fntc

Fédération des
Tiers de Confiance

LA TRAÇABILITÉ AU SERVICE DE LA DÉMATERIALISATION

COLLECTION
LES GUIDES DE LA CONFIANCE
DE LA FNTC

Par le groupe de travail « e-traçabilité »
de la Fédération Nationale des Tiers de Confiance

DANS LA COLLECTION LES GUIDES DE LA CONFIANCE DE LA FNTC :

Guide de la traçabilité (octobre 2013)

Guide de la signature électronique (octobre 2013)

Vade-mecum juridique de la dématérialisation des documents 6ème édition (octobre 2013)

Guide Normes et Labels de la dématérialisation (octobre 2013)

Guide l'interopérabilité des coffres-forts électroniques (mars 2012)

Le bulletin de paie électronique (mars 2012)

Du livret ouvrier au bulletin de paie électronique (mars 2012)

Guide du Document Hybride et de la Certification 2D (nov. 2011)

Fascicule e-paie « le rôle du bulletin de paie dans la reconstitution de carrière » (mars 2011)

Guide du vote électronique, nouvelle édition (mars 2011)

Guide de l'archivage électronique et du coffre-fort électronique (nov. 2010)

Au-delà de la migration Etebac (sept. 2010)

Guide de la Facture électronique (janv. 2010)

Du mandat au mandat électronique (déc. 2009)

PROCHAINE PARUTION

- Guide de la créance numérique

SOMMAIRE

1 LE MOT DU PRÉSIDENT

Depuis l'origine des temps, l'homme a empreint graphiquement la pierre, l'os, l'argile, le bois, le papyrus, le parchemin et le papier, et il a su conserver les signes organisés qu'il a laissés sur ces différents supports.

En maniant habilement son stylo sur un support papier, il devient l'auteur d'un contenu dont l'examen peut permettre de définir une imputabilité, de s'assurer d'une intention, et de déclencher des effets de droit.

A la fin du 20ème siècle, l'essor de l'informatisation a provoqué la substitution de nos supports et de nos interfaces, et l'émergence de la dématérialisation.

Mais la dématérialisation semble provoquer l'évaporation de nos repères tangibles.

Nous avons l'impression fâcheuse qu'elle confère une forte volatilité aux évènements issus de la chaîne de production et de conservation numérique.

Alors, disposons-nous aujourd'hui de marques et de traces pour faire la preuve de notre passage sur les supports « électroniques » ?

Les experts de la Fédération Nationale des Tiers de Confiance ont effectué un précieux travail d'analyse afin de définir la notion de « traçabilité numérique » et son cadre juridique, et de fixer les grandes lignes de l'architecture technique, opérationnelle et organisationnelle qui sous-tend sa mise en œuvre et son exploitation.

Les auteurs de ce guide offrent au public une attrayante contribution à l'accessibilité des arcanes du Numérique, et ils concrétisent à nouveau la volonté de la FNTC de participer activement à la construction d'une dématérialisation intelligible, fiable et sereine.

Alain Bobant
Président de la FNTC

2 INTRODUCTION

Nouvelle révolution industrielle, la dématérialisation a entraîné dans son sillage des modifications fondamentales des activités humaines et des échanges qui en découlent.

Pour donner aux actions effectuées dans le monde immatériel une valeur équivalente à celle que l'on attribue aux documents sous forme papier, et ainsi faire naître la confiance dans l'économie numérique, une démarche technico-juridique était nécessaire. A la sécurité technique permise par les outils informatiques actuels devait correspondre une exigence juridique de traçabilité.

La traçabilité des échanges et des données est au cœur de ce dispositif global de sécurité et de confiance : comme dit l'adage, « Idem est non esse et non probari », ce qui signifie qu'en droit, ce qui ne peut être prouvé n'existe pas (« pas de preuve, pas de droit »).

Dans le monde immatériel, la traçabilité n'est plus une option, elle devient une obligation pour garantir la sécurité des échanges et le respect des droits des personnes physiques comme morales.

Elle est aussi une opportunité, par la quantité d'information qu'elle porte et que l'entreprise peut exploiter.

