Centre de la sécurité des télécommunications Canada
Centre canadien pour la cybersécurité
Communications Security Establishment Canada
Canadian Centre for Cyber Security

National Cyber Security Centre
a part of GCHQ

Provenance de contenu public pour les organisations

Utilisation de la provenance de contenu pour améliorer la confiance des visiteurs au sujet de l'information en ligne d'une organisation

Canada

Vue d'ensemble

La présente publication est destinée aux praticiennes et praticiens de la sécurité. Elle sert de base pour expliquer le concept de provenance de contenu public et l'importance des outils offerts aux organisations ainsi que pour établir un historique vérifiable du contenu disponible en ligne. La publication présente de l'information à propos de la variété de technologies pouvant aider à établir la confiance des enregistrements numériques, ainsi que des exemples de leurs utilisations pour répondre à différentes exigences.

Cette publication est le résultat d'une recherche conjointe et a été coécrite par le Centre canadien pour la cybersécurité (Centre pour la cybersécurité) et le National Cyber Security Centre (NCSC) du Royaume-Uni. Le Centre pour la cybersécurité et le NCSC n'approuvent pas directement les produits, les services ou les méthodologies présentés dans la publication. Les normes et les outils décrits ne sont que des démonstrations pour l'amélioration de la cyberrésilience dans différents contextes au moyen d'une combinaison de technologies.

Table of Contents

1 | Inspiration de la confiance pour le contenu numérique : importance de la provenance de contenu

Dans le monde numérique actuel, l'information retrouvée sur Internet n'est pas toujours considérée comme une source fiable. Le nombre grandissant d'informations offertes et le rythme accéléré du contenu généré, en particulier au moyen de l'intelligence artificielle (IA), font en sorte qu'Internet est devenu un véritable champ de bataille pour les cyberactivités d'interférence et de malveillance.

Dans ce contexte, les organisations ont de plus en plus de difficultés à s'assurer de l'authenticité et de l'intégrité de leur information. C'est pourquoi elles doivent repenser comment établir et maintenir la confiance de leurs visiteuses et visiteurs. Comme souligné dans les documents du NCSC Impact of AI on cyber threat from now to 2027 (en anglais seulement) et du Centre pour la cybersécurité Cybermenaces contre le processus démocratique du Canada : Mise à jour de 2025, les capacités de l'IA continuent de profiter aux cybercriminels. Les États-nations commencent à intégrer des technologies alimentées par l'IA à leurs capacités. Les organisations auront de la sorte besoin d'outils pour améliorer leur résilience et leur sécurité afin de protéger l'intégrité de leurs données et de leur information. La pierre angulaire de ces efforts consiste à bien établir la provenance de leur contenu numérique.

La provenance fait référence au lieu d'origine. Dans le monde physique, ce concept implique la vérification de l'authenticité des artefacts. Mais celui-ci est également pertinent dans le monde virtuel. De nombreuses organisations utilisent déjà des systèmes de versionnage et de journalisation pour la provenance des documents internes. Mais ces systèmes peuvent également servir à l'extérieur des organisations. Afin d'inspirer une meilleure confiance auprès de clientèle externe, les organisations doivent ainsi améliorer leur traitement de la provenance publique de leur information.

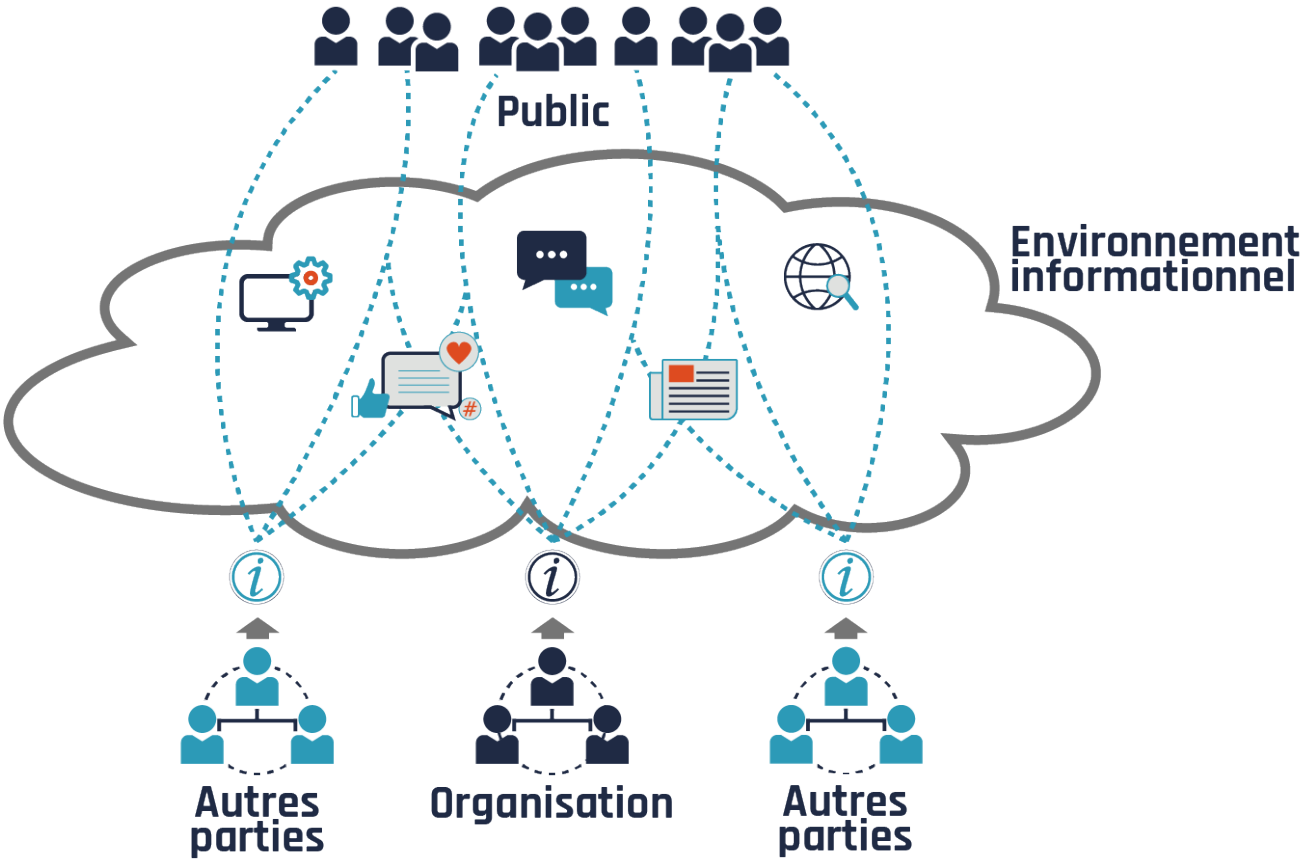
2 | Défi de la confiance numérique dans un environnement informationnel complexe

