18.
84. Les notaires savent sans doute à quel point la mer de papier dans une étude notariale peut être profonde. Considérant l'amas de feuilles en format lettre ou légal occupant chaque centimètre des surfaces plates d'une étude notariale, il est indéniable qu'une feuille puisse facilement être égarée. Qui plus est, combien de notaires ont déchiqueté par erreur une feuille irremplaçable, ou pire encore, la page de signature d'un acte notarié dûment signé après le départ du client ?
85. Myriam CYR, « L'acte notarié électronique : et si la fiction devenait réalité », (1998) 7-9 *Entracte* 3.
86. Nancy E. GWINN, « The Fragility of Paper: Can our History Record be Saved? », (1991) 13-3 *The Public Historian* 33.
87. Art. 2838 C.c.Q. ; *Loi sur le notariat*, préc., note 14, art. 35 ; *Loi sur le notariat*, L.R.Q. 1968, c. N-2, art. 27 et 54 (ci-après « LN2 »).

coup plus simple à valider. En effet, pour reprendre les propos du notaire Jacques Maisonneuve :

> Avant le photocopieur, la secrétaire devait taper à la machine le contrat avec du papier carbone ou encore, le recopier. Ensuite, il fallait vérifier si la copie était véritablement conforme à l'original. La moindre erreur dans la transcription pouvait changer le sens de l'acte. L'arrivée du photocopieur fut fantastique puisque la machine photographiait le contrat. On n'avait plus à relire et à vérifier la copie avec l'original.[88]

Le notaire certifie la copie par la mention « Copie conforme » imprimée ou tamponnée à la fin d'une photocopie sur support-papier multiusage à base de pulpe de bois. Ensuite, il signe la copie avec sa signature officielle[89] et appose son sceau sur la première page de l'acte. Les informations concernant la nature, la date de l'acte, les parties intervenues, le notaire instrumentant, le lieu et la date de publication (s'il y a lieu) et le numéro de minute sont imprimées sur un endos agrafé à la copie[90]. L'endos de la copie indique également le numéro de celle-ci.

Or, malgré le fait que la copie comporte une série de symboles d'authenticité (sceau du notaire, mention « copie conforme », signature du notaire) et qu'elle est nécessairement plus exacte qu'aux premiers jours de la pratique du notaire Maisonneuve, certains risques de fragmentation et d'atteinte à l'intégrité (ceux-là mêmes que nous avons identifiés ci-dessus pour les originaux) demeurent.

Par ailleurs, une fois la copie émise, elle n'est plus traçable ou liée à l'original dans la voûte du notaire. Cela peut poser problème, par exemple lors de la révocation de procurations générales ou spécifiques. En effet, une fois qu'il en est informé, le notaire a l'obligation d'indiquer la révocation d'une procuration sur l'original de l'acte demeurant dans sa voûte[91]. Cependant, les copies déjà émises ou photocopiées par les institutions financières ne porteront pas cette mention de révocation[92]. Évidemment les tierces parties non

---

88. Marc LAPORTE, « La pratique notariale et les développements technologiques », (1997) 6-3 *Entracte* 10.
89. LN2, art. 59 et 60.
90. A. ROY, préc., note 9, p. 82.
91. Art. 2176 C.c.Q.
92. Art. 2176 al. 2 C.c.Q. : « Si la procuration est faite par acte notarié en minute, le mandant effectue la mention sur une copie et peut donner avis de la fin du mandat au dépositaire de la minute, lequel est tenu d'en faire mention sur celle-ci et sur toute copie qu'il en délivre. »

informées ne sont pas affectées par la révocation[93], mais cet exemple démontre les limites du papier dans l'établissement d'un lien entre la copie et l'original d'un acte notarié. Or, cette absence de lien entre la copie et l'original constitue une vulnérabilité du système actuel. Ce problème pourrait être résolu par la création d'un registre de procuration ou par l'inclusion d'une clause d'expiration dans les actes de procuration. Ces solutions sont toutefois imparfaites. Par ailleurs, comme elles n'ont pas été mises en œuvre, l'on peut en déduire que ce degré d'incertitude et d'insécurité est jugé acceptable et, donc, qu'il n'est pas nécessaire de prévoir un mécanisme parfait lors de la migration vers le numérique.

À la lumière de cette analyse, l'équivalent fonctionnel technologique au papier devra assurer une certaine pérennité au document, ce qui implique le recours à un format normalisé qui ne risque pas d'être abandonné par l'industrie. Le format en question devra également pouvoir être « barré », c'est-à-dire difficile à modifier afin d'assurer l'intégrité du document. Comme nous le verrons en deuxième partie, le format PDF/A pourrait répondre à ces exigences.

1.2.2 La minute[94]

Il est utile de rappeler qu'il existe deux types d'acte notarié : l'acte en brevet et l'acte en minute[95]. Notre analyse portera toutefois uniquement sur l'acte en minute puisque celui-ci fait l'objet d'un dépôt permanent au greffe du notaire[96]. En effet, cette distinction importante (l'obligation ou non de dépôt) implique que l'identification d'un équivalent fonctionnel à la minute s'avère plus complexe que pour le brevet.

Rappelons que la notion de minute, du latin *minuta* (écriture menue) nous vient d'une époque où, étant donné le coût du papier, les notaires avaient l'habitude d'écrire leurs actes en caractères fins. Il est donc intéressant de constater qu'une mesure de rationnement a donné son nom à un mécanisme de sécurité. En effet, le concept de minute est aujourd'hui principalement associé à sa fonction admi-

93. Art. 2181 C.c.Q.
94. Pour une analyse de la minute, voir également : CHAMBRE DES NOTAIRES, préc., note 83, p. 11 et s.
95. *Loi sur le notariat*, préc., note 14, art. 34
96. *Ibid.*, art. 35 et 62.

nistrative d'identification d'un acte en particulier parmi tous les actes reçus par un notaire instrumentant et déposés dans un greffe, et non à la taille des écritures documentant ce processus. Si ce voyage historique peut sembler superflu, il met en exergue un autre élément à prendre en compte dans l'identification des mesures de sécurité à mettre en place pour protéger des actes notariés dématérialisés, à savoir : l'objectif original de la mesure que nous désirons transposer dans l'environnement numérique. Si la sécurité demeure un simple effet secondaire d'un mécanisme et non son objectif, il est légitime de se questionner sur la pertinence de la prise en compte de cet effet secondaire dans l'identification de l'équivalent fonctionnel à mettre en place. Notons toutefois que cela ne saurait être notre interprétation de la minute puisque sa fonction d'identification est bien établie : « Les actes en minute faisant partie d'un greffe sont reçus séparément et numérotés consécutivement en commençant par le numéro un »[97]. Par ailleurs, comme chaque numéro attribué à un acte doit être précisé dans l'acte notarié en plus du greffe auquel il appartient[98], il serait difficile d'écarter le rôle joué par la minute afin d'assurer la disponibilité, l'intégrité et l'irrévocabilité des actes.

Ce rôle s'avère toutefois relativement minime. En effet, la minute n'est qu'un numéro ; elle ne fait pas référence au notaire, à son greffe, au lieu de son étude, à la date ou à la nature de l'acte. Certes, ces informations sont indiquées dans le répertoire ou au début de l'acte minuté, mais la minute en soi ne peut nous informer de sa propre nature. Elle n'est liée aux répertoires que par sa transcription manuelle sur support papier. Elle nous semble donc lacunaire tant par son inexactitude que par son manque de dynamisme. Par ailleurs, l'obligation de la chronologie de la minute pose un défi important de formalisme notarial. En pratique, la minute est souvent un ajout postérieur à la clôture de l'acte, ce qui s'avère quelque peu ironique puisque « [a]ltérer un acte après sa clôture est une faute grave »[99].

Toutefois, la plus grande faiblesse de la minute – telle qu'elle est présentement mise en œuvre – découle du fait qu'elle est tributaire des aléas liés tant à la pratique notariale qu'au quotidien des notaires – lesquels demeurent des êtres humains parfois préoc-

97. *Ibid.*, art. 36.
98. *Ibid.*, art. 52.
99. A. ROY, préc., note 9, p. 66.

cupés, distraits, ou simplement désorganisés[100]. Cette vulnérabilité du mécanisme actuel d'inscription des minutes est d'ailleurs bien connue du législateur, d'où les mesures de correction prévues à l'article 37 de la *Loi sur le notariat* :

> Si le même numéro est attribué à plus d'une minute ou si une autre erreur de numérotation est commise, l'acte demeure authentique ; mais dès que l'erreur est constatée, le notaire ou s'il s'agit d'un greffe commun ou social, un indivisaire ou un associé doit inscrire, après les signatures, sur toute minute qui contient l'erreur, une déclaration sous son serment professionnel relatant la nature de l'erreur et il doit inscrire au répertoire le numéro tel qu'il apparaît sur la minute. Une copie de cette déclaration doit être transmise au secrétaire de l'Ordre sans délai.
>
> En cas d'omission d'un numéro, il doit être inséré dans le greffe dès que l'erreur est constatée, à l'endroit où aurait dû être l'acte portant le numéro omis, une déclaration constatant l'omission de ce numéro. Le numéro omis doit être inscrit au répertoire avec la mention qu'aucun acte n'y correspond. Une copie de cette déclaration doit être transmise au secrétaire de l'Ordre sans délai.
>
> Les obligations imposées aux notaires par le présent article incombent également aux personnes qui, notamment à titre de gardiens provisoires ou de cessionnaires, sont dépositaires du greffe.[101]

Quoi qu'il en soit, il ne fait aucun doute que la minute joue un rôle important qui doit être reproduit dans l'environnement technologique. L'obligation consécutive et chronologique de la minute oblige le notaire à respecter les dates de la réception d'un acte notarié. Le notaire a un devoir de probité. Ainsi, l'obligation de minuter assure l'intégrité de la méthode pratique du notaire. En ce sens, la minute offre certaines similitudes à l'obligation de documentation prévue à la *Loi concernant le cadre juridique des technologies de l'information* pour le transfert ou la transmission de documents technologiques[102].

Ainsi, un greffe numérique devra nécessairement conserver un mécanisme d'identification des actes et de leurs signataires – pro-

---

100. T. BRASSARD, « De la tenue systématique des bureaux de notaires », (1918) 21 *R. du N.* 128, 137.
101. Notons que cette vulnérabilité est connue depuis des décennies. Voir J.S. MACKAY, préc., note 80.
102. Voir les articles 17 et 34 de la *Loi concernant le cadre juridique des technologies de l'information*, préc., note 8.

cessus essentiel au maintien de la disponibilité et de l'irrévocabilité desdits actes. Toutefois, ce mécanisme pourra être automatisé, ce qui viendra corriger la vulnérabilité identifiée par le législateur à l'article 37 de la *Loi sur le notariat*. Nous y reviendrons.

1.2.3 La signature manuscrite

Comme le prévoit l'article 50 de la *Loi sur le notariat* :

> L'acte notarié est clos par la signature des parties et des témoins requis suivant le cas, en présence du notaire instrumentant et par la signature de ce dernier, qui doit être apposée le même jour et au même lieu où la dernière des parties à signer l'a fait.[103]

Cette disposition permet d'emblée d'identifier deux types de signatures distincts, à savoir la signature des parties et témoins (1.2.3.2), d'une part, et la signature du notaire (1.2.3.1), d'autre part. Débutons par cette dernière.

1.2.3.1 La signature du notaire

Rappelons que la signature d'un acte par le notaire sert deux fonctions fondamentales : l'identification du signataire (en l'occurrence le notaire instrumentant et officier public, membre de l'Ordre professionnel des notaires du Québec[104]) et la manifestation de sa volonté de conférer un caractère authentique à l'acte qu'il reçoit[105]. Pourtant, comme nous le verrons, ces fonctions sont plus ou moins bien servies par le mécanisme de signature manuscrite. En effet, la signature ne permet pas toujours d'identifier le signataire (elle ne comporte pas nécessairement le nom et prénom du signataire, elle est parfois illisible, etc.) et, à force de répétition constante, a tendance à évoluer au fil du temps.

Notons que, sur ces points, la signature manuscrite du notaire offre un certain avantage par rapport aux signatures d'autres individus puisqu'elle doit faire l'objet d'un dépôt auprès de l'Ordre[106].

---

103. *Loi sur le notariat*, préc., note 14, art. 50 al. 1.
104. Cette fonction est par ailleurs complétée par le fait que l'article 21 de la *Loi sur le notariat* (préc., note 14) prévoit que la signature du notaire doit aussi comprendre la mention « notaire » ou « notary ».
105. Art. 2827 C.c.Q.
106. *Loi sur le notariat*, préc., note 14, art. 8(1). Notons que cette règle s'applique également au paraphe manuscrit du notaire. Qui plus est, toute nouvelle

(à suivre...)

Ainsi, advenant la contestation d'une signature apposée à l'aide d'un stylographe à la fin d'un acte imprimé sur papier chiffon, il est possible de la comparer à la signature déposée. Si ce mécanisme offre une façon de contrôler l'authenticité d'une signature, il demeure toutefois imparfait pour diverses raisons. D'abord, comme nous le verrons ci-après, « un expert ne pourra jamais prétendre à 100 % qu'un scripteur a ou non exécuté une signature »[107]. L'utilité du dépôt d'une signature auprès de l'Ordre est donc limitée. Ensuite, malgré l'obligation de déposer toute nouvelle signature officielle, il importe de rappeler que la *Loi sur le notariat* prévoit que l'omission de procéder de la sorte n'est pas fatale à la validité d'un acte :

> **60.** Tout acte reçu par un notaire et signé par lui, mais qui ne porte pas la signature officielle de ce notaire telle que déposée auprès du secrétaire de l'Ordre, n'en est pas moins authentique et a le même effet que s'il eût été signé de la signature officielle de ce notaire.

C'est donc dire que la signature manuscrite du notaire n'offre pas nécessairement le niveau de sécurité souhaité, d'autant que, selon le type de signature, celle-ci n'est pas toujours unique, ni inimitable. Ainsi, il est possible d'avancer que la signature manuscrite du notaire, bien que jugée fondamentale afin d'assurer l'authenticité d'un document émanant d'un officier public, n'est pas aussi sécurisée que ne laissent croire les pratiques existantes. Or, vu l'importance accordée à la signature d'un acte par le notaire, il nous paraît justifié, comme le permet par ailleurs l'article 21 de la *Loi sur le notariat*, de favoriser la signature numérique de l'acte par le notaire[108] (sous réserve d'« obtenir l'autorisation du secrétaire de l'Ordre pour utiliser sa signature officielle apposée au moyen d'un procédé technologique »). Rappelons que, contrairement à d'autres types de signatures électroniques[109], la signature numérique est « basé[e] sur l'utilisation d'un algorithme de chiffrement qui permet de vérifier l'intégrité du document et d'en assurer la non-répudia-

---

(...suite)
version ou version modifiée de la signature manuscrite doit faire l'objet d'un nouveau dépôt. Voir la *Loi sur le notariat*, *ibid.*, art. 23.

107. *Wilson* c. *McKay*, 2005 CanLII 10196, par. 47 (QC C.S.).

108. C'est d'ailleurs ce que prétend Pierre Trudel. Voir : Pierre TRUDEL, *Introduction à la Loi concernant le cadre juridique des technologies de l'information*, Montréal, Éditions Yvon Blais, 2012, p. 50.

109. Sur la notion de signature électronique, voir Patrick CORMIER, *Analysis of Digital & Electronic Signatures in the Canadian Justice Sector*, Canadian Centre for Court Technology, 2012.

tion »[110]. Ce type de signature – celui-là même qui est déjà utilisé par les notaires (les signatures émises par Notarius s'inscrivent dans cette catégorie) – assure donc un niveau de sécurité de loin supérieur à celui qu'offre la signature manuscrite, ce qui cadre mieux avec la fonction visant à sécuriser les actes notariés dématérialisés.

Qui plus est, l'utilisation d'une signature numérique attribuée par une autorité particulière aura pour effet d'agir comme un outil important contre l'exercice illégal de la profession[111] puisque, présentement, tout acteur doué muni d'un stylo peut se prétendre notaire.

1.2.3.2 La signature des parties et des témoins

Comme nous venons de le souligner, la signature vise deux fins : identifier le signataire et représenter la manifestation du consentement de celui-ci. La signature manuscrite des parties et des témoins remplit très mal ces objectifs[112]. En effet, contrairement à la signature du notaire, celle des autres parties ne peuvent être authentifiées en les comparant à un échantillon déposé auprès d'un tiers neutre. Il est donc difficile de les utiliser pour identifier un individu *post facto*, surtout lorsque rien, dans le corps d'une signature, ne permet de l'associer à un individu en particulier. Il est bien entendu possible de demander un échantillon d'écriture pour le comparer à la signature apposée à l'acte, mais – tel que l'a souligné le législateur[113] – la signature d'une personne tend à évoluer. Il est d'ailleurs admis que la comparaison de signatures ne saurait constituer une science exacte[114]. Qui plus est, comme la signature peut

110. OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Le grand dictionnaire terminologique*, « Signature numérique », en ligne : <http://granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=8384641>.
111. *Loi sur le notariat*, préc., note 14, art. 31, 32 et 33. Voir notamment le communiqué de la Chambre des notaires en date du 8 avril 2011, en ligne : <https://inforoute.cdnq.org/prive/nouvelles/communiques/communique-web-video-par-le-president-sur-les-centres-de-traitement-et-l-exercice-illegal>. Voir également *Chambre des notaires du Québec* c. *Gagné*, J.E. 93-319 (C.S.) et *Chambre des notaires du Québec* c. *Gaston Saucier*, C.S. Chicoutimi, nº 150-61-000839-964, 10 décembre 1996. Voir finalement Pauline PAIEMENT, « Un avocat plaide coupable à quatorze accusations d'exercice illégal », (1997) 6-2 *Entracte* 8.
112. R. SICILIANO, préc., note 75.
113. *Loi sur le notariat*, préc., note 14, art. 23.
114. Voir *Dallaire (Succession de)*, 2013 QCCS 1549, par. 17. Voir également *Wilson* c. *McKay*, préc., note 107, par. 37 et 47 ; *Union des employés de service, local 298* c. *Syndicat des salariés de l'Hôpital St-Luc*, 1989 CanLII 6844 (QC T.T.).