Ce guide est destiné à toutes les parties prenantes aux processus d'échanges dématérialisés qui ont ou auront besoin de mettre en place la traçabilité pour garantir le bon fonctionnement des services, prévenir les litiges, mieux servir les clients, gagner en transparence…

Que vous soyez Directeur général, chef de projet, juriste, informaticien ou tout simplement un particulier faisant usage de services sur Internet, ce guide s'adresse à vous.

Vous y trouverez, sous forme d'une Foire Aux Questions, une première approche pragmatique du sujet. Dans un deuxième temps, nous tenterons de définir formellement le terme « traçabilité », avant de détailler les bonnes pratiques relatives à sa mise en œuvre. Enfin, quelques exemples permettront d'illustrer le propos général.

3 FAQ

3.1 Pourquoi tracer ?

La traçabilité a pour but de pouvoir reconstituer l'historique des opérations effectuées sur un Système d'Information.
La traçabilité est rendue nécessaire par des considérations de natures diverses :

- juridiques : augmenter les chances de rendre opposables des preuves établies par voie électronique ;
- métier : offrir de nouveaux services ;
- techniques : suivre la qualité de service offerte ;
- marketing : connaître ses clients (par exemple par la méthode de hiérarchisation des traces appelée le « scoring ») ;
- commerciales : mieux vendre ses services ;
- organisationnelles : mettre en œuvre les ressources et les procédures adéquates.

=► *Voir Bonnes pratiques, page 11* / *Bien décrire le contexte.*

3.2 Que tracer ?

Les traces doivent contenir les informations significatives permettant de reconstituer a posteriori l'historique des opérations effectuées dans le cadre du ou des processus sur lesquels porte la traçabilité : qui, quoi, quand.

=► *Voir Bonnes pratiques, page 13* / Identifier les données à tracer.

3.3 Qui a accès aux traces ?

Le contrôle d'accès aux traces doit être strict et modulé en fonction de leur contenu, de leur finalité et de la réglementation applicable. Les traces doivent être accessibles sur demande par les autorités judiciaires et antiterroristes, et les autorités de tutelle, telles que par exemple l'Autorité de Contrôle Prudentiel ou l'Autorité de Régulation des Jeux en Ligne.

=► *Voir Bonnes pratiques, page 20* / Définir les accès aux traces.

3.4 Quelles formes prennent les traces ?

Selon les utilisateurs à qui elles s'adressent, les traces prendront des formes différentes : les « logs applicatifs » extrêmement techniques destinés aux administrateurs système seront ainsi très différents des traces fonctionnelles utilisées par le support clients ou des traces certifiées à produire en justice.

=► *Voir Bonnes pratiques, page 19* / Identifier les formes de traçabilité à appliquer.

3.5 Les traces ont-elles une valeur juridique ?

Oui, elles peuvent en avoir une.
Des traces fiables peuvent permettre d'étayer la preuve d'un fait dans un contexte de dématérialisation, pour constater un accès à partir de traces de connexion, la date d'une action, etc. Il est possible de renforcer la valeur probante des traces par exemple via le constat d'un Huissier de justice, dont la pratique est adaptée à ce type d'opération, d'un agent de l'APP (Agence pour la Protection des Programmes), ou d'un autre organisme assermenté.
Pour des traces liées à un contrat sous forme électronique, l'établissement d'une Convention de preuve comprenant les conditions d'acceptation desdites traces et/ou une Politique de traçabilité permet de s'assurer de la fiabilité des traces et d'en apporter au mieux la preuve devant les tribunaux.

=► *Voir Bonnes pratiques, page 15* / Définir le cadre juridique de la traçabilité.

3.6 Quel est le statut des accusés de réception ?

Dans certains cas, il existe un cadre juridique renvoyant à la notion d'accusé de réception, par exemple pour la lettre recommandée électronique (article 1369-8 du Code civil) ou pour la remise d'un écrit électronique (article 1369-9 du Code civil).
L'article 1369-9 al. 1du code civil énonce :
« Hors les cas prévus aux articles 1369-1 et 1369-2, la remise d'un écrit sous forme électronique est effective lorsque le destinataire, après avoir pu en prendre connaissance, en a accusé réception. »
Toutefois, l'accusé de réception n'est pas expressément défini.
Dans le cas général, les accusés de réception émis par les systèmes informatiques à destination des utilisateurs ont un statut intermédiaire entre données métier et données de traçabilité.