L'environnement informationnel d'aujourd'hui comporte une variété de formes de communication, allant des médias traditionnels et des médias sociaux jusqu'aux conversations téléphoniques, sans oublier les affiches rencontrées dans la rue. Il est de la sorte facile d'accéder rapidement à une grande quantité d'information chaque jour. Il existe différents processus au sein de cet environnement qui permettent de recueillir et d'organiser les données et les métadonnées dans le but de répondre aux besoins de différents groupes, comme les chercheuses et chercheurs d'information, les diffuseurs et les publicistes. De plus, les plateformes de médias sociaux favorisent une rediffusion à grande échelle, sans oublier l'option d'ajouter des commentaires.

Bien que l'environnement informationnel bénéficie du contenu généré par les créatrices et créateurs et les consommatrices et consommateurs, cela présente également certains défis. Tout au long de son cycle de vie, un élément de contenu original peut être collecté, réorganisé, résumé, agrégé, remis en forme, republié et modifié. Les modifications peuvent être délibérées, mais pas nécessairement. De plus, elles peuvent être réalisées sans l'intention de tromper, mais pas toujours. En outre, les modifications sont parfois difficiles à détecter, car, l'information persiste rarement sous sa forme originale. Cela signifie que nous ne pouvons pas nous assurer que ce qui était visé par le contenu sera conservé. Ou pire encore que l'intention n'a pas été déformée.

Pour les praticiens de la sécurité, la protection de l'information dans ce type d'environnement représente un défi de taille. Traditionnellement, les praticiens devaient se concentrer sur la protection de la confidentialité, de l'intégrité et de la disponibilité des données numériques directement sous la responsabilité de l'organisation. Cependant, maintenant, ils doivent également protéger l'information accessible au public, même si cela est quelque peu hors de leur contrôle. Pour tenter de répondre à ce défi, les organisations peuvent favoriser la confiance du public grâce à des mécanismes de vérification de source et d'historique du contenu.

Figure 1: Communication de l'information de l'organisation dans un environnement informationnel



Description longue – Figure 1 : Communication de l'information de l'organisation dans un environnement informationnel

Pour communiquer avec le public, les organisations partagent de l'information dans leur environnement informationnel. Cet environnement est composé de toutes les formes de communication entre l'organisation et les visiteuses et visiteurs. Cela comprend les médias sociaux, le contenu de sites d'agrégation et de services de recherche Web, les médias traditionnels, comme la radio et la télévision, etc. D'autres parties peuvent contribuer aux communications en ajoutant leur propre contenu sous la forme de commentaires, de filtrage de contenu sélectif et autres ajouts. De la sorte, le message global reçu ou consulté par le public peut ne pas correspondre à ce que la partie initiale souhaitait. Il se peut même que le message soit inexact.

2.1 Provenance de contenu numérique

Le terme de provenance est défini comme étant « le lieu d'origine », ce qui sert de guide pour vérifier l'authenticité et la qualité d'un artefact particulier. Ce terme est traditionnellement utilisé dans le contexte des arts et en histoire. Dans les environnements numériques, ce concept peut être appliqué de différentes façons afin de répondre aux défis particuliers du domaine, comme l'histoire du contenu sur Internet, l'intégrité de la chaîne d'approvisionnement, la gestion des données, la certification logicielle, la gestion des processus scientifiques, le suivi des transactions financières ainsi que la gestion de la chaîne de possession judiciaire. Et chaque application a ses propres exigences.

La présente publication se concentre sur la provenance de contenu public. La provenance de contenu offre de l'information factuelle à propos de l'historique du contenu numérique, sans toutefois faire une évaluation de la valeur ou de la vérité du contenu en tant que tel. Les décisions sur le caractère véridique du contenu sont laissées aux consommateurs, mais de l'information supplémentaire vérifiable est tout de même fournie afin de les aider à effectuer une détermination finale. La provenance de contenu peut présenter différents types d'information vérifiable, y compris, mais sans se limiter à ce qui suit :

- personne ou entité déclarant quelque chose à propos du contenu;
- date et heure de la déclaration;
- image, comparée à la vignette vérifiée;
- déclarations, comme l'emplacement, l'appareil ou les modifications réalisées par un logiciel;
- énoncé concernant le travail qui est une création originale ou générée par l'IA;
- affectation des droits appartenant aux autres personnes (par exemple, licences Creative Commons ou autres licences de droit d'auteur).

En établissant clairement les faits au sujet de l'historique du contenu numérique public, comme l'origine, l'authenticité et la qualité, les organisations peuvent favoriser une meilleure confiance avec leurs visiteuses et visiteurs, leurs clientes et clients et leurs intervenantes et intervenants.

2.2 Analogie pour la provenance de contenu numérique

Une bonne analogie pour expliquer la provenance est le notariat. De nombreux systèmes juridiques exploitent les principes du notariat pour établir des signatures authentifiées dans le cadre des instances judiciaires. Une ou un notaire est une tierce partie de confiance qui exerce un rôle de témoin d'une façon jugée acceptable pour les exigences juridiques.