(à suivre…)

consister en une simple marque[115], telle une croix[116], il s'agit d'un mécanisme d'identification relativement faible.

Cela étant, le rôle d'identifiant de la signature est-il vraiment nécessaire pour assurer la validité d'un acte notarié ? Il serait possible d'arguer que la réponse à cette question est négative. En effet, rappelons que « [l]e notaire doit, par tout moyen raisonnable, vérifier l'identité, la qualité et la capacité des parties à un acte notarié dont il reçoit la signature »[117]. Ainsi, le signataire étant identifié préalablement à la signature de l'acte, sa signature n'est réellement utile, à notre avis, que pour manifestation de consentement.

C'est donc dire que la réelle mesure de sécurité réside dans le respect, par le notaire, de ses obligations déontologiques[118] et non dans la signature des parties.

Comment donc remplacer la signature manuscrite apposée à un acte notarié ? Si l'on désire atteindre un niveau de sécurité identique à l'existant, l'apposition d'une signature manuscrite numérisée, soit à l'aide d'un stylet[119], soit en apposant une image de notre signature[120] s'avère une solution évidente. Il s'agit toutefois d'un mécanisme peu imaginatif qui ne profite pas des avantages offerts par la technologie[121]. Ainsi, par exemple, la signature par nom d'utilisateur – mot de passe[122], l'utilisation de jetons, ou encore la

---

(...suite)
Cela explique d'ailleurs pourquoi les experts ne s'entendent pas toujours sur l'authenticité d'une signature. Voir par exemple *Tremblay* c. *Perrone (Succession de)*, 2006 QCCS 3073 ; *Vanel* c. *Vanel*, 2005 CanLII 22750 (QC C.S.).

115. Art. 2827 C.c.Q.
116. Voir *Lccjti.ca*, 2017, « signature » , en ligne : <http://www.lccjti.ca/definitions/signature/>.
117. *Loi sur le notariat*, préc., note 14, art. 43. La disposition poursuit en précisant que : « Lorsque, en application du deuxième alinéa de l'article 50, la signature de l'une des parties est reçue par un autre notaire que le notaire instrumentant, il appartient à cet autre notaire de vérifier l'identité, la qualité et la capacité de la partie concernée ».
118. *Code de déontologie des notaires*, préc., note 46.
119. Pensons, par exemple, aux mécanismes utilisés dans les bureaux de poste.
120. La Cour du Québec a notamment reconnu la validité d'une telle signature dans *Roussel* c. *Desjardins Sécurité financière, compagnie d'assurance-vie*, 2012 QCCQ 3835.
121. Sur cette question, voir N. VERMEYS et K. BENYEKHLEF, préc., note 18.
122. Voir P. CORMIER, préc., note 109.

signature biométrique[123] constituent des approches mieux adaptées au médium et offrent un niveau de certitude plus élevé.

Mentionnons que, sauf exceptions[124], la signature numérique ne constitue pas ici une solution pratique, voire envisageable. En effet, et pour diverses raisons, il semble difficilement justifiable de se soumettre à la relative lourdeur du processus d'obtention d'une telle signature[125]. D'abord, le niveau de sécurité qu'elle procure est exponentiellement plus élevé que le niveau actuel (pourtant jugé acceptable). Ensuite, elle s'avère quelque peu redondante puisque d'autres mécanismes telle la vérification de l'identité du signataire par le notaire instrumentant sont déjà en place. Finalement, rappelons que l'article 2827 C.c.Q. prévoit qu'une signature « consiste dans l'apposition qu'une personne fait à un acte de son nom ou d'une marque qui lui est personnelle et qu'elle utilise de façon courante » (notre soulignement). Ainsi, la création d'une signature numérique aux seules fins de l'acte notarié semble incompatible avec la lettre de cette disposition[126].

1.2.4 L'encre

L'encre constitue présentement le principal mécanisme visant à assurer la pérennité de l'information contenue dans un acte et, donc, de sa disponibilité. Le recours à cette technologie vise également à assurer l'immutabilité de l'acte notarié dès le moment de sa clôture et durant sa conservation[127]. En effet, l'article 45 de la *Loi sur le notariat* ne saurait être plus clair à cet effet :

> Les actes notariés sont écrits avec une encre de bonne qualité[128], dactylographiés ou imprimés lisiblement d'une manière permanente.

123. En effet, le World Wide Web Consortium (W3C) a récemment annoncé la mise sur pied d'un nouveau système d'authentification (WebAuthn) pouvant incorporer de tels mécanismes. Voir : « Web Authentication: An API for accessing Public Key Credentials Level 1 », (2018) en ligne : <https://www.w3.org/TR/2018/CR-webauthn-20180320/>.
124. Nous vous référons ici aux cas où le signataire possède déjà une signature numérique qu'il utilise régulièrement.
125. Sur cette question, voir P. CORMIER, préc., note 109.
126. Sur cette question, voir Nicolas W. VERMEYS, *Droit codifié et nouvelles technologies*, Montréal, Éditions Yvon Blais, 2015, p. 55.
127. A. ROY, préc., note 9, p. 66.
128. Notons que, si l'expression « encre de bonne qualité » nous semble relativement floue, elle demeure plus précise que celles prévues dans certains textes plus anciens. Par exemple, l'article 41 du *Code de notariat de 1883* indiquait tout

(...à suivre)

> L'emploi de formulaires multipliés par tout moyen technique est permis[129] pourvu qu'ils possèdent les mêmes caractéristiques que les actes dactylographiés ou imprimés. Ces actes ne doivent contenir aucun blanc, lacune ou intervalle, autre que les espaces normaux, qui ne soit marqué d'un trait.[130]

Ajoutons finalement que, comme le prévoient les articles 35 et 39 de la *Loi sur le notariat*, « [l]es inscriptions des actes doivent, au moment de la clôture de l'acte, être permanentes, sans lacune et être protégées contre les altérations »[131]. Notons ici que, si l'encre apposée à l'aide d'un stylographe[132] ou d'un dactylographe[133] semble remplir cet impératif, d'autres moyens, dont ceux faisant appel aux technologies de l'information, sont également envisageables. D'ailleurs, il est pertinent de rappeler, comme nous l'avons souligné ci-dessus dans la section portant sur le papier, que la quasi-totalité des actes sont aujourd'hui écrits à l'aide d'un ordinateur. Si ces actes sont présentement imprimés pour être signés de façon manuscrite et, le cas échéant, modifiés à l'aide d'une dactylo, ces étapes demeurent superflues. En effet, un document technolo-

---

(...suite)
simplement que les notaires doivent utiliser une « bonne encre ». Une expression nous semblant préférable est celle utilisée à l'article 13 de la *Loi du 25 Ventôse 1803*, telle que modifiée en 1926, soit une « encre noire indélébile d'une composition approuvée par la chancellerie ». Voir Henri TURGEON, « L'écriture des actes notariés », (1949) 52 *R. du N.* 421, 422. Ceci étant, si l'on pouvait débattre sur ce qui constitue une « encre de bonne qualité », la nécessité de recourir à celle-ci s'avère évidente. En effet, dans un article publié en 1944, Léon Roy, alors directeur des archives judiciaires du Québec, tente d'instruire les notaires sur les « bonnes encres », ainsi que les risques courus à la suite de l'utilisation d'une encre de mauvaise qualité. Voir Léon ROY, « Permanence des écritures modernes », (1944) 47 *R. du N.* 531. Voir également H. TURGEON, *ibid.*, 426 : « Si, parce qu'un notaire a utilisé le stylographe à bille, de la mauvaise encre ou un ruban d'occasion, l'écriture finit par s'effacer, c'est l'intérêt public qui peut en souffrir ».

129. Notons que cette possibilité semble être envisagée depuis 1672. Voir H. TURGEON, *ibid.*, 421.
130. *Loi sur le notariat*, préc., note 14, art. 45 al. 1.
131. *Ibid.*, art. 35 al. 2 et 39 al. 2.
132. Notons que le stylo utilisé par les notaires a évidemment évolué au fil des ans. De la plume d'oie au stylo feutre, en passant par la pointe de métal adaptée à un porte-plume, le stylo à plume et le stylo à bille, plusieurs outils ont fait leur apparition. Cela étant, la forme du stylo demeure non pertinente puisqu'il ne s'agit que d'un véhicule pour répandre l'encre utilisée par le notaire. Voir : J. MARTINEAU, préc., note 1.
133. Introduit dans les pratiques notariales au cours des années 1920, le dactylographe est rapidement devenu un outil « indispensable ». Voir : T. BRASSARD, préc., note 100, 132. Ce n'est toutefois qu'en 1926 que la loi sera modifiée afin de permettre l'utilisation du dactylographe autant pour les copies que pour les originaux des actes notariés. Voir J. MARTINEAU, préc., note 1.

gique peut très bien respecter les exigences des articles 35 et 39 de la loi.

D'ailleurs, nous estimons que le document technologique saurait mieux respecter ces exigences que son équivalent papier. En effet, outre les risques d'évanescence qui, sous réserve du respect de l'obligation de recourir à une encre de bonne qualité et de ne pas laisser les actes exposés au soleil (ce qui est peu probable s'ils sont conservés dans une voute), demeurent relativement faibles, la sécurité assurée par l'encre est tributaire du support sur lequel elle est apposée. En effet, tel que nous l'avons déjà soulevé, le papier demeure un support fragile et facile à détruire. L'exemple du 11 septembre 2001 est ici éloquent. Alors que les documents « papier » détenus par les divers cabinets d'avocats qui occupaient des locaux du World Trade Center ont tous été détruits ou répandus sur les rues de Manhattan, les documents technologiques détenus par les institutions financières pour lesquels des redondances existaient sur divers serveurs situés ailleurs dans le monde sont demeurés intacts[134]. Un autre exemple, beaucoup plus présent dans l'esprit des notaires québécois, est celui de la tragédie de Lac-Mégantic. Alors que des milliers de testaments entreposés dans les voûtes d'études notariales ont été détruits par les flammes[135], les données financières détenues par la succursale de la Banque Nationale également touchée par l'incendie n'ont pas été affectées puisqu'elles étaient hébergées sur un serveur situé à l'extérieur du périmètre. Résultat : la Banque a pu ouvrir une nouvelle succursale quelques jours après l'incendie[136], alors que la Chambre des notaires

134. L'exemple le plus parlant est sans doute celui des attaques du 11 septembre 2001 sur les tours du World Trade Center à New York. Alors que les documents papier ont tous été détruits, le commerce n'a pas été affecté irrémédiablement puisque des copies électroniques de ces mêmes documents demeuraient disponibles sur divers serveurs à travers le monde. Comme le souligne la SEC : « electronic records help protect against loss of a physical site ». Voir « Summary of "Lessons Learned" from Events of September 11 and Implications for Business Continuity », (2002) en ligne : <http://www.sec.gov/divisions/marketreg/lessonslearned.htm>.

135. Philippe TEISCEIRA-LESSARD, « Des milliers de testaments détruits à Lac-Mégantic », (2013) *La Presse*, en ligne : <http://www.lapresse.ca/actualites/dossiers/tragedie-a-lac-megantic/201307/13/01-4670446-des-milliers-de-testaments-detruits-a-lac-megantic.php>. Voir également : CHAMBRE DES NOTAIRES, préc., note 83.

136. Voir : « La Banque Nationale poursuit le déploiement de ses mesures de soutien à Lac-Mégantic », (2013) en ligne : <https://www.bnc.ca/fr/a-propos-de-nous/nouvelles/salle-de-presse/communiques-de-presse/2013/20130710-la-banque-nationale-poursuit-le-deploiement-de-ses-mesures-de-soutien-a-lac.html>.

aura pris près de deux ans pour récupérer quelque 14 000 actes notariés détruits[137]. Si le papier demeure le maillon faible, l'encre n'est pas sans failles. Par exemple, rappelons qu'afin d'assurer le respect de l'intégrité d'un document « papier », tout écrit ajouté, interligné ou surchargé est réputé non écrit[138]. Les renvois et sous-renvois doivent être inscrits en marge, ou continués à la fin de l'acte si leur longueur l'exige, à condition d'être paraphés par tous les signataires de l'acte, sous peine de nullité[139]. Le nombre de renvois, sous-renvois et ratures doit être mentionné avant la signature des parties[140] et doit comporter certaines précisions, par exemple : « LECTURE FAITE, les parties signent en présence du notaire. Quatre (4) lettres, trois (3) mots et, cinq (5) chiffres rayés sont nuls et deux (2) renvois en marge sont bons ».

Ainsi, les parties qui souhaitent modifier un acte après sa clôture doivent convenir de conclure un nouvel acte afin de révoquer l'acte précédent[141]. Par ailleurs, bien que la *Loi sur le notariat* prévoie expressément qu'une fois l'acte clos, les inscriptions contenues dans ce dernier doivent être protégées contre toute altération[142], en pratique, les notaires « altèrent » souvent l'acte notarié au dactylo par l'ajout du numéro de minute, de la date ou du nom d'un mandataire à la suite de sa clôture. Ainsi, malgré le fait que ces ajouts ne modifient pas le contenu de l'acte et ne mettent pas en péril son authenticité, il demeure que la disposition prohibant toute altération aux actes notariés suivant leur clôture n'est pas respectée à la lettre. Dans le même ordre d'idées, bien que cela ne soit pas perçu ainsi, les notaires portent presque nécessairement atteinte à l'intégrité des actes qu'ils reçoivent, le tout en contravention de l'article 6 de la *Loi concernant le cadre juridique des technologies de l'information* :

> 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.

---

137. « La Chambre des notaires du Québec ferme son point de service à Lac-Mégantic », (2015) *Radio-Canada*, en ligne : <https://ici.radio-canada.ca/nouvelle/740010/fermeture-point-de-service-lac-megantic-chambre-des-notaires>.
138. *Loi sur le notariat*, préc., note 14, art. 46.
139. *Ibid.*, art. 47.
140. *Ibid.*, art. 49.
141. A. ROY, préc., note 9, p. 66.
142. *Loi sur le notariat*, préc., note 14, art. 35 al. 2 (actes en minute) et art. 39 (actes en brevet) ; A. ROY, *ibid.*, p. 91.

> 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.
>
> Dans l'appréciation de l'intégrité, il est tenu compte, notamment des mesures de sécurité prises pour protéger le document au cours de son cycle de vie. [Notre soulignement]

Ainsi, si l'altération accessoire ultérieure est justifiée – à tort ou à raison – par l'obligation de souscrire aux autres règlements d'indexation numérique et chronologique des actes notariés, il demeure que le fait d'apposer ces informations « sur l'acte », plutôt que de les associer « à l'acte » (ce qui serait envisageable grâce à un mécanisme technologique) enfreint la lettre de la loi. Ici, la migration vers un acte dématérialisé offrirait non seulement une solution fonctionnellement équivalente permettant d'assurer la permanence, l'intégralité et l'intégrité des inscriptions au moment de la clôture de l'acte[143], mais elle permettrait également de mieux respecter certaines des obligations du notaire, lesquelles, dans un monde papier, semblent contradictoires.

1.2.5 Le sceau

Commee le prévoyait l'article 21 de l'ancienne *Loi sur le notariat*[144] :

> **21.** 1 Tout notaire doit avoir un cachet ou sceau particulier reproduisant, d'après un modèle uniforme, les armes du Québec, avec, en exergue, ses nom et prénom ou initiales et les mots : « notaire », « Québec, Canada ». Les notaires en exercice le 1er mars 1969 peuvent continuer à utiliser le sceau qu'ils possèdent.
>
> 2. (Paragraphe abrogé).
>
> 3. Tout notaire doit apposer ce sceau sur les actes en brevet qu'il reçoit et sur les copies et extraits des actes de son répertoire ou des greffes dont il est dépositaire ou cessionnaire.

Cette obligation, qui remonte au XIIIe siècle[145] (bien qu'elle n'ait été étendue aux notaires du Québec qu'en 1899[146]), découle en fait

143. *Loi sur le notariat*, *ibid.*, art. 35 al. 2 et 39 al. 2.
144. LN2, art. 21.
145. J. MARTINEAU, préc., note 1.
146. Joseph Edmond ROY, « Histoire du notariat au Canada », (1902) 5 *R. du N.* 604.

d'un besoin de suppléer à l'ignorance et de tenir lieu des signatures des parties[147]. Ainsi, le sceau constitue un mécanisme parmi tant d'autres[148] permettant « de confirmer la sincérité de la signature des notaires, d'attester que l'acte est revêtu de la sanction de l'autorité publique et d'en empêcher la contrefaçon »[149]. Comme le précise Jean Martineau :

> C'est parce que les notaires sont détenteurs d'une parcelle de l'autorité publique que leurs actes sont considérés comme des lois. Des lois à caractère privé qui engagent les signataires. Et c'est parce qu'ils sont délégataires de cette autorité publique qu'ils doivent avoir un sceau particulier.[150] (Notre soulignement)

Pourtant, l'apposition par le notaire de son sceau sur la marge gauche de la première page d'un acte pour affirmer que la copie est une reproduction fidèle et inaltérée de l'original, notamment par l'attestation et l'identification de l'officier public duquel elle émane, n'offre aucune garantie réelle de sécurité. L'apposition du sceau s'assimile à une action de nature administrative. Plausiblement, la non-apposition du sceau n'entraînerait pas la perte du caractère authentique de la copie conforme d'un original[151]. En effet, le sceau, peu importe la forme qu'il prendra (sceau de cire, sceau d'encre, autocollant, sceau qui gaufre le papier, etc.[152]), demeure un signe extérieur et superficiel de l'authenticité des copies délivrées par les notaires. Qui plus est, son apposition sur une seule page d'un acte n'empêche pas la substitution de pages subséquentes ou la modification de l'acte après l'apposition du sceau. Évidemment, si une copie de l'original est conservée par le notaire, une telle manigance sera rapidement découverte. Toutefois, si, pour une raison quelconque, la copie modifiée constitue la seule version disponible d'un acte, le sceau ne sera d'aucune utilité pour en établir l'intégrité.