En effet, il s'agit en général d'un résumé des informations métier constitutives d'une transaction, correspondant à une étape à part entière de la transaction, et à ce titre les accusés de réception peuvent être considérés comme des données métier.

Toutefois, leur finalité est de permettre à leur destinataire de disposer d'un élément de preuve sur la transaction effectuée, et à ce titre, les accusés de réception ont une fonction de traçabilité, surtout dans la mesure où ils sont souvent le seul élément de preuve auquel l'utilisateur a accès.

La FNTC préconise d'inclure dans les systèmes d'information la génération d'accusés de réception ou de traces mises à disposition des utilisateurs de manière à garantir un équilibre des informations à vocation probatoire disponibles pour chacune des parties.

La transparence ainsi offerte renforce la confiance et est de nature à réduire le risque de contentieux lié à l'usage des systèmes d'information.

3.7 Peut-on utiliser le numéro de sécurité sociale dans les traces ?

Non, selon l'article 226-16-1 du code pénal, sauf autorisation spécifique.

3.8 Peut-on enregistrer des données à caractère personnel dans les traces ?

Oui, mais en respectant les exigences légales de déclaration ou d'autorisation du traitement, et en adaptant la durée de conservation à l'objet du traitement : par exemple, on conservera les données de traces relatives à des transactions commerciales jusqu'à expiration du délai de recours contentieux.

3.9 Les traces sont-elles concernées par le « droit à l'oubli ? »

Le « droit à l'oubli » consiste à pouvoir, à titre personnel, faire disparaître des informations nous concernant. Il ne s'agit pas d'un vrai droit mais d'une revendication sur la base de la loi Informatique et Libertés :
• l'article 6 (la durée de conservation doit être la durée nécessaire) ;
• l'article 38 (droit d'opposition pour motif légitime) ;
• l'article 40 (droit de rectification et nécessité d'effacement des données obsolètes).

Il ne s'agit pas à proprement parler du domaine de la traçabilité mais plutôt des données à caractère personnel.

3.10 Peut-on et doit-on faire disparaître des traces ?

Oui ! Si les traces contiennent des données personnelles, il est impératif de définir la durée de conservation des traces et de les supprimer à l'issue de cette période.

En revanche, il n'est pas recommandable de faire disparaître des traces dans le but de masquer volontairement un événement !

Il est important de conserver les traces tant qu'une action en justice peut être diligentée. (Un développement sur les durées correspondantes peut être trouvé dans le guide de l'archivage électronique et du coffre-fort électronique édité par la FNTC.)

=► *Voir Bonnes pratiques, page 21* / Prévoir la fin de vie des traces.

4 DÉFINITION DE LA TRAÇABILITÉ

Au sens général, la traçabilité est : « l'aptitude à retrouver l'historique, l'utilisation ou la localisation d'une entité au moyen d'identifications enregistrées » (selon la norme ISO 8402 : Management et assurance de la qualité).

Appliquée aux Systèmes d'Information et/ou aux échanges numériques, la e-traçabilité d'un système peut être définie comme ***l'aptitude à reconstituer a posteriori un historique fidèle des événements qui se sont déroulés au sein du système.***

Le système doit être compris au sens large : il peut intégrer plusieurs entités informatiques différentes, distantes ou non, communicantes ou non.

Les événements tracés peuvent être de natures très diverses : une action humaine (clic d'un utilisateur sur un bouton, téléchargement d'un document, authentification…) ou une action automatique (génération d'un document, dépôt ou transfert d'un document dans un coffre-fort, accusé de réception, envoi d'un mail, vérification d'un solde bancaire, déclenchement d'un traitement sur alarme ou à une date donnée…).

La fidélité des traces dépend du respect des règles ci-dessous :

- la traçabilité doit être volontaire et organisée ;
- le contenu informationnel de la trace doit correspondre de façon automatique et certaine à l'événement tracé ;
- une trace doit être identifiable ;
- une trace doit être interprétable ;
- une trace doit être intègre (non modifiable) ;
- une trace doit être datée ;
- l'accès aux traces doit être contrôlé.