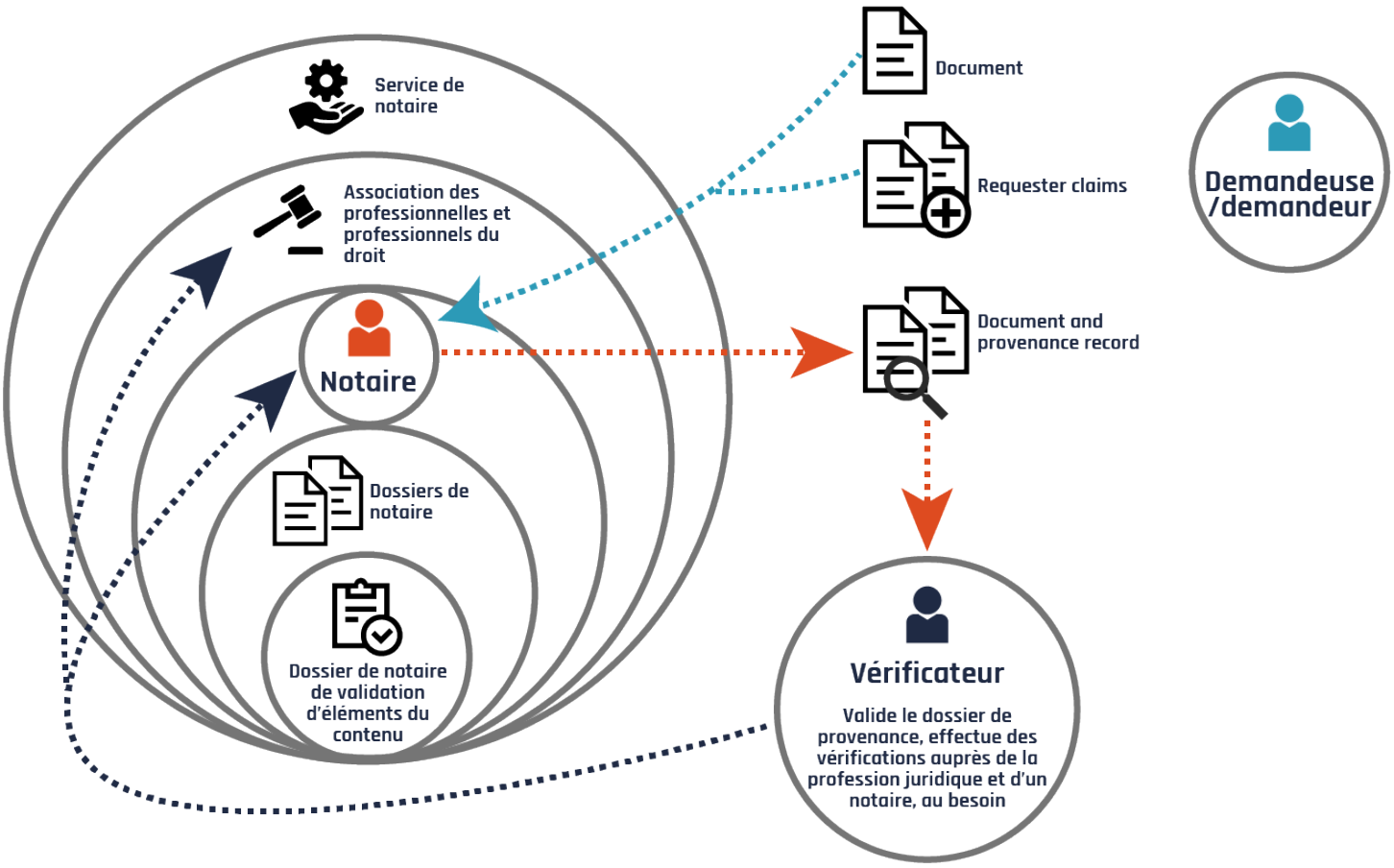
Les membres du public qui ont besoin de documents pour des exigences juridiques ont ainsi recours aux services d'une ou d'un notaire, qui pourra confirmer leur identité et s'assurer que la signature est consentante. La ou le notaire attestera par la suite l'authenticité du document, ainsi que la date et

l'heure de l'attestation. Une telle attestation fait intervenir une déclaration formelle de l'authenticité du document et de la validité des signatures. Un document notarié est légalement reconnu et peut servir de preuve en cour.

De façon similaire, le propriétaire de contenu numérique peut utiliser un service d'attestation pour vérifier les détails du contenu, comme les données de hachage ou une vignette, et établir des preuves vérifiables, comme l'emplacement, le moment et les détails notariés. Cependant, ces activités sont réalisées par des moyens cryptographiques, plutôt qu'en utilisant des documents papier.

En outre, tout comme les notaires qui conservent un registre de tous les documents notariés, les services d'attestation peuvent consigner les transactions d'attestation dans le cadre de leurs services. La fonction de base des notaires est illustrée à la figure 2 ci-dessous.

Figure 2 : Fonction de notaire à titre d'analogie pour la vérification de la provenance



Description longue – Figure 2 : Fonction de notaire à titre d'analogie pour la vérification de la provenance publique

Fonction de notaire à titre d'analogie pour la vérification de la provenance publique. De nombreuses juridictions exploitent le travail des notaires pour agir à titre de valideur de document tiers à des fins juridiques. Le demandeur soumet ses documents au notaire et indique ses déclarations. La ou le notaire valide les documents ainsi que les déclarations et fournit une attestation officielle à la demandeuse ou au demandeur, comme un timbre ou un document. La ou le notaire consigne les

actions réalisées dans un dossier notarié. Le demandeur pourra fournir par la suite le dossier notarié de l'attestation à toute personne souhaitant une vérification. La vérificatrice ou le vérificateur, typiquement la cour, pourra également vérifier auprès du notaire pour vérifier que l'attestation a été réalisée. La vérificatrice ou le vérificateur pourra également consulter une association professionnelle afin de déterminer si la ou le notaire détient un permis d'exercice pour réaliser ses fonctions.

2.3 Comment assurer la confiance du contenu numérique

Pour comprendre pourquoi les organisations doivent tenir compte de la provenance publique, il est utile de considérer le contexte plus vaste de la confiance numérique. Les problèmes de confiance sur Internet ne sont pas nouveaux, et ils font partie intégrante du développement du commerce électronique.

Un objectif important pour les organisations est d'établir la confiance auprès de leurs visiteurs, de leurs clients et de leurs intervenants.

Le rapport 2022 du World Economic Forum décrit les huit dimensions suivantes pour la confiance des technologies numériques. Ces facteurs sont importants pour l'assurance de l'information sur une base plus générale.