---

147. J. MARTINEAU, préc., note 1 ; Gilles ROUZET, « Aux origines du sceau : du sceau de tabellion romain à celui de notaire public », (1989) 65 *Gnomon. Revue internationale d'histoire du notariat* 26.
148. Pensons notamment au témoin instrumentant selon l'article 1208 C.c.B.-C. Voir : J. MARTINEAU, *ibid.* ; G. ROUZET, *ibid.*
149. L.J.N.M. RUTGEERTS, *Manuel de droit notarial et de droit fiscal*, Bruxelles, Imprimerie de A. Labroue et compagnie, 1853, p. 84.
150. J. MARTINEAU, préc., note 1.
151. A. ROY, préc., note 9, p. 89 ; Paul-Yvan MARQUIS, *La responsabilité civile du notaire*, Montréal, Éditions Yvon Blais, 1999, p. 340 et 341 ; *Gauthier* c. *Bouchard*, (1934) 37 R.P. 280, 282 (C.S.).
152. J. MARTINEAU, préc., note 1.

Comme le souligne Marc Lacoursière, si le « sceau sert à protéger un document, identifier une personne ou assurer la confidentialité du document »[153], ces objectifs seront en fait plus facilement assurés par le recours à des solutions technologiques telles la cryptographie ou la biométrie[154]. D'ailleurs, il est utile de préciser que l'article 13 de la *Loi concernant le cadre juridique des technologies de l'information* prévoit expressément qu'un procédé technologique peut remplacer l'utilisation d'un sceau :

> Lorsque l'apposition d'un sceau, d'un cachet, d'un tampon, d'un timbre ou d'un autre instrument a pour fonction :
>
> 1º de protéger l'intégrité d'un document ou d'en manifester la fonction d'original, celle-ci peut être remplie à l'égard d'un document technologique, au moyen d'un procédé approprié au support du document ; [...].

Comme nous le verrons ci-après, la signature numérique du notaire saurait, à notre avis, constituer « un procédé approprié au support du document ».

1.2.6 Le greffe du notaire

Malgré tout ce qui précède, la principale mesure de sécurité associée à la préservation d'actes notariés demeure l'obligation pour le notaire de se pourvoir d'une « voûte de sûreté »[155], c'est-à-dire d'une « chambre-forte » ou d'un « coffre-fort »[156]. En effet, comme le prévoit l'article 32 du *Règlement sur la tenue des dossiers et des études des notaires*[157] :

> Le notaire conserve ses minutes, répertoire, index, livres de comptabilité en fidéicommis, logiciels d'application, incluant notamment les logiciels de gestion, de base de données et de comptabilité, les mises à jour ainsi que les copies de sauvegarde des données dans une chambre-forte ou un coffre-fort offrant la garantie d'une résistance au feu de 927 ºC pour une période d'au moins 1 heure.[158]

---

153. Marc LACOURSIÈRE, « Le défi du législateur face au cyberespace », (2011) 2 *C.P. du N.* 123, 157.
154. *Ibid.*, 157 et s.
155. Victor MORIN, « L'organisation du notariat au Canada », (1930) 22 *R. du N.* 313.
156. J.S. MACKAY, préc., note 80.
157. Préc., note 79.
158. Voir *Maryse Laliberté* c. *X*, Comité de discipline, Chambre des notaires du Québec, nº 26-00-00850, 31 août 2000. Notons que, sur demande du Comité

(à suivre...)

Cette exigence de posséder un greffe constitue par ailleurs le principal obstacle à la migration vers un système d'actes notariés dématérialisés puisque, malgré la création de greffes électroniques dans d'autres pays[159], ceux-ci sont perçus comme étant moins sécuritaires que leur équivalent physique par certains membres des professions juridiques[160]. Néanmoins, bien que le coffre-fort constitue un symbole de sécurité dans l'imaginaire collectif, il demeure que celui-ci, s'il assure indéniablement un niveau de confidentialité élevé[161], n'est pas aussi efficace dans la protection de l'intégrité et de la disponibilité des documents qui y sont conservés.

En effet, comme le dévoile la lecture de l'article 32 du *Règlement sur la tenue des dossiers et des études des notaires*, le coffre-fort ou la chambre-forte sont principalement requis afin d'assurer une protection contre le feu[162], le vol ou la consultation par un tiers non autorisé. Cependant, ces voutes, pour reprendre une appellation historique[163], n'offrent aucune protection (ou, pour être plus juste, n'ont pas l'obligation d'offrir une protection) contre la fumée causée par le feu ou contre l'eau utilisée pour l'éteindre. Ainsi, les classeurs ignifuges ne constituent une contre-mesure qu'à un nombre restreint de vulnérabilités liées au papier chiffon. La tragédie de Lac-Mégantic en fait foi[164].

Dans un reportage de *La Presse* intitulé « Le miracle de la voûte »[165], on présente une voûte offrant une protection contre

---

(...suite)
administratif, du secrétaire, du syndic ou d'un inspecteur, le notaire doit fournir un certificat d'architecte, ingénieur ou technologue professionnel attestant que sa chambre-forte ou son coffre-fort est conforme aux exigences du règlement.

159. C'est le cas, notamment, en France et en Italie. Voir la section 2.2 ci-après.
160. Ce constat est le fruit de questions ayant été soumises à l'un des auteurs de ce document dans le cadre de cours, de colloques et de conférences.
161. Notons toutefois que ce niveau de sécurité demeure imparfait. Voir *Guardian Trust Company* c. *Frappier & Holland Inc.*, [1978] C.A. 304. Dans cette affaire, des documents ont été dérobés d'une voûte bancaire faute d'avoir assuré une surveillance adéquate des individus y ayant accès.
162. Notons par ailleurs que la validité de cette protection, c'est-à-dire si un classeur ignifuge (surtout après plusieurs années d'utilisation) répond ou non à l'exigence prescrite par l'article 32 du Règlement, ne pourra être validée qu'une fois l'incendie déclaré.
163. V. MORIN, préc., note 155.
164. Voir : CHAMBRE DES NOTAIRES, préc., note 83.
165. Marie-Michèle SIOUI, « Le miracle de la voûte », (2013) en ligne : <http:/ www.lapresse.ca/videos/actualites/201307/19/46-1-le-miracle-de-la-voute.php/639e5a5f10ed4b0ea84adb3a23543fa7>.

l'incendie de 30 000 minutes, laquelle a survécu à la tragédie de Lac-Mégantic. Fabriquée en 1958 et composée de béton armé et de briques coupe-feu, la voûte en question a résisté à une chaleur de plus de 3 000 degrés Celsius. Les mesures prises dans la construction de cette voûte vont donc au-delà des exigences légales. Manifestement, une voûte ignifuge ou un coffre-fort qui respecte les normes règlementaires n'auraient pas survécu à un tel incendie. La Chambre des notaires admet d'ailleurs que les voûtes ignifuges n'ont pu résister à l'intensité des flammes[166]. Or, comme il n'existe aucune solution pour le remplacement des actes originaux détruits ou perdus (sauf, dans certains cas, la reconstitution à partir des copies conformes émises)[167], les coffres-forts et les chambres fortes n'offrent qu'un niveau limité de sécurité. Soit, les tragédies comme celle de Lac-Mégantic sont (heureusement) relativement rares, mais il demeure que le système est perfectible, notamment par l'apport des technologies de l'information. Le reportage de *La Presse* souligne d'ailleurs le fait qu'un désastre comme celui de Lac-Mégantic démontre la pertinence de procéder à la création d'un minutier central où les notaires pourraient déposer leurs actes[168]. Si une telle approche ne reçoit pas, pour différentes raisons, l'aval de certains membres de la profession[169], elle assurerait une plus grande sécurité aux actes conservés.

1.2.7 Le répertoire et l'index du répertoire[170]

Comme le prévoit l'article 19 de l'ancienne *Loi sur le notariat* : « [t]out notaire doit avoir et tenir en bon état de conservation un répertoire des actes qu'il reçoit en minute, dans lequel il inscrit consécutivement, dès leur clôture, la date et le numéro des actes,

166. « Tragédie du Lac-Mégantic – Questions et Réponses », (2013) en ligne : <http://www.cnq.org/fr/17-nouvelle-tragedie-de-lac-megantic-questions-et-reponses.html>.
167. *Ibid.*
168. *Ibid.* Cette position avait d'ailleurs été proposée par plusieurs avant même l'avènement de la tragédie de Lac-Mégantic. Voir notamment Marc LACOURSIÈRE, « Les défis du législateur face au cyberespace », (2011) 2 *C.P. du N.* 123 et Isabelle DE LAMBERTERIE, « Quelles problématiques pour l'établissement et la conservation d'un acte authentique électronique ? », dans Isabelle DE LAMBERTERIE (dir.), *Les actes authentiques électroniques : réflexion juridique prospective*, Paris, La Documentation française, 2002, p. 57, 67 et 68.
169. Cette information nous a été confiée par certains membres et représentants de la Chambre qui ont été consultés dans la rédaction de ce texte.
170. Pour une analyse du répertoire et de l'index du répertoire, voir : CHAMBRE DES NOTAIRES, préc., note 83, p. 14 et s.

leur nature et espèce et le nom des parties ». L'article 20 de la même loi complète en précisant que « [t]out notaire doit tenir et conserver selon les règlements du Conseil d'administration un index au répertoire »[171]. Le répertoire doit être relié, conservé en bon état et doit respecter les exigences des règlements du Conseil d'administration, notamment quant à sa conservation dans une chambre-forte ou un coffre-fort offrant la garantie d'une résistance au feu[172].

Le répertoire répond donc à un besoin principalement administratif, c'est-à-dire de permettre au notaire de facilement identifier la date d'un acte, sa nature et les parties qui y ont comparu. Il permet également de facilement identifier le prochain numéro de minute. En ce sens, l'utilité du répertoire, sur le plan de la sécurité, est limitée. Cet outil est surtout utile afin d'assurer la disponibilité des actes en permettant de les retracer rapidement.

Dans une perspective contemporaine, le répertoire et l'index du répertoire – s'ils sont tenus conformément aux règlements – sont aussi efficaces qu'un dictionnaire ; fort utiles pour une référence, mais supérieurs dans leur version technologique, vu l'efficacité accrue que permet les diverses fonctions programmables. Nous pouvons envisager que, dans le cas de la numérisation du greffe, la « recherche » d'une minute sera réduite à quelques secondes, soit le temps nécessaire au chargement d'un dossier à l'écran.

* * *

L'exercice critique que nous venons d'effectuer nous permet un certain nombre de conclusions préliminaires. La première, que nous avons posée comme hypothèse au début de la présente section, découle du fait que les mesures jugées comme étant raisonnables pour un notaire pratiquant sous le modèle actuel offrent un niveau de sécurité sans doute inférieur au sentiment de sécurité des notaires et de leurs clients. Bref, les actes notariés sont, en fait, moins bien protégés que ne pourrait le croire un observateur neutre. Cela

171. Voir également l'article 31 du *Règlement sur la tenue des dossiers et des études des notaires*, préc., note 79. Notons que le contenu de ces dispositions est repris à l'article 66 de la *Loi sur le notariat* (préc., note 14), bien que celui-ci ne soit toujours pas entré en vigueur.

172. LN2, art. 19 ; *Règlement sur la tenue des dossiers et des études des notaires*, *ibid.*, art. 32 ; A. ROY, préc., note 9, p. 64. Les articles 98(2) et 98(4) de la *Loi sur le notariat* (*ibid.*) prévoient que le répertoire pourra être conservé sur un support dématérialisé.

implique par ailleurs qu'il serait relativement simple, contrairement à ce qui est soutenu par les défenseurs du *statu quo*, de s'assurer d'un niveau de sécurité équivalent advenant le passage vers un greffe électronique. En effet, à la lumière de ce qui précède, et en mettant pour l'instant de côté la lettre des textes de loi applicables à la pratique notariale, il serait envisageable de procéder à une migration vers le numérique des actes notariés si des mécanismes étaient mis en place pour assurer une équivalence fonctionnelle avec les fonctionnalités identifiées ci-après :

Fonctionnalité	**Composante de sécurité assurée**	**Mécanisme actuel**	**Mécanisme technologique**
Identification des parties	Irrévocabilité Authentification	Vérification par le notaire ; signature des parties	Vérification par le notaire ; mot de passe/code
Manifestation du consentement des parties	Irrévocabilité	Signature des parties et des témoins	Mot de passe/code
Identification du notaire	Irrévocabilité Authentification	Signature du notaire et sceau	Signature numérique du notaire
Octroi d'un caractère authentique à l'acte	Irrévocabilité	Signature du notaire et sceau	Signature numérique du notaire
Assurer la pérennité de l'acte et de son contenu	Disponibilité Intégrité	Papier et encre ; coffre-fort	Format normalisé ; redondances
Assurer l'inaltérabilité de l'acte et de son contenu	Intégrité Irrévocabilité	Ratures ; indication du nombre de mots	Fichier protégé et/ou chiffré
Permettre de retrouver un acte	Disponibilité	Minute ; Répertoire et index du répertoire	Fonction de recherche

Notons que ce tableau ne fait pas mention de l'obligation de confidentialité, bien qu'elle sera facilitée par le dépôt du document confidentiel dans le coffre-fort du notaire (le cas échéant), puisqu'elle n'est pas tant liée à un mécanisme précis identifié ci-dessus qu'à des politiques et de bonnes pratiques adoptées par le notaire afin de satisfaire ses obligations législatives et déontologiques.

2. La sécurité des actes notariés dématérialisés – projections

Alors que la première partie de ce texte visait principalement à identifier l'état de la sécurité des actes notariés, nous nous tournons maintenant vers le futur afin, notamment, d'imaginer comment le cadre législatif actuel devra être adapté aux réalités du numérique. En effet, malgré le fait que le législateur ait, suivant les articles 35 et 39 de la *Loi sur le notariat*, ouvert la porte à la création d'actes et autres documents sous format technologique, cette ouverture demeure sujette à l'adoption d'un règlement à cet effet par le Conseil d'administration de la Chambre. Bien que nous comprenions que cette réglementation soit en processus de rédaction, il demeure pour l'instant que le recours au papier, à une encre de qualité, aux signatures manuscrites des parties prenantes, etc. demeure de mise. En effet, l'article 2813 du *Code civil du Québec* nous rappelle que « [l]'acte authentique est celui qui a été reçu ou attesté par un officier public compétent selon les lois du Québec ou du Canada, avec les formalités requises par la loi » [notre soulignement].

Si, comme nous l'avons abordé en première partie, les formalités présentement « requises par la loi » ont toutes un ou plusieurs équivalents technologiques[173], la question devient donc celle d'identifier laquelle ou lesquelles privilégier afin d'assurer la sécurité d'actes notariés dématérialisés. La présente partie vise ainsi à identifier les mesures envisageables, c'est-à-dire de dresser un portrait des solutions technologiques assurant un niveau de sécurité fonctionnellement équivalent aux mesures de sécurité actuellement mises en œuvre par les notaires (2.2). Avant de ce faire, il importe toutefois de comprendre les risques associés à la dématérialisation des actes notariés (2.1), puisque ceux-ci joueront un rôle indéniable dans l'identification des mesures de sécurité à adopter.

2.1 Les risques pour la sécurité des actes notariés dématérialisés

Comme nous l'avons souligné en première partie, et commee l'a démontré la tragédie de Lac-Mégantic, il existe de nombreux risques liés à la disponibilité, à l'intégrité, à la confidentialité, à l'authentification et à l'irrévocabilité des actes notariés suivant le régime juridique actuel. C'est ce qui, selon nous, justifie une migration vers

173. *Loi concernant le cadre juridique des technologies de l'information*, préc., note 8, art. 9.

tion vers un environnement numérique. En effet, « [d]es avantages spécifiques à l'acte authentique électronique sont même à souligner : établissement de l'acte à distance, conservation optimale dans un centre ultra sécurisé et consultation facilitée »[174]. Toutefois, l'avantage le plus important demeure le fait que les documents technologiques peuvent être décuplés sur divers sites, ce qui permet d'en assurer la protection en cas de catastrophe.

Évidemment, le numérique comporte ses propres risques. En effet, les médias regorgent d'exemples de documents technologiques détruits, corrompus ou divulgués accidentellement ou volontairement. Si ces risques sont bien réels, il importe toutefois de ne pas les surévaluer, surtout lorsque comparés à un système imparfait tel que celui présenté sommairement en première partie. Les lignes qui suivent visent donc à circonscrire ces risques afin de faciliter la recherche de mécanismes qui sauront les maintenir à un niveau jugé acceptable.