- **Cybersécurité :** atténuer les risques des utilisations malveillantes ou accidentelles des technologies
- **Sécurité :** prévenir les préjudices (par exemple, émotionnels, physiques ou psychologiques) envers les personnes ou les membres de la société découlant d'une technologie ou du traitement des données
- **Transparence** : établissement de la visibilité et de la clarté au sujet des utilisations et des opérations numériques
- **Interopérabilité :** s'assurer que les systèmes d'information peuvent se connecter et échanger de l'information pour une utilisation mutuelle, sans charges excessives ou restrictions
- **Vérifiabilité :** s'assurer que les organisations et les tierces parties sont en mesure de vérifier et de confirmer les activités et les résultats des processus technologiques et de gouvernance, des systèmes ou des utilisations de données
- **Redressement :** fournir la possibilité d'un recours aux personnes, aux groupes ou aux entités si celles-ci ont été affectées négativement par des processus technologiques, des systèmes ou des utilisations de données
- **Justice :** s'assurer que les technologies et que le traitement des données d'une organisation tient compte de la possibilité d'un effet disparate et tente d'obtenir des résultats justes et

équitables pour tous les intervenants, compte tenu des circonstances pertinentes et des attentes

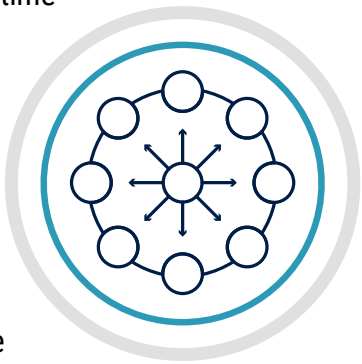
- **Respect de la vie privée :** s'assurer que la plupart des personnes ont le contrôle sur la confidentialité de leur information nominative

La plupart des organisations modernes traitent ces huit dimensions à un certain degré. Toutefois, les exigences de confiance numérique doivent s'adapter au fur et à mesure de l'évolution d'Internet. Ces exigences sont également motivées par des changements comportementaux des personnes sur Internet et des percées de l'IA.

2.4 La provenance de contenu numérique pour améliorer la confiance du public dans une organisation

La provenance de contenu numérique peut aider à traiter et à améliorer la confiance envers une organisation, et ce, en exploitant les huit dimensions ci-dessous. Par exemple :

- **Cybersécurité :** Aide à vérifier que le contenu provient d'une source légitime et sûre, ce qui réduit le risque de contenu malveillant. Favorise également le maintien de registres inaltérable pour la création de contenu et les modifications afin d'empêcher les altérations non autorisées.



- **Sécurité :** Réduit l'impact de l'information inexacte à propos des personnes et des organisations. Un enregistrement de provenance vérifiable peut servir à contredire de l'information inexacte qui se trouve en ligne.
- **Transparence :** Établit des métadonnées vérifiables à propos du contenu en tant que tel. Ces métadonnées permettent d'établir un historique des éléments de contenu, y compris le moment de création et les traitements. La disponibilité au public de ces données permet des processus associés au contenu plus transparents.
- **Vérification :** Établit un enregistrement de contenu numérique et des moyens pour faire des vérifications. Ces moyens peuvent être utilisés par des programmes d'audit.
- **Justice :** Établit un enregistrement formel vérifiable de l'information à propos du contenu. Cela peut comprendre de l'information à propos du créateur, du propriétaire et des droits associés au contenu numérique. L'information vérifiable peut servir pour rendre des décisions lors des contestations à propos des droits et de la validité du contenu.

La provenance de contenu peut fournir au public un moyen de vérifier la précision du contenu créé par une organisation ou à son sujet. Cela permet également d'améliorer la confiance du public envers les organisations.

3 | Provenance : Choix des systèmes et des technologies qui conviennent

Le sujet de la provenance de contenu n'est pas entièrement nouveau, mais les percées technologiques, comme l'IA générative, exercent de la pression pour une évolution plus rapide.

Des cadres qui offrent des moyens pour structurer les systèmes de provenance sont encore en cours de mise au point.

Il existe de nombreuses facettes associées au défi de la provenance de contenu. Ainsi, différentes approches sont nécessaires. Il se peut qu'une approche particulière ne permette pas de résoudre entièrement toutes les exigences de provenance de contenu d'une organisation. Certains exemples de défi de provenance actuels incluent l'étiquetage des médias synthétiques, la provenance de la source numérique des médias, la détection des hypertrucages et la provenance de contenu agrégé.

Les organisations devront de la sorte déterminer un cadre qui sera pertinent à leurs besoins. Les aspects importants à considérer lors de la sélection d'un cadre incluent ce qui suit :

- la confiance des moyens d'établissement de l'enregistrement de provenance – est-ce que des méthodes de chiffrement, comme des horodatages de confiance (section 3.2.1) et des identités cryptographiques (section 3.2.2) permettent de protéger l'intégrité;
- la vérification de la provenance par les membres du public – est-ce qu'il existe des mécanismes simples pouvant être compris du public en général?

Les organisations auront leurs propres exigences pour la provenance de contenu, mais elles doivent être conscientes de l'évolution rapide des exigences et des normes pour les infrastructures de provenance publique. Elles doivent tenir compte des normes utilisées dans leurs propres solutions pour assurer la fonctionnalité de provenance, comme les processus de vérification à grande échelle.

En plus de devoir choisir une solution de provenance permettant de répondre à des objectifs particuliers, une organisation devra sélectionner les technologies à utiliser. Cette décision sera motivée par les objectifs organisationnels ainsi que la disponibilité des solutions technologiques.

3.1 Facteurs à considérer pour choisir un système de provenance

Les systèmes de provenance varient du point de vue de la complexité, des coûts et de l'efficacité. De plus, une organisation devra choisir sa solution en tenant compte de ses propres objectifs. Il est en outre important de savoir que les technologies de provenance numérique sont encore à leur balbutiement et que les exigences organisationnelles évolueront inévitablement. Pour toutes ces raisons, il se peut qu'une organisation choisisse de mettre en œuvre des solutions partielles ou itératives.

La présente section fournit de l'information sur les aspects à considérer lors de la sélection d'une méthode d'établissement de provenance.

3.1.1 Source de confiance

Quelle est la source de confiance pour l'enregistrement de provenance de contenu? Les organisations peuvent utiliser des services internes, mais devront tout de même considérer les façons permettant d'éviter l'impression négative associée à « l'auto-signature » de l'enregistrement de provenance. Ce défi peut être traité grâce à des opératrices et opérateurs ou à des vérificatrices et vérificateurs tiers. Les organisations devront considérer la réputation et la stabilité des organisations tierces servant à l'établissement des enregistrements de provenance.

3.1.2 Durée de vie des enregistrements de provenance

Quelle période temporelle est utilisée pour l'enregistrement de provenance? Au minimum, l'enregistrement doit permettre de retracer le contenu jusqu'à sa date de publication et d'identifier si l'information provient d'un appareil réel ou a été généré par un système alimenté par l'IA. Idéalement, il devrait être possible de retracer la provenance jusqu'au matériel source à l'origine de la création et d'inclure des données de provenance des autres éléments de contenu intégrés, comme les images.

3.1.3 Facilité de la vérification

À quel point est-il simple de vérifier la provenance d'un élément de contenu? Dans la plupart des cas, la vérificatrice ou le vérificateur sera un membre du public en général. Le mécanisme de vérification doit être simple à utiliser et fournir des données compréhensibles et précises au sujet de l'enregistrement de provenance.

3.1.4 Coûts associés aux activités de provenance

Quel est le coût d'un enregistrement de provenance? L'organisation doit être en mesure d'absorber de tels coûts.

3.1.5 Force de la déclaration de provenance

Quelle est la force d'une déclaration de provenance? Est-ce que les faits à propos des déclarations d'identité et de date et heure peuvent résister à un examen? Une validation cryptographique par d'autres parties peut renforcer la déclaration et améliorer la confiance du public concernant l'enregistrement de provenance de contenu.

3.1.6 Durée d'une déclaration de provenance

Quelle est la durée de vie nécessaire d'un enregistrement de provenance? Si l'échelle temporelle correspond à des années ou à des dizaines d'années, alors il sera nécessaire de tenir compte à la fois du stockage du contenu et des mécanismes de vérification.

3.1.7 Utilité de la provenance

Comment le mécanisme de provenance permettra-t-il de réduire les erreurs ou la déformation de l'information d'une organisation? Est-ce que les mécanismes aideront le public à prendre des décisions

à propos du contenu de l'organisation? D'autres mesures de correction de l'information pourront être plus efficaces pour répondre aux défis d'une organisation particulière.

3.1.8 Exigences de correction

À quel point sera-t-il possible de corriger l'information inexacte? Tous les pays ont établi des mécanismes juridiques pour répondre à certaines déclarations d'information inexactes au sujet des organisations (lois sur la diffamation). Ainsi, la plupart des pays disposent de lois pour traiter les problèmes d'infractions des droits d'auteur et de marque de commerce. Celles-ci, ainsi que d'autres lois, peuvent être utilisées par les organisations afin de corriger les données inexactes à leur sujet.

Dans certains cas, comme pour les droits d'auteur, il existe des exigences très structurées pour déterminer le matériel en infraction et aviser les services hôtes d'effectuer une suppression. Il peut s'agir d'un mécanisme d'étiquetage ou de processus automatisés pour les soumissions et les réponses. Les recours juridiques existants et à venir, ainsi que les processus connexes, devront être considérés, ainsi que les coûts et le temps nécessaire pour l'exploitation des mécanismes de correction.

3.1.9 Respect de la vie privée

Est-ce qu'il sera possible de respecter la vie privée des personnes? L'identification des acteurs est un détail de provenance important, mais il ne sera pas toujours possible d'utiliser cette donnée, car cela peut poser certains risques pour la sécurité, la réputation ou d'autres préoccupations pertinentes pour les personnes qui fournissent du contenu. Dans certains cas, les lois peuvent exiger de masquer l'identité d'une personne.

3.2 Facteurs à considérer pour choisir des technologies de provenance

En plus de devoir choisir une solution de provenance permettant de répondre à des objectifs particuliers, une organisation devra sélectionner les technologies à utiliser. Cette décision sera motivée par les objectifs organisationnels ainsi que la disponibilité des solutions technologiques.

Les technologies pertinentes pour une organisation incluent les suivantes :

- des mécanismes d'intégrité cryptographiques, comme une identité au moyen d'une infrastructure à clé publique (ICP), des mécanismes de hachage et des données d'horodatage de confiance, qui pourront servir à rattacher ensemble des parties de contenu pour la solution de provenance afin d'assurer la véracité et l'intégrité des enregistrements de provenance;
- des mécanismes d'authentification pour les appareils, les logiciels et les personnes, ainsi que des ancrages de confiance, qui sont une partie essentielle pour l'établissement de la pertinence d'un enregistrement de provenance;
- un stockage décentralisé, ce qui peut faciliter la tâche;
    - un moyen d'assurer la continuité du contenu et des enregistrements lorsqu'une organisation est démantelée;
    - un mécanisme pour assurer qu'une partie n'ait pas le contrôle total du contenu numérique ou des registres;
- des registres inviolables, qui permettront de traiter le défi de la permanence d'enregistrement de provenance en créant des dossiers impossibles à modifier sans un enregistrement de modification et qui seront indépendants du contenu.

Il sera nécessaire également de considérer les parties qui mettront en œuvre ces diverses technologies afin d'optimiser la confiance engendrée. On peut s'attendre à ce que les organisations qui « auto-signent » leurs propres enregistrements de provenance ne constatent pas de réelle amélioration en matière de confiance pour leur contenu.

3.2.1 Horodatages de confiance

Les horodatages de confiance sont utiles aux mécanismes de provenances, car ils permettent d'établir un horodatage validé pour un état de contenu déterminé. Avec une mise en œuvre adéquate, personne ne devrait être en mesure de modifier un horodatage après sa consignation. Ce concept est d'ailleurs normalisé dans les documents RFC 3161 et American National Standards Institute Accredited Standards Committee X9.95 standard (ANSI ASC X9.95; en anglais seulement).

Ces mécanismes exploitent des méthodes de chiffrement pour calculer la valeur de hachage du document et de l'horodatage. Une organisation tierce réalise généralement l'horodatage afin d'améliorer le mécanisme en question. Des services commerciaux sont disponibles pour ce genre de fonction.