2.1.1 Les risques relatifs à la disponibilité des actes notariés dématérialisés

Comme nous l'avons déjà souligné, un acte notarié dématérialisé demeure ni plus ni moins un document technologique ; il est donc composé d'informations portées par un support faisant appel à une technologie[175]. Ainsi, la disponibilité de l'acte dépendra ultimement de ces deux composantes. En d'autres mots, l'obligation d'assurer la disponibilité d'un acte notarié dématérialisé visera tant la disponibilité des informations qu'il contient (2.1.1.1) que de l'infrastructure informatique et logicielle sur laquelle il réside (2.1.1.2). Les choix technologiques liés à la création de tout greffe technologique devront donc tenir compte de cette réalité et ne pas entraver l'accès légitime à ces composantes.

2.1.1.1 Disponibilité de l'information

L'obligation d'assurer la disponibilité de données visera principalement, dans le contexte d'actes notariés dématérialisés, la possi-

174. « La sécurité juridique 2.0 : défi remporté ! », dans *La sécurité juridique : un défi authentique*, dossier de presse, 111e congrès des Notaires de France, 2015, en ligne : <https://www.notaires.fr/sites/default/files/DP%20final_Congr%C3%A8s%20des%20notaires%202015.pdf>, p. 11.
175. *Loi concernant le cadre juridique des technologies de l'information*, préc., note 8, art. 3.

bilité pour les signataires de cet acte ou autres parties visées par celui-ci[176] d'y avoir accès en temps opportun[177]. En soi, cette obligation ne cause aucun problème dans un environnement numérique. Au contraire, comme nous l'avons souligné en première partie, il est souvent beaucoup plus facile de retracer un document technologique que son équivalent papier vu les fonctions de recherche associées au numérique. Toutefois, le papier détient un avantage marqué quant à la certitude que, sous réserve d'une conservation adéquate, ce document demeurera consultable dans 10, 15, voire 25 ans. En effet, les actes notariés confectionnés sur papier ou même les antécédents du papier il y a plus d'une centaine d'années sont toujours accessibles et lisibles[178]. Ainsi, pour que l'on puisse considérer qu'un acte notarié dématérialisé assure un niveau de disponibilité fonctionnellement équivalent au papier,

> [l]es moyens technologiques devront [...] assurer l'accès aux données contenues aux actes notariés dématérialisés, quel que soit le logiciel utilisé lors de sa confection. L'acte notarié rédigé et conservé sur support informatique en 2010 devra pouvoir être lu, consulté et imprimé en 2030, même si le logiciel utilisé 20 ans plus tôt n'existe plus ![179]

Or, cette exigence s'avère quelque peu problématique. En effet, pour ne prendre qu'un exemple, les fichiers *Word Perfect* (.WPD) 4.0 (1986) ou 5.1 (1989), formats pourtant dominants il y a à peine 30 ans, sont souvent incompatibles avec les logiciels de traitement de texte d'aujourd'hui[180]. En effet, comme le souligne Marc Lacoursière :

> La pérennité du document électronique est, en théorie, externe au notaire et dépend plutôt de l'évolution de supports technologiques.

176. Pensons à l'exécuteur testamentaire et aux héritiers en matière de testaments notariés.
177. C'est notamment ce qui est prévu à l'article 10 *in fine* de la *Loi sur le notariat*, préc., note 14.
178. Par exemple, au Québec, BAnQ détient certaines archives notariales qui remontent à 1932. Un échantillon de ces documents a d'ailleurs été numérisé et rendu disponible via Internet. Voir la collection de la Bibliothèque nationale, en ligne : <http://bibnum2.banq.qc.ca/bna/notaires/>. Archives Montréal détient également divers actes notariés remontant à l'époque de la fondation. Voir : <https://archivesdemontreal.ica-atom.org/actes-notaries-nos-1-199-1657-1661>. C'est sans compter les actes conservés dans les greffes de certains notaires. Voir : CHAMBRE DES NOTAIRES, préc., note 83, p. 9.
179. A. ROY, préc., note 9, p. 95.
180. Bertrand SALVAS, « Pratique du droit et outils électroniques : les embûches de la technologie », (2004) 106 *R. du N.* 513, par. 129.

> [...] nul ne peut certifier que les instruments technologiques que nous utilisons de nos jours – versions des logiciels, CD-Rom, clés USB, etc. – seront compatibles avec leurs successeurs dans plusieurs années.[181]

Bertrand Salvas souligne également cette problématique en précisant que le problème de la disponibilité des données ne découle pas des appareils et médiums d'archivage qui par « [l]'adoption de bonne pratique de gestion des copies de sauvegarde [permettent] d'assurer la disponibilité presque éternelle des fichiers en tant que tels »[182]. Il est plutôt d'avis que les risques découlent de la lisibilité des fichiers sauvegardés, « la question étant en effet de s'assurer que les logiciels de demain puissent toujours décoder et comprendre les fichiers d'hier »[183].

Ainsi, l'obligation d'assurer une certaine pérennité aux actes dématérialisés[184] milite en faveur de l'adoption d'un format unique et pérenne. Elle implique également la révision périodique des formats choisis[185] afin d'éviter de se retrouver dans la situation fâcheuse de ne pas être en mesure de consulter un acte enregistré au greffe.

En effet, comme le prévoit l'article 23 de la *Loi concernant le cadre juridique des technologies de l'information*, « [t]out document auquel une personne a droit d'accès doit être intelligible, soit directement, soit en faisant appel aux technologies de l'information ». Or, un document technologique dans un format abandonné ne remplirait pas cette obligation. Il sera donc important pour la Chambre des

---

181. M. LACOURSIÈRE, préc., note 168.
182. B. SALVAS, préc., note 180, par. 126.
183. *Ibid.*, par. 127.
184. Par exemple, en France, l'article 5 de la Délibération nº 2014-243 du 12 juin 2014 portant adoption d'une norme simplifiée relative aux traitements automatisés de données à caractère personnel mis en œuvre par les notaires aux fins de signature électronique, de dépôt et de conservation des actes authentiques sur support électronique au sein du Minutier central électronique des notaires de France (MICEN) (NS-055) prévoit que : « Les informations relatives à l'acte sont conservées soixante-quinze ans à compter du dépôt ».
185. C'est notamment ce qui est prévu en France où « [l]e reformatage régulier du MICEN prévu par la loi et l'adaptation du format des fichiers dans le temps permettent de suivre les mutations technologiques et assurent la pérennité des données ». Voir : « La sécurité juridique 2.0 : défi remporté ! », préc., note 174, p. 11. Selon Marc Lacoursière, l'adoption d'une telle politique découlerait implicitement de l'obligation de diligence raisonnable imposée aux notaires. Voir : M. LACOURSIÈRE, préc., note 168.

notaires[186] de prévoir des lignes directrices afin que tout acte notarié soit produit dans un format pérenne reconnu. Les formats utilisés en matière d'archivage, notamment ceux ayant reçu l'aval de Bibliothèque et archives nationales du Québec (BAnQ) ou de l'Organisation internationale de normalisation (ISO) constituent des options qui méritent d'être évaluées. Parmi les critères à retenir, mentionnons le fait qu'un format doit être ouvert[187], accessible[188] et « léger »[189].

2.1.1.2 Disponibilité des infrastructures

La disponibilité de l'information ne pourra être assurée à moins que les infrastructures informatiques et logicielles où sont hébergées ces données ou encore qui en permettent la lecture ou l'analyse soient elles-mêmes disponibles. En effet, la mise en œuvre d'un greffe technologique – peu importe la forme qu'il prendra – nécessitera la mise en place d'un plan de continuité des activités[190] advenant une panne des serveurs ou une perte de connexion au réseau local, voire à Internet (selon le modèle retenu). Au-delà de l'obligation déontologique qui incombe au notaire de « permettre à son client de prendre connaissance des documents qui le concernent dans tout dossier et, sous réserve de dispositions législatives incompatibles, d'obtenir copie de ces documents »[191], l'adoption d'un plan de continuité des activités est imposé par l'article 19 de la *Loi concernant le cadre juridique des technologies de l'information*, lequel prévoit : « [t]oute personne doit, pendant la période où elle est tenue de

186. Conformément à son obligation d'« établir des normes de sécurité relatives à l'utilisation des technologies de l'information pour la réception des actes notariés ». *Loi sur le notariat*, préc., note 14, art. 98(5).
187. Par exemple, en Italie, seuls les formats ouverts sont considérés. Voir : Pasquale STARACE, « Processi di trasmissione ed elaborazione documentazione giuridica », (2013) en ligne : <http://www.dis.uniroma1.it/~tenace/download/ischia/PresentazioneSicurezza.pptx>.
188. Nous faisons ici allusion au fait qu'un format doit être couramment utilisé.
189. Nous faisons ici allusion au fait que certains formats sont plus « lourds » que d'autres. Par exemple, un fichier audio en format Mp3 occupera une fraction de l'espace disque requis pour le même fichier enregistré en format PCM.
190. « Plan visant à assurer le rétablissement en temps opportun ou la disponibilité continue des fonctions et services opérationnels de l'entreprise dans l'éventualité où les ressources habituelles, comme les bureaux, les terminaux, les micro-ordinateurs et les réseaux, cesseraient d'être disponibles ». OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Le grand dictionnaire terminologique*, 2006, « Plan de continuité des activités », en ligne : <http://www.granddictionnaire.com/index.aspx>.
191. Art. 42 du *Code de déontologie des notaires*, préc., note 46.

conserver un document [...] voir à la disponibilité du matériel qui permet de le rendre accessible et intelligible et de l'utiliser aux fins auxquelles il est destiné ». En effet, même si un acte notarié est théoriquement disponible, l'article 42 du *Code de déontologie des notaires* ne sera, à notre avis, pas respecté si le serveur sur lequel l'acte est hébergé devient inaccessible ou si les données qui composent cet acte sont chiffrées ou dans un langage que les logiciels disponibles sont incapables de décoder.

L'obligation d'assurer la disponibilité des actes soulève d'ailleurs une question importante quant à la forme du greffe. En effet, si certains notaires préféreront sans doute établir leur propre greffe, la création d'un greffe universel contrôlé par la Chambre[192] – similaire au modèle français[193] – n'est pas sans intérêt, notamment parce que si l'achat d'un coffre-fort ne nécessite aucune connaissance particulière, l'entretien de serveurs sécurisés exige une expertise que peu de notaires détiennent. Évidemment, le notaire pourra choisir de confier l'entretien et la garde des serveurs sur lesquels est hébergé son greffe à un tiers, mais cela requerra des précautions afin de s'assurer que des tiers ne pourront avoir accès à l'information hébergée et que l'hébergeur ne pourra s'approprier ladite information ou en empêcher l'accès[194]. Il sera également important de surveiller la situation financière de l'hébergeur pour éviter une perte de disponibilité due à la faillite de ce dernier[195].

La présence d'un greffe offert par la Chambre (ou un tiers accrédité) offre un autre avantage en matière de disponibilité advenant le décès d'un notaire. En effet, s'il est possible d'obtenir l'autorisation de procéder à l'ouverture d'un coffre-fort si les personnes qui en connaissent la combinaison ou en possèdent la clé sont indisponibles, un serveur sécurisé, (un identifiant biométrique, par exemple) demeurera dans bien des cas impénétrable selon le type d'algorithme utilisé et la force du mécanisme d'identification. La Chambre des notaires devra donc imposer la création d'un mécanisme lui permettant l'accès aux greffes des membres en cas de décès, ce qui est évidemment plus simple si elle assure elle-même la gestion de ces greffes.

---

192. Cette approche est notamment proposée par Marc Lacoursière. Voir : M. LACOURSIÈRE, préc., note 168. Voir également I. DE LAMBERTERIE, préc., note 168.
193. Voir la section 2.2 pour une description de ce modèle.
194. Voir N. VERMEYS, J.M. GAUTHIER et S. MIZRAHI, préc., note 51.
195. *Ibid.*

Finalement, peu importe le modèle retenu, le mot d'ordre demeure la redondance des systèmes[196]. Comme nous l'avons mentionné plus haut, il s'agit de la principale mesure de sécurité visant à assurer la disponibilité des documents et, à vrai dire, le principal facteur de sécurité militant en faveur d'une dématérialisation des actes notariés.

2.1.2 Les risques relatifs à l'intégrité des actes notariés dématérialisés

Nous l'avons vu, l'article 6 de la *Loi concernant le cadre juridique des technologies de l'information* prévoit que « [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 ». Le notaire devra donc s'assurer de mettre en place des mécanismes propres à assurer l'intégrité des informations durant chacune des étapes du cycle de vie des actes créés, d'autant que cette obligation est réitérée aux articles 35 et 39 de la *Loi sur le notariat*.

Les risques pouvant guetter un acte notarié dématérialisé en matière d'intégrité sont évidents. Il s'agit du cas où un individu, qu'il s'agisse d'un tiers malveillant ou d'un employé négligent, viendrait modifier l'acte. En effet, s'il est possible d'apporter des modifications à un texte imprimé, cela demeure tout de même plus difficile que de modifier son équivalent technologique. Soit, il existe des façons de vérifier si l'intégrité d'un document a été touchée, notamment par la consultation des métadonnées y associées[197], mais ce type de vérifi-

---

196. C'est notamment l'approche choisie en France : J.H., « 75 ans de conservation pour les actes authentiques des notaires », (2010) *Les Echos*, en ligne : <https://www.lesechos.fr/01/06/2010/LesEchos/20688-045-ECH_75-ans-de-conservation-pour-les-actes-authentiques-des-notaires.htm> et en Italie : P. STARACE, préc., note 187. Dans les deux cas, les systèmes prévoient des redondances sur des serveurs situés dans des zones géographiques distinctes. En France, on précise même que les serveurs sont « dupliqués en deux sites placés sur deux plaques tectoniques différentes ». Voir : Bertrand LEMAIRE, « La France signe et archive le premier acte notarié dématérialisé au monde », (2008) *Le Monde Informatique*, en ligne : <http://www.piaf-archives.org/actualites/la-france-signe-et-archive-le-premier-acte-notari%C3%A9-d%C3%A9mat%C3%A9rialis%C3%A9-au-monde>.

197. Sur cette question, voir : François SENÉCAL et Patrick GINGRAS, « Métadonnées : Plaidoyer pour des mal aimées et des incomprises », (2015) 74 *R. du B.* 249.

cation en aval arrive nécessairement trop tard puisque l'acte aura perdu sa valeur juridique.

Il importe donc de prévoir non seulement un mécanisme permettant de valider le fait que l'intégrité du document est demeurée intacte[198], mais également un mécanisme permettant de protéger le document contre toute forme d'altération. Ce mécanisme peut découler de l'une des fonctionnalités offertes par le format sélectionné, ou par un logiciel distinct.

2.1.3 Les risques relatifs à la confidentialité des actes notariés dématérialisés

L'obligation de confidentialité du notaire demeure évidemment la même peu importe le support sur lequel un acte en particulier est enregistré. Le défi du notaire réside ainsi dans le maintien de sa vigilance quant aux autres personnes qui ont accès aux renseignements confidentiels de ses clients. Le notaire a l'obligation de surveiller que son personnel ne communique pas à un tiers un renseignement confidentiel protégé par le secret professionnel[199]. Une divulgation de renseignement personnel et confidentiel par un employé ou un stagiaire pourrait en effet engager la responsabilité du notaire[200].

Évidemment, si les risques sont théoriquement les mêmes, les menaces et vulnérabilités diffèrent. En effet, si le non-respect de

---

198. Par exemple, le service de *Dépôt notarial électronique* français génère une empreinte électronique de chaque document qui y est déposé. Comme l'explique le site officiel du service : « L'empreinte électronique est à un document ce que l'empreinte génétique est à un individu. Si on change, ne serait-ce qu'une virgule dans un document, son empreinte change. Un document ne peut pas être reconstitué à partir de son empreinte. L'empreinte est construite en combinant deux algorithmes de chiffrement irréversible (dénommés SHA-256 et SHA-1) rendant impossible que deux documents distincts produisent la même empreinte ». Le site poursuit en précisant que « [l]a concordance des empreintes calculées lors du dépôt et de la restitution permet de prouver : la conformité du document en prouvant que le document restitué est bien celui qui existait avec la concordance des empreintes lors de la restitution, le notaire est en mesure de prouver que le document restitué est identique à celui qui a été déposé ». Voir : SITE OFFICIEL DU DÉPÔT ÉLECTRONIQUE NOTARIAL, en ligne : <http://www.depotelectronique.fr/>.
199. *Code de déontologie des notaires*, préc., note 46, art. 39.
200. Art. 2088 C.c.Q. ; P.-Y. MARQUIS, préc., note 151, p. 194 ; Jean-Louis BAUDOUIN, « Le secret professionnel en droit québécois et canadien », (1974) 5 *R.G.D.* 1, 11 et 12.

l'obligation de confidentialité pour un document physique implique qu'un tiers devra se déplacer sur les lieux où se situe le greffe du notaire, le greffe numérique, en supposant qu'il est connecté à un réseau quelconque (ce qui s'avère nécessaire pour faciliter la redondance permettant d'assurer la disponibilité des actes), deviendra accessible pour quiconque est en mesure de se connecter au réseau sur lequel ce greffe est situé. D'où l'importance de sécuriser ce réseau et d'effectuer une surveillance des activités qui y ont lieu. Par exemple, en France, la *Délibération nº 2014-243 du 12 juin 2014* prévoit que « [l]e MICEN qui reçoit et conserve les actes n'est interconnecté à aucun autre système »[201], limitant ainsi les risques qu'un tiers puisse accéder au réseau du MICEN à l'aide d'objets connectés[202].

Comme mentionné en première partie, dès qu'une information confidentielle se retrouve à l'intérieur d'un document technologique (en l'occurrence, un acte notarié dématérialisé), c'est l'article 25 de la *Loi concernant le cadre juridique des technologies de l'information* qui vient établir les obligations de l'entité responsable dudit document (en l'occurrence, le notaire). En vertu de cette disposition, le notaire « responsable de l'accès à un document technologique qui porte un renseignement confidentiel doit prendre les mesures de sécurité propres à en assurer la confidentialité »[203].