3.2.2 Identité cryptographique

Les identités cryptographiques font partie de l'ICP. Elles sont liées à une clé cryptographique privée connue seulement de l'entité en question. L'identité peut correspondre à une personne, à une organisation, à une entité machine (comme un appareil ou un service) ou encore à une entité anonyme.

Les identités cryptographiques sont souvent ancrées dans les autorités de certification publiques. Elles peuvent jouer un rôle important pour l'établissement de la provenance de contenu, car elles lient des personnes et des appareils à du contenu, y compris des vérifications pertinentes. Cela peut de la sorte renforcer la fiabilité des mécanismes de provenance.

3.2.3 Registres numériques (chaîne de blocs)

La chaîne de blocs est une technologie de registre numérique distribué qui enregistre les transactions d'une manière sécurisée et sans possibilité de violation. Chaque transaction, ou bloc, est associé cryptographiquement au précédent et forme de la sorte une chaîne continue. Cette chaîne de blocs fournit un historique complet et transparent de toutes les transactions. Il est ainsi pratiquement impossible de modifier ou de manipuler le contenu sans être détecté.

Les chaînes de blocs sont souvent mises en œuvre dans un système de fichiers décentralisé, ce qui signifie qu'ils ne sont pas sous la responsabilité d'une personne ou d'une organisation. De plus, elles ne sont pas sujettes à un point de défaillance unique. Les organisations peuvent exploiter les chaînes de blocs ou encore utiliser une mise en œuvre de type privée, en fonction de ses besoins particuliers en matière de provenance.

Le NCSC a publié un guide pour l'utilisation de la technologie de registre distribué (en anglais) afin d'aider à déterminer si un registre distribué est une technologie appropriée, selon différents scénarios.

3.2.4 Archivage Web

L'archivage Web fait référence au processus de collecte et de conservation du contenu numérique du World Wide Web afin que celui-ci reste accessible à l'avenir, même si le contenu a été supprimé d'un site particulier. L'objectif principal de l'archivage Web est de créer un enregistrement permanent du contenu du Web, de saisir les évolutions des sites Web et de tenir compte des changements des renseignements en ligne. Ce processus est très précieux pour la préservation de la provenance de contenu des médias numériques, car il permet de saisir les ressources numériques sous leur forme originale dans leur contexte, d'établir le lien avec la ou le propriétaire et d'examiner les différentes versions du contenu. La Internet Archive Wayback Machine est un exemple général de service d'archivage Web.

L'approche de l'archivage Web peut être étendue à un mécanisme de provenance plus robuste intégrant des signatures cryptographiques et des horodatages. Les données archivées pourront de la sorte servir à vérifier l'authenticité et l'intégrité du contenu numérique et à établir un contexte historique.

3.2.5 Filigrane numérique

Les filigranes numériques ne sont pas un mécanisme de provenance en soi, mais on les mentionne ici, car ils permettent souvent de répondre à certains défis de la confiance numérique. Les filigranes numériques peuvent être ouverts ou encore dissimulés.

- Les **filigranes ouverts** font intervenir un marquage facilement détectable ajouté au contenu, comme des images et des vidéos. Cela correspond souvent à un motif que les utilisateurs peuvent voir. La modification du filigrane mènera à une déformation de l'image ou de la vidéo, qui sera détectable par l'utilisateur final, à moins d'avoir recours à des mécanismes de transformations plus sophistiqués.
- Les **filigranes dissimulés** font également intervenir un marquage, mais celui-ci ne sera pas visible directement dans le contenu. Toutefois, l'image ou la vidéo sera aussi déformée en cas de modification. Cette déformation ne sera pas directement détectable par les utilisateurs, mais les personnes à l'origine de la publication pourront le détecter.

Ainsi, les filigranes ouverts et dissimulés peuvent présenter un moyen pour détecter les tentatives de déformation de contenu numérique. Cependant, il est possible de supprimer de nombreuses formes de filigrane ouvert au moyen des logiciels d'édition moderne. De plus, l'efficacité des filigranes dissimulés est limitée par le petit nombre de parties pouvant détecter les changements. Ces considérations limitent donc l'utilité des filigranes pour répondre aux exigences de confiance du secteur numérique. Toutefois, les filigranes peuvent tout de même ajouter de la valeur dans une mise en œuvre de défense en couches.

3.2.6 La Coalition for Content Provenance and Authenticity

La Coalition for Content Provenance and Authenticity (C2PA) est une organisation du secteur visant à répondre au problème de la prévalence d'information trompeuse au moyen de normes techniques. Il s'agit d'une norme ouverte et bien établie pour documenter et certifier la source et l'historique du contenu des médias.

L'initiative CAI (Content Authenticity Initiative), qui fait intervenir des entreprises importantes du secteur des technologies et des médias, est responsable de faire la promotion de la norme C2PA. La norme C2PA est relativement nouvelle, mais néanmoins importante dans le secteur de la provenance. Elle est toutefois encore en cours de développement.

La norme C2PA exploite des méthodes de chiffrement afin d'établir la provenance de contenu multimédia. Elle repose sur un registre qui est stocké dans le cadre du contenu. Le registre peut saisir de l'information à propos des modifications d'un élément de contenu, y compris l'auteur ou l'éditeur, de l'horodatage et de l'emplacement. De plus, il est lié de manière cryptographique au contenu. Plusieurs registres peuvent être stockés dans un magasin de registres afin de tenir compte de l'historique des modifications apportées au contenu. Le magasin de registres est également connu sous le nom de Content Credential (représenté par l'icône constituée des lettres « C » et « R »). La norme exploite en outre des horodatages de confiance et des filigranes.

3.3 Pourquoi les systèmes de provenance privée ne conviennent-ils pas au contenu public?

La plupart des organisations présentent différents systèmes internes pour le versionnage et la journalisation dans le but de faire le suivi des modifications apportées au contenu. Ces systèmes sont privés dans le sens que les systèmes et les mécanismes d'intégrité, comme les autorités de certification ICP, sont souvent internes à l'organisation.

Une infrastructure de provenance privée fonctionne bien pour certaines exigences d'entreprise et juridiques, mais reste largement impraticable pour des exigences de provenance publique. Une des raisons principales est que le mécanisme est entièrement géré par l'organisation et conçu exclusivement pour une utilisation interne et restreinte. De plus, les systèmes de provenance privée misent en grande partie sur la séparation des responsabilités à titre de mécanisme principal pour l'intégrité des documents.

Les systèmes de provenance privée n'ont pas les fonctionnalités nécessaires de visibilité, de transparence et de pertinence pour faire en sorte que leurs capacités de provenance soient utiles pour établir la confiance pour l'information d'une organisation auprès des visiteuses et visiteurs. Pour répondre aux exigences publiques, les organisations devront reconsidérer les mécanismes de provenance pour au moins une partie de leur contenu.

4 | Déploiement des systèmes de provenance de contenu public : considérations et cas d'utilisation

Les organisations n'ont pas toutes les mêmes exigences d'établissement de la provenance publique de leur contenu. Les exigences peuvent dépendre de différents facteurs. Par exemple :

- défis de confiance pour l'information publique particulière concernée
- stratégie générale pour répondre aux défis de confiance de l'information publique
- public cible
- volume de contenu
- ressources financières

Les exigences particulières peuvent en outre évoluer rapidement compte tenu des changements rapides de l'environnement informationnel, des cyberattaques populaires et de l'utilisation de l'IA.

4.1 Points à considérer par les organisations

Lorsqu'il est question d'un déploiement d'un système de provenance de contenu public, il existe une variété de questions auxquelles les organisations doivent répondre.

4.1.1 Stratégie pour établir la confiance de l'information publique

Les stratégies de confiance d'information publique varieront selon différents facteurs, comme le sujet, les visiteuses et visiteurs et les objectifs que ces derniers rechercheront dans leur utilisation de l'information publique de l'information.

De nombreuses organisations disposent déjà de certaines capacités pour établir la confiance de l'information présentée au public et pour contredire les déclarations qui sont fausses à leur sujet. Utiliser une provenance publique aidera à établir la confiance pour le contenu de l'organisation, mais cela ne sera peut-être pas un moyen aussi efficace et rentable que d'autres stratégies.

Les organisations pourront décider d'utiliser ou non une solution de provenance pour répondre aux différents défis auxquels elles sont confrontées. Celles qui choisiront d'utiliser des technologies de provenance devront également prendre en considération la mise en œuvre qui sera nécessaire.

4.1.2 Introduction de la provenance dans le cycle de vie du contenu

Certaines organisations peuvent avoir une très grande quantité de contenu. Et une partie de ce contenu peut être disponible publiquement. D'autres éléments de contenu, comme les ébauches de document, peuvent ne pas être disponibles publiquement pour l'instant, mais le seront à l'avenir.

Le contenu peut se trouver à différentes étapes de mise à jour et de modification lors de la préparation en vue d'une publication. Il pourra être distribué sur une grande variété de systèmes et également être sujet à des modifications par de nombreuses personnes.

Les organisations peuvent aussi disposer de contenu qui ne sera jamais destiné au public. D'autres contenus peuvent présenter des défis ou des risques pour l'organisation en tant que telle. De la sorte, les organisations pourront choisir des mesures de provenance robustes seulement pour certains types de contenu. Elles pourront également choisir de protéger du contenu au point de publication, plutôt qu'au point de création.

4.1.3 Délai pour la vérification de contenu

Les exigences du public pour les délais de vérification de l'information peuvent varier en fonction du contexte de l'information. Certaines exigences de vérification d'information auront une portée à court terme, comme dans le cas des élections, alors que d'autres s'appliquent plutôt à une échelle générationnelle, comme les preuves concernant les événements historiques distants.

Pour les événements à court terme, le risque organisationnel sera associé au fait que la vérification de la provenance de l'information soit plus longue que ce qui est requis pour la période de l'événement. La période temporelle peut avoir une incidence sur la conservation de l'enregistrement de provenance, ainsi que sur le caractère accessible associé.

4.1.4 Coût

Les mécanismes de provenance numériques sont relativement nouveaux et présentent des coûts pour la mise en œuvre, l'utilisation et la maintenance. Dans la plupart des cas, les organisations devront modifier leurs processus opérationnels pour profiter d'une utilisation efficace des mécanismes de provenance. De plus, les technologies de provenance évoluent rapidement, et une mise en œuvre à très court terme peut rapidement devenir obsolète.

Les organisations pourront choisir d'accorder la priorité aux solutions de confiance non publiques ou encore de choisir une solution intérimaire ou partielle, par exemple en utilisant des mesures de provenance publique seulement pour le contenu critique.

4.1.5 Clientèle et format

La clientèle pour l'information de provenance ne sera pas nécessairement la même que la clientèle de base de l'organisation. Cela dépendra en fait de la réponse stratégique et tactique de l'organisation pour l'utilisation de son information.

Les formats de l'information de provenance seront de plus différents selon le système employé par la clientèle particulière.

Les entreprises des médias disposent de droits d'auteur pour leur information et seront en mesure d'utiliser des outils de droit d'auteur pour retirer le matériel en infraction d'Internet. Dans un tel cas, la clientèle pour les preuves de provenance sera les professionnels des services juridiques, les fournisseurs d'accès Internet et les entreprises des médias sociaux. L'information de provenance devra ainsi être mise en forme pour répondre à différentes exigences de preuve. Une mise en œuvre d'entreprise de média pour ses mécanismes de provenance sera vraisemblablement différente de celle

utilisée pour les organisations dont la clientèle des informations de provenance est le public en général.

4.1.6 Maturité des technologies de provenance publique

Les organisations devront également considérer la maturité des technologies de provenance publique. Les technologies de versionnage et de journalisation qui permettent de répondre aux exigences de provenance interne des organisations sont matures. Les technologies de provenance privée sont moins développées. Toutefois, certaines technologies connexes servant aux applications de provenance privée, comme le hachage et le chiffrement, peuvent servir aux systèmes publics.

Les systèmes de provenance accessibles par le public présentent des exigences supplémentaires. C'est le cas par exemple des appareils terminaux, comme les caméras, qui peuvent cryptographiquement signer du contenu ou encore de l'utilisation de registres inviolables. Ces technologies sont en cours de développement, mais ne sont pas encore matures.