Pour ce faire, plusieurs procédés et technologies peuvent être mis en œuvre dont ceux énumérés à l'article 25 de la *Loi concernant le cadre juridique des technologies de l'information*, à savoir :

- Un contrôle d'accès effectué au moyen d'un procédé de visibilité réduite[204] ;

201. Délibération nº 2014-243 du 12 juin 2014 portant adoption d'une norme simplifiée relative aux traitements automatisés de données à caractère personnel mis en œuvre par les notaires aux fins de signature électronique, de dépôt et de conservation des actes authentiques sur support électronique au sein du Minutier central électronique des notaires de France (MICEN) (NS-055), art. 2 *in fine*.
202. « Matériel électronique qui peut envoyer et recevoir des informations par le biais d'une liaison sans fil avec un téléphone intelligent, une tablette ou un ordinateur ». OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Le grand dictionnaire terminologique*, 2015, « Objet connecté », en ligne : <http://granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=26529868>.
203. *Loi concernant le cadre juridique des technologies de l'information*, préc., note 8, art. 25.
204. Par exemple, en France, il est prévu que « [l]es techniciens chargés de la maintenance du MICEN ont accès, pour des raisons d'administration technique et

(à suivre…)

- Un contrôle d'accès effectué au moyen d'un procédé qui empêche une personne non autorisée de prendre connaissance du renseignement.

Ces contrôles d'accès peuvent notamment impliquer l'utilisation de mesures de chiffrement des données, de mots de passe, etc. et varieront selon les types de renseignements collectés. En effet, il importe de rappeler que l'article 10 de la *Loi sur la protection des renseignements personnels dans le secteur privé* prévoit que les mesures de sécurité à mettre en place doivent être raisonnables selon la sensibilité, la finalité, la quantité et la répartition des renseignements, ainsi que le support sur lequel ils se retrouvent. Bref, elles se doivent d'être adéquates et proportionnelles aux dommages envisagés en cas d'ingérence ou de divulgation.

Ainsi, l'article 25 de la *Loi concernant le cadre juridique des technologies de l'information* vient en quelque sorte compléter et étendre les obligations prévues à l'article 16 du *Règlement sur la tenue des dossiers et des études des notaires* :

> Le notaire qui utilise le support informatique pour le traitement et la conservation de tout ou partie des éléments, renseignements et documents relatifs à un dossier doit :
>
> 1º sauvegarder les données ainsi recueillies et en conserver une copie conformément à l'article 32 ;
>
> 2º utiliser une base de données distincte de toute autre pour la tenue des dossiers visés au présent règlement ;
>
> 3º protéger l'accès de ces données notamment par l'utilisation d'un mot de passe.

Pour compléter la liste des mesures de sécurité devant être mises en œuvre afin de protéger un acte notarié dématérialisé, l'article 4.7 et l'annexe 1 de la *Loi sur la protection des renseigne-*

(...suite)
fonctionnelle, aux fichiers conservés dans la base, sans possibilité de consultation du contenu d'un acte ». Délibération nº 2014-243 du 12 juin 2014 portant adoption d'une norme simplifiée relative aux traitements automatisés de données à caractère personnel mis en œuvre par les notaires aux fins de signature électronique, de dépôt et de conservation des actes authentiques sur support électronique au sein du Minutier central électronique des notaires de France (MICEN) (NS-055), art. 4.

ments personnels et les documents électroniques[205], bien qu'il ne soit pas directement applicable en l'occurrence, offre un éclairage intéressant en précisant la nécessité d'aborder la sécurité sous trois angles distincts[206].

Premièrement, le notaire devra prévoir l'adoption de mesures de sécurité de nature matérielle telles que le verrouillage des classeurs ou l'accès limité au bureau[207]. En effet, un acte dématérialisé se retrouvera nécessairement sur un serveur ou autre support informatique, lequel sera situé en un lieu géographique donné. Ainsi, sans limiter l'accès physique à ce support, l'on ne saurait assurer la confidentialité des documents qu'il héberge.

Deuxièmement, il devra prévoir l'adoption de mesures de sécurité de nature administrative telles que des autorisations sélectives pour le personnel, une politique relative à la divulgation d'information aux tiers, etc.[208]. L'adoption de telles politiques s'avère nécessaire pour bien établir non seulement les mesures de sécurité physique et techniques à mettre en place, mais également pour identifier les rôles et responsabilités de chacun dans leur respect, leur maintien et leur mise à jour. En effet, il importe de rappeler qu'une politique de sécurité ou, pour être plus exact, les mesures de sécurité qu'elle met de l'avant soit directement, soit à l'aide de guides, de procédures ou d'autres documents auxquels elle renvoie[209], est un document vivant qui nécessite une réévaluation continue[210].

Finalement, des mesures de sécurité de nature technique devront également être adoptées. Nous nous référons ici aux types de mesures déjà identifiées comme l'utilisation d'un mot de passe ou

---

205. *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, ch. 5 (ci-après « LPRDE »).
206. LPRDE, Annexe 1, art. 4.7. En effet, l'annexe 1 reprend les principes énoncés dans la norme nationale du Canada intitulée « Code type sur la protection des renseignements personnel », CAN/CSA-Q830-96.
207. Raymond DORAY, « Le notaire et la protection des renseignements personnels », (2006) 1 *C.P. du N.* 53, 66 ; LPRDE, art. 5(1) et annexe 1, art. 4.7.3a).
208. LPRDE, annexe 1, art. 4.7.3b) et 4.7.4.
209. Voir N.W. VERMEYS, préc., note 6, p. 78 et s.
210. Par exemple en France, le notaire se doit de voir à « la mise à jour des mesures de sécurité au regard de la réévaluation régulière des risques ». Voir Délibération nº 2014-243 du 12 juin 2014 portant adoption d'une norme simplifiée relative aux traitements automatisés de données à caractère personnel mis en œuvre par les notaires aux fins de signature électronique, de dépôt et de conservation des actes authentiques sur support électronique au sein du Minutier central électronique des notaires de France (MICEN) (NS-055), art. 7.

le chiffrement des actes[211]. Une autre mesure technique à mettre en œuvre visera à limiter les recherches rapides à l'intérieur d'actes dématérialisés pour y puiser certains renseignements personnels utiles. En effet, il est utile de rappeler que de telles pratiques sont soumises aux balises imposées par l'article 24 de la *Loi concernant le cadre juridique des technologies de l'information* :

> L'utilisation de fonctions de recherche extensive dans un document technologique qui contient des renseignements personnels et qui, pour une finalité particulière, est rendu public doit être restreinte à cette finalité. Pour ce faire, la personne responsable de l'accès à ce document doit voir à ce que soient mis en place les moyens technologiques appropriés [...].

Que représente une telle limitation pour le notaire ? Bien qu'elle semble aller plus loin que ce qu'exige le législateur québécois, la position de son homologue français paraît intéressante : « Seule une recherche sur les données renseignées par l'office au moment de l'inscription de l'acte et permettant son indexation est possible, à l'exclusion de toute recherche plein texte dans le corps de l'acte. »[212]

Pour résumer ce qui précède, l'introduction des actes notariés dématérialisés nécessitera une révision des mesures de sécurité à être adoptées au sein d'études notariales. Elle impliquera la réévaluation de mesures de sécurité existantes, une modification de la conduite du personnel dans sa manipulation d'actes notariés, ainsi que l'adoption de nouvelles mesures de sécurité propres à l'environnement technologique associé à la tenue d'un greffe virtuel ou d'un minutier électronique central.

2.1.4 Les risques relatifs à l'authentification des actes notariés dématérialisés

En matière d'actes notariés, l'authentification peut renvoyer à deux concepts distincts. Il peut s'agir de l'authentification des signataires de l'acte (2.1.4.1) ou de l'authentification de l'acte lui-même (2.1.4.2). Si ces deux concepts demeurent intrinsèquement liés, ils impliquent des risques distincts.

---

211. LPRDE, annexe 1, art. 4.7.3c).
212. Délibération nº 2014-243 du 12 juin 2014 portant adoption d'une norme simplifiée relative aux traitements automatisés de données à caractère personnel mis en œuvre par les notaires aux fins de signature électronique, de dépôt et de conservation des actes authentiques sur support électronique au sein du Minutier central électronique des notaires de France (MICEN) (NS-055), art. 4.

2.1.4.1 Authentification des signataires

En matière d'authentification des parties à un acte notarié dématérialisé, le principal risque n'est pas propre à l'informatique. Il découle plutôt du fait qu'un notaire pourrait manquer à sa tâche de bien identifier les signataires, voire de consentir lui-même ou elle-même à l'acte pour son client. Évidemment, comme cela irait à l'encontre des obligations déontologiques[213] et légales[214] du notaire, ce risque demeure faible ou, tout au moins, une contre-mesure viable existe déjà afin de le mitiger.

Toutefois, ce risque est accentué si l'acte est signé hors de la présence physique du notaire. En effet, s'il est admis qu'un acte notarié doit normalement être signé « en présence du notaire instrumentant »[215], le troisième alinéa de l'article 50 de la *Loi sur le notariat* ouvre la porte à la signature hors la présence du notaire[216] :

> Dans les limites et suivant les conditions prévues par règlement du Conseil d'administration, la signature des parties et des témoins à un acte reçu sur un support autre que le papier, peut être apposée hors de la présence du notaire et celui-ci n'est pas alors tenu de signer l'acte au même lieu où la dernière des parties à signer l'a fait.

Cette position, laquelle s'inscrit tant dans la foulée de la *Loi concernant le cadre juridique des technologies de l'information* que de récentes ouvertures jurisprudentielles[217], impliquera donc que l'authentification du signataire puisse être assurée par un processus ou un document technologique. Notons d'emblée que ce mode d'authentification ne cause pas problème puisque « [l]orsque la loi exige de fournir une attestation, une carte, un certificat, une pièce ou une preuve d'identité ou un autre document servant à établir l'identité d'une personne, cette exigence peut être satisfaite au moyen d'un document faisant appel à la technologie appropriée à son support »[218].

---

213. Voir notamment l'article 1 du *Code de déontologie des notaires*, préc., note 46.
214. Voir notamment l'article 43 de la *Loi sur le notariat*, préc., note 14.
215. *Ibid.*, art. 50 al. 1.
216. Sur cette question, voir : M. LACOURSIÈRE, préc., note 168, section 2.3.4.1.
217. Voir *Entreprises Robert Mazeroll Ltée* c. *Expertech – Batisseur de réseaux Inc.*, 2005 CanLII 131 (QC C.Q.).
218. *Loi concernant le cadre juridique des technologies de l'information*, préc., note 8, art. 42.

Par exemple, la *Loi concernant le cadre juridique des technologies de l'information* prévoit le recours possible aux certificats pour « établir un ou plusieurs faits dont la confirmation de l'identité d'une personne »[219]. Bref, le mécanisme de certification encadré par cette loi pourrait, en théorie, être utilisé pour valider l'identité des signataires d'un acte notarié. Notons toutefois que le processus de certification prévu à la *Loi concernant le cadre juridique des technologies de l'information*[220] nous paraît particulièrement lourd[221] et peu attrayant dans un tel contexte.

Quoi qu'il en soit, si l'authentification est faite à l'aide d'un document technologique quelconque, l'intégrité[222] et la confidentialité[223] de celui-ci devront être assurées. La loi prévoit également que ce document devra « en outre être protégé contre l'interception lorsque sa conservation ou sa transmission sur un réseau de communication rend possible l'usurpation de l'identité de la personne visée par ce document »[224].

2.1.4.2 Authentification des actes

L'authentification de l'acte notarié dématérialisé est sujette aux mêmes risques que son homologue papier : comment s'assurer qu'un document donné soit réellement authentique ? Évidemment, l'article 2813 du Code civil crée une présomption à cet effet, mais cette présomption n'est pas irréfragable. Pour l'acte dématérialisé, la signature numérique du notaire, jumelée aux mécanismes visant à en assurer l'intégrité devrait suffire. Par ailleurs, rappelons que le recours à un certificat pourrait également constituer un mécanisme valide d'authentification des actes, puisque l'article 47 de la *Loi concernant le cadre juridique des technologies* prévoit qu'un certificat peut notamment servir à établir l'existence de certains attributs d'un document.

---

219. *Ibid.*, art. 47.
220. Voir les articles 47 à 62 de la *Loi concernant le cadre juridique des technologies de l'information*, *ibid.*
221. Notons d'ailleurs que ces dispositions n'ont, à ce jour, fait l'objet d'aucune interprétation de la part des tribunaux.
222. *Loi concernant le cadre juridique des technologies de l'information*, préc., note 8, art. 40 et 41.
223. *Ibid.*, art. 41.
224. *Ibid.*

2.1.5 Les risques relatifs à l'irrévocabilité des actes notariés dématérialisés

Il va de soi que le lien entre un acte notarié et ses signataires devra être établi. Ce truisme demeure évidemment au cœur des préoccupations des notaires en matière d'actes dématérialisés, notamment lorsqu'un acte est « signé » hors la présence du notaire instrumentant[225]. Ici, la *Loi concernant le cadre juridique des technologies de l'information* expose les critères qu'un mécanisme permettant d'assurer l'irrévocabilité des actes notariés dématérialisés devrait respecter :

> **38.** 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. [Nos soulignements]

Notons ici que cette disposition ne limite pas à une signature (ou une marque personnelle)[226] les mécanismes envisageables. Le recours à un identifiant et à un mot de passe pourrait, à notre avis, satisfaire à cette exigence. Au même titre, le recours à une signature numérique n'est clairement pas nécessaire pour arriver aux fins fixées. Une signature manuscrite numérisée sous la forme d'un fichier « jpeg » ou autre semble suffisant. D'ailleurs, est-il utile de le rappeler, la Cour du Québec a déjà donné son aval à une telle pratique :

> [...] lLa signature électronique d'un avocat sur une procédure est valable et que le greffe aurait dû accepter et noter au plumitif l'inscription et la déclaration (274.1 C.p.c.).
>
> Il est possible que le refus du greffe soit associé à la crainte que l'acceptation de la signature électronique pose un danger de fraude, de contrefaçon et de fabrication de faux accru. L'avocat n'est pas à l'abri de ces risques, mais s'il en est victime, il pourra contester la

225. *Loi sur le notariat*, préc., note 14, art. 50 al. 3.
226. Art. 2827 C.c.Q.

> signature (2828 C.c.Q.). Cependant, ce fait ou cette possibilité ne rend toutefois pas pour autant la signature électronique invalide.[227]

Si cette situation peut surprendre à première vue, elle est pourtant conforme aux pratiques actuelles en matière de dépôt des procédures. Qui plus est, pour revenir à l'objet de notre étude, comme la signature de l'acte notarié dématérialisé s'inscrit dans un processus impliquant plusieurs mécanismes de validation du consentement des signataires, l'apposition d'une image de signature, voire d'une signature « tapuscrite », semble suffisante selon le contexte (possibilité pour le notaire de confirmer qui appuie sur le clavier au moment de la « signature » de l'acte). Il s'agit d'ailleurs de l'approche favorisée en France :

> L'acte, dématérialisé dans un format XML et au format PDF/A, est associé à ses annexes (un scan de plan...) et [aux] signatures manuscrites scannées des parties [...]. L'ensemble est alors signé électroniquement par le notaire, ce qui lui donne sa valeur. La signature des parties n'a donc pas besoin d'être électronique, ce qui dispense les signataires d'acquérir chacun un certificat propre à validité limitée dans le temps.[228]

Bref, nous nous retrouvons ici dans un cas d'analyse de risques où le procédé adopté conformément à l'article 38 de la *Loi concernant le cadre juridique des technologies de l'information* devra être choisi en fonction du niveau de certitude requis dans un contexte donné. Lorsque les risques de faux documents sont plus élevés, lorsque les conséquences sont plus dramatiques, ou lorsque le notaire n'est pas en mesure de voir de ses propres yeux qui consent à la signature de l'acte, il sera préférable d'utiliser un procédé plus sophistiqué comme le chiffrement à clé publique :

> Les algorithmes asymétriques assurent la non-répudiation d'un message signé dans la mesure où seul l'expéditeur possède la clé secrète utilisée pour cette signature, ce qui empêche le récepteur de simuler une transmission à la place de l'expéditeur.[229]

---

227. *Roussel* c. *Desjardins Sécurité financière, compagnie d'assurance-vie*, préc., note 120.
228. B. LEMAIRE, préc., note 196.
229. OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Le grand dictionnaire terminologique*, 2005 « Non-répudiation », en ligne : <http://www.granddictionnaire.com/index.aspx>.

En revanche, comme nous l'avons déjà souligné, un tel mécanisme, n'étant pas « utilisé de façon courante »[230] par une majorité de signataires, pourrait être considéré comme invalide. Qui plus est, la complexité du processus de validation pour obtenir une telle signature ne semble pas justifier d'y recourir. Ces arguments militent donc, encore une fois, en faveur d'un mécanisme moins sécuritaire, mais offrant un niveau de sécurité raisonnable tel le binôme « nom d'utilisateur » – « mot de passe ».

2.2 Les solutions technologiques assurant un niveau de sécurité fonctionnellement équivalent aux mesures de sécurité actuellement mises en œuvre par les notaires

Une analyse des précédentes sections et sous-sections du présent texte nous aura permis d'identifier les composantes sécuritaires nécessaires à un écosystème visant la création, la modification, la conservation, voire l'éventuelle destruction d'actes notariés dématérialisés ou, pour reprendre l'expression utilisée par le législateur québécois, le cycle de vie[231] des actes notariés dématérialisés.