Les organisations peuvent choisir de procéder à des mises en œuvre partielles ou d'essai. Elles peuvent aussi choisir d'établir des architectures qui permettent l'intégration de nouvelles technologies au fur et à mesure qu'elles seront disponibles.

4.2 Exemple de cas d'utilisation

Comme nous l'avons illustré, les exigences pour la provenance publique varieront selon les organisations et les défis qu'elles rencontreront pour la communication des faits à leurs visiteuses et visiteurs, ainsi qu'en fonction des stratégies et des tactiques de confiance pour leur information publique. Ces différentes exigences donneront forme à l'infrastructure de provenance.

Nous fournissons ici cinq cas d'utilisation différents en exploitant les caractéristiques de provenance qui ont été déterminées à la section 3.1 Facteurs à considérer pour choisir un système de provenance.

4.2.1 Cas d'utilisation 1 : Une organisation souhaite un mécanisme de provenance pour tout son contenu public

Une organisation qui souhaite utiliser une solution provenance pour son propre contenu public a deux possibilités :

- établir un enregistrement de provenance irréfutable comprenant une date et une heure de publication;
- créer des enregistrements de provenance pour toutes les étapes intermédiaires de la création du contenu.

L'enregistrement de provenance devient alors un outil pour le personnel des communications de l'organisation, ainsi que pour d'autres personnes qui doivent évaluer et valider les faits à propos du contenu, ou encore réfuter les déclarations qui sont fausses.

Le public doit être en mesure de repérer et de vérifier le contenu facilement. Pour que l'approche soit utile, les mécanismes de vérification doivent être simples, intuitifs et fiables.

4.2.2 Cas d'utilisation 2 : Une organisation souhaite un mécanisme de provenance de contenu seulement à court terme

La durée requise pour un enregistrement de provenance peut varier en fonction de l'utilisation prévue. Comme de nombreuses formes de document numérique, certains enregistrements de provenance pourront être requis seulement pendant une courte période. C'est le cas par exemple du contenu transitoire ayant une pertinence à très court terme, comme l'annonce d'un événement. La provenance de l'annonce peut avoir une grande valeur avant un événement, mais risque de diminuer rapidement par la suite.

L'infrastructure de provenance qui appuie les exigences à court terme n'a pas à tenir compte des facteurs d'exigence longue durée, ce qui simplifie la mise en œuvre et les considérations liées au cycle de vie.

4.2.3 Cas d'utilisation 3 : Une organisation souhaite un mécanisme de provenance de contenu seulement à long terme

Certaines organisations devront fournir leurs enregistrements de provenance pendant une longue période temporelle. Les témoignages de première main des événements importants en sont un exemple. On peut penser aux générations futures qui devront vérifier l'authenticité du contenu numérique actuel. Cela est particulièrement vrai dans un monde où les capacités de l'IA générative augmentent.

Démontrer la véracité des témoignages enregistrés dans un échéancier de plus de 25 ans peut présenter un défi, car les composants de certification pour les identités et les horodatages pourraient ne plus exister. Le mécanisme de provenance doit de la sorte tenir compte des changements technologiques ainsi que du roulement des entités d'affaires, comme les fournisseurs de certificat et les services d'hébergement. Le mécanisme de vérification doit lui-même perdurer.

Le maintien des mécanismes de provenance et de vérification à long terme devra vraisemblablement reposer sur des magasins de contenu distribué et des registres distribués, étant donné que, avec le temps, les organisations pourront fermer, ce qui est une partie normale du cycle de vie des organisations. De tels mécanismes sont pour l'instant à des phases précoces de leur développement et pourront se révéler coûteux, tant du point de vue de la mise en œuvre que de l'utilisation.

4.2.4 Cas d'utilisation 4 : Une organisation doit préserver l'anonymat et le respect de la vie privée de son contenu

Certaines exigences de provenance sont associées à des considérations ayant trait au respect de la vie privée et à l'anonymat. C'est le cas par exemple dans le secteur du journalisme, où les sources peuvent travailler dans des environnements dangereux et souhaitent conserver l'anonymat pour leur protection. L'anonymat pourra être préservé grâce à des identités anonymes de confiance pour les personnes ou encore des dispositifs de saisie de confiance qui peuvent préserver l'anonymat de l'utilisatrice ou de l'utilisateur. Bien que la force d'une déclaration de provenance soit ainsi un peu diminuée, cela ajoute tout de même une certaine valeur.

D'autres moyens de provenance, comme les horodatages de confiance et les certifications de confiance, peuvent élever les niveaux (notamment dans le secteur journalistique), renforcer la valeur des enregistrements de provenance et aider à conserver leur pertinence.

4.2.5 Cas d'utilisation 5 : Correction de droit d'auteur ou autres corrections juridiques

Les enregistrements de provenance de contenu public peuvent potentiellement servir aux organisations pour leurs efforts de correction des infractions des droits d'auteur associées à leur contenu.

Un mécanisme de provenance peut servir à identifier les autorisations de droit d'auteur offertes aux personnes pour l'utilisation de contenu (par exemple, la licence Creative Commons) d'une manière que le public pourra vérifier.

De nombreuses juridictions sont en train de mettre au point des mécanismes pour traiter les autres formes de mauvaise utilisation de l'information.

Les organisations qui mettent en œuvre des mécanismes de provenance à cette fin devront peut-être considérer les exigences de la clientèle spécialisée et de correction juridique dans la conception de leurs systèmes.

5 | Prochaines étapes

L'espace de la provenance de contenu est en rapide évolution en raison des défis émergents, mais il se trouve tout de même encore à un stade de développement. Si vous pensez utiliser un mécanisme de provenance de contenu dans le cadre de votre stratégie de confiance d'entreprise, vous devez tenir compte de ce qui suit :

- comprendre comment votre information et l'information à propos de votre organisation sont reçues par votre clientèle et les autres parties, et comment cela affecte la confiance de vos visiteurs envers votre organisation;
- considérer comment les technologies de provenance de contenu peuvent répondre aux défis de confiance du public de votre organisation;
- rester à l'affût des changements dans les technologies et les menaces de confiance émergentes dans l'environnement informationnel.