La question devient alors de savoir s'il existe une ou des technologies pouvant répondre aux impératifs sécuritaires que nous avons identifiés. En effet, le retard des notaires dans la numérisation de leurs procédés pourrait s'expliquer en partie par le fait que, lors de la réforme de 2000, certains estimaient que « [l]es moyens technologiques [...] disponibles et accessibles [n'étaient] pas à même d'assurer le respect des exigences de sécurité et d'inaltérabilité qu'impose la loi en matière d'actes notariés »[232]. Or, plus de 15 ans plus tard, nous considérons que cette prétention n'est simplement plus valide.

Afin de tester cette hypothèse, nous avons jugé utile de la confronter à des modèles technologiques existants, soit ceux adoptés dans certains pays. En effet, comme le souligne une étude préparée par la Commission européenne pour l'efficacité de la justice (CEPEJ)[233], les notaires de plusieurs États européens ont déjà entamé une migration vers la dématérialisation de leurs actes :

---

230. Art. 2827 C.c.Q.
231. *Loi concernant le cadre juridique des technologies de l'information*, préc., note 8, art. 6.
232. A. ROY, préc., note 9, p. 95.
233. COMMISSION EUROPÉENNE POUR L'EFFICACITÉ DE LA JUSTICE, « Étude spécifique de la CEPEJ sur les professions juridiques », (2017) en ligne : (à suivre...)

> En Autriche, en Estonie et en France, des documents juridiques entièrement dématérialisés sont conservés dans un système d'archivage électronique centralisé. L'Autriche s'est dotée, il y a plus de 30 ans, de registres notariaux électroniques. Aujourd'hui, les notaires autrichiens peuvent s'appuyer sur des registres électroniques sûrs, efficaces et acceptés de tous tels que le Registre central autrichien des testaments, le Séquestre du notariat autrichien, le Registre central autrichien des pouvoirs de représentation et le Registre des testaments de vie du notariat autrichien.[234]

En France, où les actes notariés dématérialisés sont utilisés depuis 2008[235], la sécurité de ceux-ci repose sur trois piliers :

- le réseau privé des notaires ;
- la signature électronique qualifiée ; et
- les serveurs d'archivages de Real.not dupliqués en deux sites placés sur deux plaques tectoniques différentes[236].

Concrètement, le cycle de vie des actes notariés dématérialisés français peut être décrit ainsi :

- Le notaire prépare, comme aujourd'hui, l'acte sur un logiciel de rédaction. Ensuite, il scanne l'ensemble des pièces annexes afin de les joindre électroniquement à l'acte. L'ensemble formera l'acte à régulariser.
- Lors du rendez-vous de signature, le notaire présente au client l'acte sur écran. La lecture se fait directement sur cet écran [et] peut être suivie par l'ensemble des parties au contrat. Le notaire valide le contenu de l'acte et des annexes. Cette validation se fait avec les outils informatiques de signature qui sont accessibles grâce à la clé « Real » du notaire (clé informatique cryptée contenant l'identification et la signature du notaire et qui ressemble à une clé USB), protégée par un code secret.

(...suite)
<https://rm.coe.int/etude-specifique-de-la-cepej-sur-les-professions-juridiques-contributi/168076ccba>.

234. *Ibid.*, p. 9.
235. B. LEMAIRE, préc., note 196.
236. *Ibid.*

- Cette validation effectuée, l'acte apparaît sur une tablette sur laquelle les signatures des différentes parties pourront être apposées grâce à un stylet électronique.

- La date et le lieu de la signature sont alors validés et les clients signent directement sur la tablette l'acte et les annexes.

- Une fois les différentes signatures recueillies, c'est au notaire de signer l'acte, au moyen là encore de sa clé Real validée par son code secret.

- Le client peut alors recevoir copie de cet acte par voie électronique[237].

Par la suite, l'acte sera enregistré dans un fichier contenant :

- L'acte lui-même avec son texte, ses annexes et les signatures de toutes les parties, les notaires et éventuellement les clercs habilités[238] ;

- Un ensemble de données structurées normalisées (format XML) permettant la recherche de l'acte dans le minutier, ainsi que les échanges de données avec d'autres systèmes (les archives publiques par exemple)[239].

Ce fichier sera finalement « envoyé automatiquement et instantanément sur les serveurs dédiés du notariat dans une sorte de coffre-fort électronique (le Minutier central), auquel seul le notaire signataire a accès »[240].

À la lumière de ce qui précède, il est possible d'affirmer que :

---

237. « L'acte authentique électronique : un rêve devenu réalité », (2012) 23 *La lettre des notaires de France*, en ligne : <https://www.notaires.fr/sites/default/files/janvier%202012.pdf>.
238. « Cette IMAGE de l'acte permettra une restitution, sur écran ou sur papier, de l'acte et des éléments numérisés, IDENTIQUE à celle visualisée par le notaire au moment de la signature ». Voir : Thierry BLANCHET, « La réalisation du Minutier central des notaires de France (la conservation des actes authentiques électroniques) », (2004) en ligne : <http://www.frlii.org/spip.php?article60>.
239. *Ibid.*
240. « L'acte authentique électronique : un rêve devenu réalité », préc., note 237.

> [l]a sécurité des actes électroniques est garantie à tous les niveaux : accès réservé au notaire rédacteur, signature certifiée et inviolable, contenu inaltérable, transferts ultra-sécurisés, audits, veilles permanentes… Le reformatage régulier du MICEN prévu par la loi et l'adaptation du format des fichiers dans le temps permettent de suivre les mutations technologiques et assurent la pérennité des données. Celles-ci, dupliquées en plusieurs lieux distincts sous haute surveillance et mises à jour en temps réel, sont par ailleurs à l'abri de tout évènement destructeur tel qu'inondation, incendie ou tremblement de terre.[241]

Notons que le service décrit ci-dessus est distinct du Dépôt notarial électronique également disponible en France, lequel permet de conserver « [t]ous types de fichiers (texte, son, vidéo, dessin, logiciels, fichiers…) copiés sur un support (CD-Rom, DVD, clé USB, disque dur externe), quel que soit leur volume »[242]. Plus précisément, ce service permet :

- D'assurer la parfaite conservation des documents déposés dans un coffre-fort électronique parfaitement sécurisé ;
- De constituer des preuves certaines de la date de leur dépôt, de leur origine et de leur intégrité ;
- De prouver leur détention par le client à cette date et d'établir la preuve indiscutable de leur conformité au moment de leur restitution à terme ;
- D'établir un lien juridique et technique entre les données conservées dans le coffre-fort électronique et les preuves déposées au rang des minutes de l'étude ; et
- De restituer à tout moment les documents déposés au client[243].

---

241. « La sécurité juridique 2.0 : défi remporté ! », préc., note 174, p. 11.
242. SITE OFFICIEL DU DÉPÔT ÉLECTRONIQUE NOTARIAL, préc., note 198. Voir également « Dépôt électronique notarial : l'association de la meilleure preuve juridique et de la meilleure technologie », en ligne : <http://paris-notaires-services.fr/notaires/depot-electronique-notarial/>.
243. « Dépôt électronique notarial : l'association de la meilleure preuve juridique et de la meilleure technologie », *ibid.* Voir également Anne MOREAUX, « Notariat et transformation numérique », (2017) en ligne : <http://www.affiches-parisiennes.com/notariat-et-transformation-numerique-7333.html>.

Concrètement, le processus implique six étapes décrites dans le site de la Chambre des notaires de Paris[244] :

1. Préparation : Le notaire calcule les empreintes[245].

2. Mise au coffre : Le notaire signe l'enveloppe[246] et la met au coffre-fort électronique (authentification forte par carte à puce).

3. Acte authentique : Dépôt des empreintes et des accusés de mise au coffre par acte authentique au rang de ses minutes.

4. Récupération par le notaire de l'objet du dépôt à la demande et en présence du client.

5. Calcul par le notaire des empreintes de l'enveloppe et contrôle de la concordance avec celles déposées au rang de ses minutes[247]. Restitution des données au client et destruction de toute trace chez le dépositaire.

6. Acte authentique : Dépôt d'un acte de restitution au rang des minutes.

En Italie, bien que l'approche retenue soit quelque peu distincte du modèle français, « les actes notariés peuvent être exécutés

---

244. CHAMBRE DES NOTAIRES DE PARIS, « Service notarial de dépôt électronique », (2007) en ligne : <http://www.fedisa.eu/fedisa2007/fichiers/2007_11_29_09_29_38.pdf>. Voir également, « Dépôt électronique notarial : l'association de la meilleure preuve juridique et de la meilleure technologie » et Anne MOREAUX, *ibid.*

245. « L'empreinte électronique est à un document ce que l'empreinte génétique est à un individu. Si on change, ne serait-ce qu'une virgule dans un document, son empreinte change. Un document ne peut pas être reconstitué à partir de son empreinte. L'empreinte est construite en combinant deux algorithmes de chiffrement irréversible (dénommés SHA-256 et SHA-1) rendant impossible que deux documents distincts produisent la même empreinte ». Voir : SITE OFFICIEL DU DÉPÔT ÉLECTRONIQUE NOTARIAL, préc., note 198.

246. L'enveloppe est constituée « des données du client et des métadonnées d'indexation ». Voir « Dépôt électronique notarial : l'association de la meilleure preuve juridique et de la meilleure technologie », préc., note 242.

247. « La concordance des empreintes calculées lors du dépôt et de la restitution permet de prouver : La conformité du document en prouvant que le document restitué est bien celui qui existait avec la concordance des empreintes lors de la restitution, le notaire est en mesure de prouver que le document restitué est identique à celui qui a été déposé ». Voir : SITE OFFICIEL DU DÉPÔT ÉLECTRONIQUE NOTARIAL, préc., note 198.

sous une forme entièrement numérique » depuis 2010[248]. Ainsi, divers actes notariés sont effectués de façon technologique, notamment :

- les procurations délivrées par les banques[249] ;
- les contrats par lesquels l'État acquiert des biens ou des services[250].

Fait intéressant, la *Legge 16 febbraio 1913 n. 89 Sull'ordinamento del notariato e degli archivi notarili*[251] prévoit même un mécanisme permettant la reconstitution d'actes notariés en cas de perte des actes, répertoires et registres informatiques[252].

Comme c'est le cas en France[253], les parties sont invitées à signer leurs actes à l'aide d'une tablette électronique et d'un stylet. Par contre, la technologie utilisée pour assurer l'authentification du signataire et l'irrévocabilité du lien avec l'acte est plus sophistiquée. En effet, depuis janvier 2016, les notaires italiens ont recours à iStrumentum, un logiciel de signature électronique développé par les entreprises Notartel et Aruba et offert par le Conseil national des notaires[254]. En plus d'apposer l'image de la signature des parties à l'acte, ce logiciel capture et lui associe une série de données biométriques lors de la signature. Ainsi, la pression exercée sur la tablette, la position de la main, la vitesse, l'accélération et le rythme de signa-

---

248. COMMISSION EUROPÉENNE POUR L'EFFICACITÉ DE LA JUSTICE, préc., note 233, p. 8.
249. « [T]outes les grandes banques italiennes émettent maintenant des procurations à l'aide d'actes numériques authentiques notariés, de sorte que les copies numériques puissent être téléchargées partout, en toute sécurité et en temps réel ». COMMISSION EUROPÉENNE POUR L'EFFICACITÉ DE LA JUSTICE, *ibid.*
250. « [C]ertains de ces contrats doivent en effet être exécutés par un acte notarié authentique numérique, ce qui permet à l'État de créer une base de données actualisée, transparente et accessible des principaux contrats ». COMMISSION EUROPÉENNE POUR L'EFFICACITÉ DE LA JUSTICE, *ibid.*
251. Legge 16 febbraio 1913 n. 89 Sull'ordinamento del notariato e degli archivi notarili. (1) (G.U. n. 55, 7 marzo 1913, Serie Generale), art. 62-quater. (1).
252. Notons que ce mécanisme semble similaire à celui mis en place par la *Loi concernant le remplacement et la reconstitution des actes notariés en minute détruits lors du sinistre ferroviaire du 6 juillet 2013 dans la Ville de Lac-Mégantic*, RLRQ, c. R-21.1, mais avec une composante technologique.
253. « L'acte authentique électronique : un rêve devenu réalité », préc., note 237.
254. CONSIGLIO NAZIONALE DEL NOTARIATO, « Atto publico informatico », (2016) en ligne : <http://www.notariato.it/it/atto-pubblico-informatico>.

ture, voire l'inclinaison du stylo, sont enregistrés et permettent de créer un lien indissoluble entre les caractéristiques biométriques du signataire et le document signé[255].

Notons toutefois que si la création d'actes technologiques ne semble pas poser problème, leur conservation demeure source de soucis. En effet, [traduction] « [l]e plus gros problème, cependant, reste celui lié à la création d'une archive électronique qui peut garder tous les documents en conformité avec la loi »[256]. Ce n'est pas dire qu'aucun greffe numérique n'existe en Italie puisque « [l]e Conseil national des notaires fournit [...] sans frais pour l'État, la conservation de tous les documents numériques notariés, répondant aux exigences strictes énoncées par la loi (y compris l'horodatage constant des documents numériques, pour contrer de nouvelles techniques de piratage, et la mise à jour des dernières normes informatiques, pour permettre l'accessibilité future) »[257], mais ce service ne semble pas s'étendre aux actes des particuliers.

À la lumière de ces exemples et des éléments présentés préalablement, nous avons identifié quatre types de technologies qui méritent d'être prises en compte par la Chambre des notaires dans son évaluation des pratiques à favoriser aux fins de l'adoption de règles visant à encadrer la création d'actes notariés technologiques, à savoir : le format PDF/A (2.2.1) ; la signature électronique (2.2.2) ; le greffe électronique (2.2.3) et la chaîne de blocs (2.2.4).

2.2.1 Le PDF/A

En France où, comme nous l'avons déjà souligné, les actes notariés sont dématérialisés depuis 2008[258], il a été établi très tôt que le format utilisé pour enregistrer un acte devait répondre à une série de critères, à savoir :

- Restituer l'image exacte de l'acte (donc assurer son intégrité, c'est-à-dire « que l'acte ne devra être ni détérioré à la suite d'un incident technique ni falsifié à la suite d'une intrusion extérieure ») ;

255. *Ibid.*
256. Michele IASELLI, « Contratti pubblici, stipula elettronica : tutti i nodi irrisolti della normativa », (2016) en ligne : <http://www.forumpa.it/pa-digitale/documenti-contratti-pubblici-stipula-elettronica-tutti-i-nodi-irrisolti-della-normativa>.
257. COMMISSION EUROPÉENNE POUR L'EFFICACITÉ DE LA JUSTICE, préc., note 233, p. 8.
258. B. LEMAIRE, préc., note 196.

- Permettre la transmission de copies de l'acte ;
- Assurer la pérennité de l'acte ;
- Assurer la confidentialité de l'acte (« l'accès aux actes déposés doit être exclusivement réservé à l'office qui les a déposés ») ;
- Être performant (« le délai d'envoi et de réception entre les études et le minutier devra être le plus court possible (moins de 5 minutes) »)[259].

À la lumière de cette série de critères, un format semblait s'imposer, soit le PDF/A[260]. Le PDF/A (pour *Portable Document Format / Archival* – format de document portable pour l'archivage) est un format de document certifié par l'ISO et axé sur la préservation des documents technologiques, c'est-à-dire leur conservation à long terme[261].

Comme l'explique BAnQ :

> Le format PDF/A est défini par la norme ISO 19005. Il s'agit d'un format adapté pour la conservation permanente et la diffusion de documents. Il préserve la mise en page, les polices de caractères et la mise en forme. De plus, il s'agit d'un standard ouvert et libre de droits. La raison d'être du PDF/A est d'assurer la conservation à long terme de documents.[262]

La principale différence entre le PDF/A et le fichier PDF conventionnel réside dans sa structure. En effet, contrairement au fichier PDF communément utilisé, « un fichier PDF/A inclut automatiquement les polices utilisées dans le document »[263]. Ainsi, « le document conserve son aspect visuel même si lu dans 40 ans sur un

259. T. BLANCHET, préc., note 238.
260. B. LEMAIRE, préc., note 196. Notons toutefois que le format XML a également été privilégié dans certaines circonstances.
261. ISO 19005-3 : 2012, en ligne : <http://www.iso.org/>.
262. BIBLIOTHÈQUE ET ARCHIVES NATIONALES DU QUÉBEC, « La numérisation des documents : Méthodes et recommandations », (2012) en ligne : <http://www.banq.qc.ca/documents/ archives/archivistique_ged/publications/Numerisation_des_documents.pdf?language_id=3>, p. 26.
263. CENTRE CANADIEN DE TECHNOLOGIE JUDICIAIRE, « Lignes directrices concernant l'intégrité et la pérennité des dossiers judiciaires », (2013) document inédit.

ordinateur où la police est manquante »[264] puisque le fichier lui-même contient toutes les informations nécessaires à son utilisation[265]. Par ailleurs, le PDF/A a la capacité d'auto-documentation, c'est-à-dire l'incorporation interne des métadonnées relatives au document[266].

Il importe de préciser qu'il existe, à ce jour, trois formats de PDF/A, à savoir le PDF/A-1, le PDF/A-2 et le PDF/A-3. Comme le souligne BAnQ :

> Le format PDF/A-1 comporte deux niveaux de conformité, le PDF/A-1a et le PDF/A-1b. Le niveau 1a préserve la conformité de la structure logique du document. Il représente la forme la plus complète de la norme ISO 19005-1[267] (conformité intégrale). Le niveau 1b se limite à la conformité visuelle du document. Ainsi, pour les documents qu'on veut uniquement numériser en mode image, le niveau 1b est suffisant. Il en va de même pour les documents numérisés en mode image dont une lecture optique (OCR) est réalisée par la suite. Pour la conservation de documents structurés (par exemple, les fichiers produits par les logiciels de bureautique comme Word, Excel, PowerPoint, Open Office, etc.), il est recommandé d'utiliser le PDF/A-1a. Si on utilise les versions les plus récentes de ces logiciels, on peut aussi envisager de les sauvegarder en format XML. À ce sujet, veuillez consulter la section 3.3.3 – XML.[268]

Le format PDF/A-2 est quant à lui régi par la norme ISO 19005-2:2011[269]. Il permet d'utiliser « certaines fonctions des dernières versions du format PDF qui ne sont pas autorisées sous le format PDF/A-1 »[270]. Il permet notamment « l'utilisation du format JPEG 2000, des effets de transparence et des couches d'annotations, l'empaquetage des polices Opentype ainsi que le regroupement de plusieurs documents en format PDF/A dans un seul et

---

264. *Ibid.* Voir également Stacy P. REZENTES, « Law Firm Records Retention », (2016) 20-SEP *Haw. B.J.* 4, 12 : « If you want your system to hold documents for a long time, save them in PDF /A format, an archival standard of PDF ».
265. Adobe, « PDF-A archiving standard », en ligne : <http://www.adobe.com/enterprise/standards/pdfa/>.
266. « Sustainability of Digital Formats: Planning for Library of Congress Collections », en ligne : <http://www.digitalpreservation.gov/formats/fdd/fdd000125.shtml>.
267. Cette norme est disponible en ligne : <https://www.iso.org/fr/standard/38920.html>.
268. BIBLIOTHÈQUE ET ARCHIVES NATIONALES DU QUÉBEC, préc., note 262.
269. Cette norme est disponible en ligne : <https://www.iso.org/fr/standard/50655.html>.
270. BIBLIOTHÈQUE ET ARCHIVES NATIONALES DU QUÉBEC, préc., note 262.

même document (porte-documents) »[271]. Par ailleurs, « [o]utre la préservation de la conformité de l'aspect visuel du document, [le PDF/A-2] offre la possibilité de récupérer le texte en Unicode »[272].

Finalement, le format PDF/A-3 régi par la norme ISO 19005-3:2012[273], « permet [...] l'incorporation de tous les formats de documents, tels que les fichiers Excel, Word, HTML, CAD ou XML »[274].

Comment choisir le bon format de PDF ? Si un désir de suivre les évolutions technologiques imposait le recours à la norme PDF/A-3, laquelle constitue le standard actuel pour la préservation de documents technologiques[275], ce format ne semble pas être la référence *de facto* dans le milieu juridique. Citons ici l'exemple des *Lignes directrices concernant l'intégrité et la pérennité des dossiers judiciaires*[276], ainsi que celui des *National Archives* états-uniennes, lesquelles privilégient respectivement le PDF/A-2 et le PDF/A-1 pour la conservation de dossiers judiciaires[277]. En fait, le choix sera tributaire des fonctionnalités désirées. C'est notamment ce qui explique la proposition du Centre canadien de technologie judiciaire :

> Le niveau de conformité PDF/A-2 est adopté dans les présentes *Lignes directrices* en tant que support logique / format de fichier obligatoire pour permettre les annotations. La norme PDF/A-1 est écartée car elle ne permet pas les annotations. La norme PDF/A-3 est écartée car elle permet l'inclusion de fichiers en format natif dans des porte-documents PDF.[278]

D'ailleurs, il importe de noter que BAnQ permet aux autorités chargées de l'archivage des documents technologiques de sélectionner le type de format PDF/A convenant le mieux à leurs besoins. En effet, l'organisme est d'avis que :

---

271. *Ibid.*
272. *Ibid.*
273. Cette norme est disponible en ligne : <https://www.iso.org/fr/standard/57229.html>.
274. « Aperçu général de PDF/A-3 », en ligne : <http://www.pdf-tools.com/pdf20/fr/savoir-faire/normes-iso-pdf/pdfa-3-apercu/>.
275. Jennifer WONDRACEK, « The E-FAC: One Year Later », (2015) 89-JAN *Fla. B.J.* 18, 22.
276. CENTRE CANADIEN DE TECHNOLOGIE JUDICIAIRE, préc., note 263.
277. « Panel Discussion Judicial Records Forum », (2015) 83 *Fordham L. Rev.* 1735, 1769 (propos de Jason R. BARON, Esq.).
278. CENTRE CANADIEN DE TECHNOLOGIE JUDICIAIRE, préc., note 263.

> [T]ous les documents convertis en PDF/A-1 demeurent acceptables pour la conservation permanente de documents. Il n'y a aucune raison, outre celle de profiter des options supplémentaires qu'offre la version 2, de convertir en PDF/A-2 des documents déjà numérisés en PDF/A-1, pas plus que de créer des documents en PDF/A-2 plutôt qu'en PDF/A-1 si aucun des avantages du PDF/A-2 n'est utilisé.[279]

Le format PDF/A semble donc présenter toutes les caractéristiques requises afin de protéger l'intégrité et la disponibilité des actes notariés dématérialisés. Qui plus est, les métadonnées y associées en permettent l'authentification et en assurent l'irrévocabilité. Selon nous, il s'agit donc d'un format répondant aux exigences des articles 35 et 39 de la *Loi sur le notariat* (sous réserve d'approbation par règlement du Conseil d'administration), d'autant qu'il est déjà utilisé par les notaires d'outre-mer, est approuvé par BAnQ et fait l'objet d'une certification ISO.

Toutefois, si le PDF/A semble présenter toutes les qualités requises pour la conservation des actes, *quid* des documents qui y sont souvent annexés ? En effet, aux termes de l'article 57 de la *Loi sur le notariat*, les documents annexés à un acte doivent être reproduits sur le même support que l'acte auquel ils sont annexés. Rappelons que le support et la technologie sont distincts et qu'il n'est donc pas nécessaire qu'une annexe soit déposée au greffe du notaire dans le même format que l'acte notarié auquel elle est associée. Évidemment, dans plusieurs cas, il sera préférable, pour les raisons énoncées ci-dessous, de transférer les annexes en format PDF/A (dans la mesure où les critères imposés par l'article 17 de la *Loi concernant le cadre juridique des technologies de l'information*[280]

---

279. BIBLIOTHÈQUE ET ARCHIVES NATIONALES DU QUÉBEC, préc., note 262.

280. « **17.** L'information d'un document qui doit être conservé pour constituer une preuve, qu'il s'agisse d'un original ou d'une copie, peut faire l'objet d'un transfert vers un support faisant appel à une technologie différente.
Toutefois, sous réserve de l'article 20, pour que le document source puisse être détruit et remplacé par le document qui résulte du transfert tout en conservant sa valeur juridique, le transfert doit être documenté de sorte qu'il puisse être démontré, au besoin, que le document résultant du transfert comporte la même information que le document source et que son intégrité est assurée.
La documentation comporte au moins 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.
La documentation, y compris celle relative à tout transfert antérieur, est conservée durant tout le cycle de vie du document résultant du transfert. La
(à suivre…)

sont respectés). Notons toutefois que, dans certains cas, il peut s'avérer nécessaire de conserver le format natif d'un document annexé, notamment afin de conserver les fonctionnalités qui lui sont associées (pensons par exemple aux plans ou tableurs). La réglementation adoptée par le Conseil d'administration devrait donc prévoir ce type de scénario en imposant la conservation d'une copie du logiciel permettant la lecture du document annexé.

2.2.2 La signature électronique

Nous l'avons vu, la signature électronique devrait, à notre avis, prendre une forme distincte selon le signataire. En effet, alors que la signature des parties ne vise qu'à valider leur consentement à l'acte, celle du notaire en assure l'authenticité. C'est pourquoi certains auteurs sont d'avis que la signature des parties devrait être « obtenue par une simple numérisation, une signature sur une tablette graphique, un écran tactile, etc., sans devoir être une signature électronique sécuritaire[281], comme celle du notaire »[282]. Cette conception des différents niveaux de signature, comme nous l'avons déjà abordé, est par ailleurs conforme à la pratique du notariat en France et en Italie.

Rappelons que la signature est définie à l'article 2827 C.c.Q. comme étant « l'apposition qu'une personne fait à un acte de son nom ou d'une marque qui lui est personnelle et qu'elle utilise de façon courante, pour manifester son consentement ». L'article 39 de la *Loi concernant le cadre juridique des technologies de l'information* ajoute :

> 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

---

(...suite)
documentation peut être jointe, directement ou par référence, soit au document résultant du transfert, soit à ses éléments structurants ou à son support. »

281. Par « signature électronique sécuritaire », expression favorisée par le législateur fédéral, l'auteur renvoie au concept prédéfini de signature numérique. Voir : *Règlement sur les signatures électroniques sécurisées*, DORS/2005-30.

282. M. LACOURSIÈRE, préc., note 168.

> assurée et qu'au moment de la signature et depuis, le lien entre la signature et le document est maintenu.

C'est donc dire, comme nous l'avons par ailleurs exposé en première partie, que la signature peut prendre diverses formes, le législateur ayant prévu une certaine souplesse dans la définition du concept[283]. Pour les parties à l'acte ou les témoins, la signature manuscrite sur une tablette semble recevoir l'aval des pays européens que nous avons étudiés. Sans remettre en question la validité d'une telle signature, nous sommes toutefois d'avis que d'autres modèles tout aussi valides devraient être envisagés. Nous pensons notamment à la chambre de signatures accessible par nom d'utilisateur et mot de passe, laquelle a l'avantage de reposer sur une solution logicielle et non l'acquisition d'outils informatiques précis.

Si nous reconnaissons la possibilité de recourir à divers mécanismes pour signer, pourquoi alors exiger une signature plus sophistiquée de la part des notaires ? Comme nous l'avons soulevé en première partie, la signature numérique constitue un mécanisme bien plus sécuritaire que son équivalent papier. Il serait donc justifié de prévoir un mécanisme inférieur[284] – similaire à celui utilisé par les parties – d'autant que, pour le papier, le mécanisme utilisé demeure le même.

En fait, nous sommes d'avis que la signature numérique ne remplace pas simplement la signature manuscrite du notaire, elle doit également constituer une solution de rechange viable au sceau. En effet, rappelons que l'article 13 de la *Loi concernant le cadre juridique des technologies de l'information* prévoit :

> Lorsque l'apposition d'un sceau, d'un cachet, d'un tampon, d'un timbre ou d'un autre instrument a pour fonction :
>
> 1° de protéger l'intégrité d'un document ou d'en manifester la fonction d'original, celle-ci peut être remplie à l'égard d'un document technologique, au moyen d'un procédé approprié au support du document ; [...]. »

La signature numérique du notaire et les technologies y associées sauraient, à notre avis, constituer « un procédé approprié au

283. Voir *Lccjti.ca*, préc., note 116.
284. Pour la liste des mécanismes envisageables, voir P. CORMIER, préc., note 109.

support du document »[285]. Par exemple, la trousse de signature numérique Notarius comprend divers outils qui permettent à la signature numérique du notaire de faire office de sceau électronique avec la capacité de pénétrer et marquer un document technologique dont la pérennité est garantie[286].

Comme les notaires québécois ont déjà adopté la signature numérique, cette question ne mérite pas que l'on s'y penche plus en détail. Nous désirons toutefois souligner le fait que la possibilité de signer de façon technologique, combinée aux divers outils de vidéoconférence maintenant disponibles sur le marché, ouvre la porte, comme le prévoit le dernier alinéa de l'article 50 de la *Loi sur le notariat*[287], à la signature des procédures « à distance ». Notons d'emblée que cette approche ne reçoit pas l'aval de certains membres de la profession :

> La présence physique des parties devant le notaire est indispensable afin de permettre au notaire de juger de l'existence et de la qualité du consentement. En effet, l'attitude, le comportement et même les moments de silence et/ou les expressions physiques sont tous, autant d'indices de l'état d'esprit des parties et par delà, de leur adhésion inconditionnelle à l'acte projeté. Une telle vérification est essentielle à la réception de l'acte notarié.[288]

Avec respect, nous sommes d'avis que cet argument repose sur diverses présomptions erronées. D'abord, la *Loi sur le notariat* n'utilise nulle part l'expression « présence physique » ; elle ne traite que de présence. Or, comme l'a souligné la Cour du Québec : « Il est

---

285. Voir Denise BROSSEAU, « Commerce électronique et pratique notariale », (2004) 106 *R. du N.* 557 ; Isabelle DE LAMBERTERIE, « L'établissement et la conservation des actes authentiques électroniques en droit français », (2004) 106 *R. du N.* 379.
286. Voir NOTARIUS, « La signature numérique », en ligne : <http://www.notarius.com/digital-signature/#overview>.
287. « Dans les limites et suivant les conditions prévues par règlement du Conseil d'administration, la signature des parties et des témoins à un acte reçu sur un support autre que le papier peut être apposée hors de la présence du notaire et celui-ci n'est pas alors tenu de signer l'acte au même lieu où la dernière des parties à signer l'a fait ».
288. J.A. TALPIS, préc., note 5, tel que cité dans M. LACOURSIÈRE, préc., note 168. Alain Roy, lequel est toutefois ouvert à l'utilisation des technologies de l'information pour faciliter la signature à distance des actes notariés, soulève une préoccupation similaire : « On sait fort bien que l'incompréhension, l'inquiétude et l'interrogation des parties se perçoivent souvent à partir d'expressions corporelles que seule la vision du notaire permet de détecter ». Voir : A. ROY, préc., note 9, p. 60.

possible d'imaginer différentes façons technologiques d'être présent. Le *Code de procédure civile* ne définit pas ce qu'est l'audience et n'implique pas forcément que les parties soient en présence physique l'une de l'autre »[289].

En appliquant le même raisonnement à la signature d'actes notariés[290], il serait donc envisageable pour le notaire d'être présent grâce à la visioconférence[291], sous réserve de respecter certaines règles :

> Les parties ne devraient pouvoir signer l'acte électronique à distance que si les moyens technologiques en place permettent au notaire de maintenir avec elles un contact non seulement vocal, mais également visuel. On peut imaginer un système fermé de caméras retransmettant en direct dans le bureau du notaire l'image intégrale des parties contractantes. Ce n'est qu'à cette condition que le notaire pourra assurer l'exercice de ses obligations légales.[292]

Ensuite, il a été démontré que les êtres humains sont en fait plutôt mauvais dans l'identification de ce que peut représenter « l'attitude, le comportement et même les moments de silence et/ou les expressions physiques » d'un tiers[293]. Cela étant, comme la visioconférence permet – sous réserve de la qualité de la résolution – de voir son interlocuteur, cette préoccupation perd de son importance.

En fait, le principal problème est plutôt lié au fait que, si le notaire peut voir le signataire par visioconférence, il ne peut pas constater l'acte de signature. En d'autres mots, comment confirmer que le signataire est bien la personne derrière l'écran ?

---

289. *Entreprises Robert Mazeroll ltée* c. *Expertech – Bâtisseur de réseaux Inc.*, préc., note 217, par. 13. Notons qu'il s'agissait ici non pas de la signature d'un acte, mais bien d'un témoignage après défense.
290. C'est notamment ce que souligne Alain Roy : « les moyens technologiques utilisés devront permettre aux parties d'être *virtuellement* présentes devant le notaire, à défaut de l'être en personne ». Voir : A. ROY, préc., note 9, p. 60.
291. M. LACOURSIÈRE, préc., note 168. L'auteur fait écho aux propos tenus par Alain ROY et Bertrand SALVAS, « Réflexions sur l'acte notarié électronique en droit québécois », dans Vincent GAUTRAIS (dir.), *Droit du commerce électronique*, Montréal, Éditions Thémis, 2002, p. 653, 670 et 671 et I. DE LAMBERTERIE, préc., note 168.
292. A. ROY, préc., note 9, p. 60.
293. Robert M. KRAUSS, Yihsiu CHEN et Purnima CHAWLA, « Nonverbal Behavior and Nonverbal Communication: What Do Conversational Hand Gestures Tell Us? », (1996) 28 *Advances in Experimental Social Psychology* 389.

Rappelons que l'objectif de la signature « en présence du notaire » est de s'assurer du consentement des parties quant au contenu de l'acte. La signature vient simplement confirmer ce fait. Selon le modèle français (signature sur une tablette), en supposant que la tablette sur laquelle est signé l'acte est visible via visioconférence, cela aurait, à notre avis, la même valeur qu'une signature manuscrite sur un document papier. Cela implique cependant le recours à deux supports distincts (la tablette utilisée pour signer et l'ordinateur utilisé pour la visioconférence). Sinon, comment confirmer que la partie est bel et bien celle qui a signé l'acte ?

Une approche préférable, à nos yeux, est le recours à un système de visioconférence jumelé à un espace de travail partagé. Le type de technologie utilisée par la plateforme française Tamashare[294] nous semble être un exemple intéressant d'un tel cadre[295]. Cette plateforme offre un service de visioconférence et un espace de travail partagé, le tout protégé par un accès sécurisé (nom d'utilisateur et mot de passe). Ainsi, tout en se voyant l'un et l'autre, la partie et le notaire peuvent « signer » le même document via une signature tapuscrite (il serait même envisageable d'insérer une image d'une signature manuscrite ou une autre forme de signature électronique). Comme l'environnement est sécurisé et que la plateforme identifie chacun des utilisateurs, il devient pratiquement impossible pour un tiers de signer à la place de la partie. Quant au notaire, rappelons que ce dernier n'a pas à signer en présence des parties[296], bien qu'il pourrait techniquement faire de même. Ce mécanisme permet d'ailleurs une triple identification : la première associée au nom d'utilisateur et mot de passe de la partie, la deuxième visuelle et la troisième lors de la signature tapuscrite ou autre du document.

2.2.3 Le greffe technologique

Peu importe le format et les mécanismes d'authentification associés aux actes notariés dématérialisés, la principale préoccupation sécuritaire demeure celle liée à la conservation des actes,

294. Voir en ligne : <http://www.tamashare.com/fr>.
295. Notons que nous ne nous sommes attardés qu'aux fonctionnalités de la plateforme. Ainsi, l'utilisation de celle-ci comme exemple du type de fonctionnalité recherchée ne devrait être interprétée comme un endossement de cette plateforme ou de ses conditions d'utilisation.
296. *Loi sur le notariat*, préc., note 14, art. 50.

c'est-à-dire à la mise sur pied d'un greffe technologique. Rappelons que l'article 62 de la *Loi sur le notariat* – lequel n'est toujours pas en vigueur – prévoit que « [l]es actes reçus en minute par un notaire doivent être versés dans un greffe conservé au Québec ou dans tout lieu qui permet d'assurer la conservation du greffe et qui est déterminé par le Conseil d'administration. Le greffe peut être individuel, commun[297] ou social[298]. »

La conservation du greffe en sol québécois nous semble sage et conforme aux tendances internationales en matière d'hébergement[299]. En effet, un greffe hébergé à l'étranger pourrait soumettre certains actes aux lois de l'État hôte[300], ce qui irait à l'encontre des obligations déontologiques et législatives des notaires.

Quant à la distinction entre le greffe individuel, commun ou social, celle-ci importe peu d'un point de vue sécuritaire. En effet, la relation entre les différents individus ayant accès au greffe n'importe pas autant que le nombre de personnes pouvant consulter un acte. Par exemple, un greffe commun entre deux notaires sera en théorie plus sécuritaire qu'un greffe individuel auquel un notaire donnera un droit d'accès à son adjoint. Ainsi, nous ne saurions nous prononcer sur le modèle le plus efficace entre ceux-ci si ce n'est que de souligner que, plus le nombre d'utilisateurs du greffe sera important, plus le risque d'atteinte à la confidentialité d'un document sera élevé[301]. Parallèlement, toutefois, il sera possible d'investir davantage dans les mesures de sécurité et dans l'entretien nécessaires à son maintien.

---

297. « Le greffe commun est celui constitué par des notaires et qui est détenu par ceux-ci en indivision ». *Ibid.*, art. 63.
298. « Le greffe social est celui constitué par des notaires exerçant leur profession sous la forme d'une société en nom collectif ». *Ibid.*, art. 64.
299. Notons par ailleurs que, comme la *Loi sur la protection des renseignements personnels dans le secteur privé* a été jugée conforme à la LPRDÉ, il serait même envisageable d'héberger lesdits document ailleurs au pays puisque la protection y est équivalente (voir : *Décret d'exclusion visant des organisations de la province de Québec*, DORS/2003-374), d'autant que le pouvoir d'ordonner l'accès à ces documents est contrôlé par la législation fédérale et, donc, uniforme à travers le pays. Voir N. VERMEYS, J.M. GAUTHIER et S. MIZRAHI, préc., note 51.
300. Voir N. VERMEYS, J.M. GAUTHIER et S. MIZRAHI, *ibid.*
301. L'augmentation du nombre d'utilisateurs d'un greffe augmente le nombre de mots de passe, donc les risques que l'un de ceux-ci soit égaré, devinés par un tiers ou identifiés par le biais d'une « attaque par dictionnaire ».

En effet, comme nous l'avons déjà souligné, nous sommes d'avis que la tenue d'un greffe technologique individuel impose des coûts d'acquisition et de maintenance inaccessibles pour une majorité de notaires, ce qui milite en faveur de l'élaboration d'un greffe partagé voire universel pour l'ensemble des membres de la profession. C'est d'ailleurs, il est utile de le rappeler, le scénario qui a été retenu en France :

> L'acte notarié dressé sur support électronique est enregistré pour sa conservation dans un minutier central dès son établissement par le notaire instrumentaire. Ce dernier, ou le notaire qui le détient, en conserve l'accès exclusif.
>
> Le minutier central est établi et contrôlé par le Conseil supérieur du notariat sans préjudice de l'application de l'article 2 du décret nº 79-1037 du 3 décembre 1979 relatif à la compétence des services d'archives publics et à la coopération entre les administrations pour la collecte, la conservation et la communication des archives publiques.[302]

Ce minutier central électronique (le « MICEN ») est constitué d'une série de serveurs situés dans un site sous haute surveillance à Venelles[303]. Il permet la conservation de milliers d'actes notariés dématérialisés pour une période de 75 ans. Après cette période, les actes seront versés aux archives[304]. Comme le souligne un auteur, la conservation dans un minutier central assure l'accessibilité des actes puisque « [l]es évolutions rapides de l'informatique nécessitent la mise à jour permanente des systèmes de lecture, que seule une organisation centralisée peut assumer »[305]. La mise en œuvre de voûtes centrales ou régionales (ou du moins des serveurs centraux contrôlés par une entité habile à assurer la sécurité du système) nous semble donc incontournable. Au risque de nous répéter, nous sommes d'avis que des voûtes électroniques individuelles poseraient un risque trop élevé en ce qui concerne la disponibilité des documents. En effet, même en adoptant des règlements à cet effet et en augmentant le nombre d'inspections professionnelles, il s'avère difficile pour la Chambre de s'assurer que l'ensemble des membres de l'ordre adopte des mesures de sécurité adéquates visant à assurer la protection des documents technologiques conservés. Bien que

---

302. *Décret nº 71-941 du 26 novembre 1971 relatif aux actes établis par les notaires* (version consolidée au 15 janvier 2018).
303. D. FORGER, préc., note 5.
304. *Ibid.*
305. *Ibid.*, 10.

cette même affirmation soit valide pour l'acquisition d'une voûte, une différence importante mérite d'être soulignée. Pour paraphraser une expression souvent utilisée en matière de sécurité, un greffe physique est un bien, alors qu'un greffe technologique est un service. En effet, alors qu'un coffre-fort peut être acheté, installé puis oublié, son équivalent technologique implique le téléchargement de rustines et de mises à jour ponctuelles, l'acquisition de nouveaux logiciels ou outils technologiques lorsqu'une faille est découverte, etc. Bref, il en va, à notre avis, de l'obligation de la Chambre d'assurer la protection du public[306], soit d'augmenter le nombre d'enquêteurs afin de s'assurer que les systèmes des membres de l'Ordre sont conformes aux bonnes pratiques en matière de sécurité informatique (ce qui semble difficilement envisageable), soit d'offrir un greffe centralisé.

Quant aux caractéristiques que devra posséder un tel greffe, l'article 28 du *Décret nº 71-941 du 26 novembre 1971 relatif aux actes établis par les notaires* en France nous semble constituer un point de départ intéressant. Cette disposition prévoit entre autres :

> L'acte établi sur support électronique doit être conservé dans des conditions de nature à en préserver l'intégrité et la lisibilité.
>
> L'ensemble des informations concernant l'acte dès son établissement, telles que les données permettant de l'identifier, de déterminer ses propriétés et d'en assurer la traçabilité, doit être également conservé. [...]
>
> Le procédé de conservation doit permettre l'apposition par le notaire de mentions postérieures à l'établissement de l'acte sans qu'il en résulte une altération des données précédentes.

Soit, cette disposition ne propose aucune technologie précise, mais cela s'avère préférable puisque l'évolution technologique est telle qu'un outil jugé sécuritaire aujourd'hui sera probablement insuffisant demain[307]. Outre le recours au chiffrement des données, mesure notamment privilégiée par le législateur québécois[308], il nous est donc difficile d'aller plus loin dans nos recommandations.

---

306. *Code des professions*, RLRQ, c. C-26, art. 23.
307. Voir par exemple le *Rapport d'enquête sur la sécurité, la collecte et la conservation des renseignements personnels*, 2007 CanLII 41283 (CVPC).
308. Voir l'article 65 de la *Loi concernant le cadre juridique des technologies de l'information*, préc., note 8.

2.2.4 La chaîne de blocs

Bien qu'il nous semble prématuré pour la Chambre de recourir à cette technologie, nous sommes d'avis que la chaîne de blocs (en anglais *blockchain*) constitue une avenue qui mérite d'être explorée et dont la Chambre devrait suivre l'évolution. Associée au développement des cryptomonnaies[309] et devenue notoire grâce à la création du Bitcoin[310], la chaîne de blocs est une « [b]ase de données distribuée et sécurisée, dans laquelle sont stockées chronologiquement, sous forme de blocs liés les uns aux autres, les transactions successives effectuées entre ses utilisateurs depuis sa création »[311].

Comme l'ont soulevé de nombreux auteurs[312], l'utilité de la chaîne de blocs dépasse le simple domaine des cryptomonnaies. En effet, cette technologie est aujourd'hui utilisée dans le domaine des registres fonciers[313] pour assurer l'enregistrement de marques de commerce[314], ainsi que pour la création de contrats intelligents[315].

---

309. « Monnaie virtuelle sans lien avec une politique monétaire ou une banque, dont l'implémentation repose sur des algorithmes de chiffrement ». Voir OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Le grand dictionnaire terminologique*, 2014, « Cryptomonnaie », en ligne : <http://granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=26527257>.
310. Voir : Satoshi NAKAMOTO, « Bitcoin: A Peer-to-Peer Electronic Cash System », (2008) en ligne : <https://bitcoin.org/bitcoin.pdf>.
311. OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Le grand dictionnaire terminologique*, 2017, « Chaîne de blocs », en ligne : <http://granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=26531717>.
312. Voir notamment Michael CROSBY *et al.*, « BlockChain Technology Beyond Bitcoin », (2015) *Sutardja Center for Entrepreneurship & Technology Technical Report* 1. Voir également William MOUGAYAR, *The Business of Blockchain*, Hoboken, Wiley, 2016 ; et Don TAPSCOTT et Alex TAPSCOTT, *Blockchain Revolution*, New York, Penguin Random House, 2016.
313. C'est notamment le cas en Georgie : Laura SHIN, « The First Government To Secure Land Titles on the Bitcoin Blockchain Expands Project », (2017) en ligne : <https://www.forbes.com/sites/laurashin/2017/02/07/the-first-government-to-secure-land-titles-on-the-bitcoin-blockchain-expands-project/#6206c0654dcd> ; à Dubaï : Samburaj DAS, « 100%: Dubai Will Put Entire Land Registry on a Blockchain », (2017) en ligne : <https://www.ccn.com/100-dubai-put-entire-land-registry-blockchain/>, ainsi qu'en Russie : Nikhilesh DE, « Russia's Government to Test Blockchain Land Registry System », (2017) en ligne : <https://www.coindesk.com/russias-government-test-blockchain-land-registry-system/>.
314. C'est notamment ce que propose l'entreprise Cognate. Voir en ligne : <https://cognate.com/>.
315. Voir notamment Mark GATES, *Blockchain*, 2017.

En ce qui concerne la Chambre des notaires et ses membres, Rémy Charras explique :

> Bien souvent, les articles liants Notariat et Blockchain indiquent que la Blockchain, mettant en place un registre de données **permanent, public, inaltérable**, **infalsifiable et accessible à tous, supprimera le notariat** tel qu'il existe actuellement, et que l'authenticité pourra être conférée par la machine.[316]

Cette crainte n'est pas sans fondement. En effet, comme le souligne Anne-Laure Joubaire, en France,

> « [l]a blockchain a beaucoup fait parler les notaires en 2016 suite à un amendement à la loi sur la transparence de la vie publique rédigé par une députée. Le texte prévoyait que « les opérations effectuées au sein d'un système organisé selon un registre décentralisé permanent et infalsifiable de chaîne de blocs de transactions » puissent constituer des « actes authentiques ».[317]

À notre avis, les craintes manifestées à l'égard des chaînes de blocs semblent toutefois prématurées[318]. En effet, une chaîne de blocs « n'est **pas à même de vérifier le consentement des parties ni leur compréhension des termes du contrat** »[319]. Bref, cette technologie ne saurait assurer qu'une parcelle des fonctions associées aux notaires, puisque [traduction] « [l]a présence de l'intermédiaire professionnel (l'agent public, le notaire) pour la saisie des données dans le registre public n'est pas une charge inutile, mais une garantie de la qualité des données, ce qui rend le registre fiable »[320]. C'est donc dire que les chaînes de blocs ne devraient pas être envisagées comme étant des substituts au notariat, mais plutôt comme des outils pouvant être exploités par les notaires dans l'établissement d'une chaîne de titres, la constitution de leurs minutes, etc.

---

316. R. CHARRAS, préc., note 17.
317. Eliott MARKUS, « Les notaires doivent-ils craindre la blockchain ? », (2017) en ligne : <https://www.eliott-markus.com/wilo/les-notaires-doivent-ils-craindre-la-blockchain/>. Voir également R. CHARRAS, *ibid.*
318. Nous partageons en effet l'avis de M. Charras selon lequel la chaîne de blocs est beaucoup plus menaçante pour le notaire de common law que le notaire civiliste. Voir : R. CHARRAS, *ibid.* D'ailleurs, il importe de préciser que législateur français a ultimement reculé quant à l'adoption de la disposition citée ci-dessus.
319. E. MARKUS, préc., note 317.
320. Michele NASTRI, « Blockchain per i notai : opportunità e rischi », (2017) en ligne : <https:// www.agendadigitale.eu/documenti/la-blockchain-per-il-notaio-tecnologico/>.

CONCLUSION

Conclure un article comme celui-ci s'avère problématique puisqu'il s'inscrit dans le cadre d'une réflexion continue sur le futur de la profession de notaire en général et de la numérisation des actes notariés en particulier. Néanmoins, puisque notre objectif était d'identifier les mesures de sécurité à adopter ou, plus justement, les principes sécuritaires à respecter, nous nous permettons de reproduire ici l'article 7 de la *Délibération nº 2014-243 du 12 juin 2014 portant adoption d'une norme simplifiée relative aux traitements automatisés de données à caractère personnel mis en œuvre par les notaires aux fins de signature électronique, de dépôt et de conservation des actes authentiques sur support électronique au sein du Minutier central électronique des notaires de France* (MICEN) (NS-055) :

> Le responsable du traitement prend toutes précautions utiles pour préserver la sécurité des données visées à l'article 3 et, notamment, empêcher qu'elles soient déformées ou endommagées ou que des tiers non autorisés y aient accès.
>
> Un dispositif de traçabilité des accès aux actes contenus au sein du MICEN est mis en œuvre.
>
> Le notaire appose sur l'acte authentique dématérialisé sa signature électronique sécurisée, certifiée conforme aux exigences de l'article 3-I du décret nº 2001-272 sur la signature électronique, par l'utilisation de sa clé de signature personnelle appelée clé Real.
>
> Le certificat de signature de l'acte authentique sur support électronique est présumé fiable au sens du décret nº 2001-272, il est personnel et son usage nécessite la saisie d'un code PIN. Seuls les notaires disposent d'un certificat permettant de signer un acte authentique sur support électronique.
>
> La signature électronique permet de garantir l'identification du notaire signataire de l'acte et l'intégrité de l'acte pendant la phase de dépôt au MICEN.
>
> Les accès individuels à l'application s'effectuent par la clé Real.
>
> Les liaisons entre le traitement de données à caractère personnel correspondant aux finalités exposées à l'article 1er et le MICEN font l'objet d'un chiffrement et utilisent une liaison spécialisée dédiée.
>
> L'acte authentique sur support électronique est inscrit au MICEN selon un procédé qui garantit l'impossibilité pour un utilisateur de le modifier ou de le supprimer après son dépôt.

> Le responsable de traitement s'engage à respecter ces mesures de sécurité afin de répondre à l'exigence de sécurité prévue par l'article 34 de la loi du 6 janvier 1978 modifiée.
>
> La Commission rappelle toutefois que cette obligation nécessite la mise à jour des mesures de sécurité au regard de la réévaluation régulière des risques.

Cette disposition met en exergue le fait que, si dans certains cas il est important de se reporter à une technologie particulière, notamment en matière de de formats, d'autres cas requièrent une approche plus civiliste afin de s'assurer que les mesures utilisées puissent demeurer actuelles. En effet, le notaire étant « gage de sécurité »[321], il a l'obligation de sécuriser ses actes selon les normes et standards actuels et non ceux d'une époque révolue. Pour cette raison, il devra veiller à ce que les technologies accessoires à un acte notarié dématérialisé soient à même d'en assurer la sécurité tout au long de son cycle de vie. Le refus ou l'oubli de procéder de la sorte constitue, à notre avis, un manquement aux devoirs et obligations de l'officier public dans le cadre de sa pratique.

Devant cette obligation de constante réévaluation des mécanismes sécuritaires, il est tentant de maintenir le *statu quo*. Il importe toutefois de résister à cette tentation, sans quoi, le notariat risque de faire partie de cette liste grandissante des professions dépassées par la technologie[322].

Selon Jean Martineau, « les actes notariés étaient la mémoire d'un peuple »[323]. L'évolution de cette mémoire implique intrinsèquement l'évolution de la pratique et des méthodologies utilisées par les notaires pour perpétuer le caractère authentique des actes qu'ils reçoivent. De la plume d'oie à l'acte dématérialisé, l'évolution des technologies, certes, modifiera les images les plus symboliques et quintessentielles associées à la pratique notariale, mais nous offre des possibilités innombrables de mieux soutenir la devise du notariat québécois, *les écrits restent.*

---

321. Serge ALLARD, « La rédaction des contrats : mission et valeur ajoutée / réflexion sur la rédaction des actes », (2008) 2 *C.P. du N.* 31, 36.
322. Sur cette question, voir notamment Richard SUSSKIND, *The End of Lawyers*, Oxford, Oxford University Press, 2010.
323. J. MARTINEAU, préc., note 1.