Traçabilité et données métier

Un système d'information est toujours conçu dans un but métier particulier : par exemple, gérer les comptes bancaires des clients, permettre des échanges sécurisés de pièces de marchés publics, gérer les remboursements de la Sécurité Sociale, publier du contenu, piloter une machine-outil, etc.
A ce titre, le système d'information gère une grande quantité de données métier, qui peuvent contribuer au concept général de traçabilité.
La différence entre les données métier et les données de traçabilité est la **finalité** que le concepteur du système leur a assignée :

- ces données sont-elles destinées à rendre un service (par exemple le nouveau solde du compte en banque suite à un virement) : on a alors affaire à des données métier ;
- ou à pouvoir reconstituer a posteriori les actions qui se sont déroulées (par exemple la trace d'une demande de virement effectuée par le titulaire du compte) : on a alors affaire à des données de traçabilité.

Certaines données peuvent être à la fois des données métier et des données de traçabilité, selon **l'usage** qui en est fait. Par exemple, comme nous l'avons vu dans la FAQ, l'accusé de réception d'une lettre recommandée électronique est le cœur de métier de l'opérateur qui achemine le courrier, mais également une donnée de traçabilité sur le traitement du courrier.

Exclusions du guide de la confiance

Le présent guide de la confiance ne traite pas des sujets de la traçabilité alimentaire, médicale, industrielle ou commerciale, mais uniquement de la e-traçabilité telle que définie ci-dessus.

Par ailleurs, sur Internet, les utilisateurs laissent fréquemment des traces (réseaux sociaux, courrier électronique, etc.), non destinées à un usage de traçabilité mais potentiellement employées par des tiers à des fins de reconstitution d'événements, voire d'exploitation métier (data mining). Ces données, qui constituent une problématique sociétale majeure, n'entrent néanmoins pas dans le cadre du présent guide de la confiance, car il ne s'agit pas d'une traçabilité organisée telle que définie ci-dessus. Toutefois, cette traçabilité d'événements (non organisée) peut être établie de manière fiable en recourant à des constats d'huissier de justice respectant la norme AFNOR NF Z67-147 « Mode opératoire de procès verbal de constat sur internet effectué par un huissier de justice ».

5 BONNES PRATIQUES : BIEN TRACER, C'EST QUOI ?

La traçabilité se gère comme un projet à part entière, de manière transverse. Nous allons détailler dans le présent chapitre les principaux points d'attention à ne pas manquer pour le succès du projet, en illustrant notre propos par l'exemple de l'acceptation de Conditions Générales d'Utilisation (CGU) sur un site Internet.

5.1 Bien décrire le contexte

La traçabilité a pour but de pouvoir reconstituer l'historique des opérations effectuées sur un Système d'Information. Elle est rendue nécessaire par des considérations de natures diverses. Il est important de décrire le contexte dans laquelle la trace est générée.

Le contexte juridique : dans de nombreux domaines, des obligations s'imposent sur les éléments à tracer et le temps de conservation des traces ***(voir le chapitre 6 « la traçabilité par l'exemple » pour plus d'information)***.
Les traces sont des éléments de preuve qui peuvent être utilisés en cas de contentieux judiciaire ou amiable.
Lorsque ces traces sont liées à un processus de contractualisation, une convention de preuve permet de fixer à l'avance les règles qui seront prises en compte en cas de contentieux, conformément à l'art. 1316-2 du Code civil (qui dispose « Lorsque la loi n'a pas fixé d'autres principes, et à défaut de convention valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous moyens le titre le plus vraisemblable, quel qu'en soit le support. »).
La convention de preuve sera liée à la Politique de traçabilité ***dont il est fait état au chapitre 5.9.***

Le contexte métier : les traces permettent de réaliser un suivi effectif des opérations réalisées sur la plate-forme par les différents utilisateurs, de rejouer ou de vérifier des séquences d'actions (humaines ou automatiques), de constituer une base de connaissances pour le support clients… Un descriptif des procédures métier concernées et de leur importance sur l'organisation globale permettra de justifier de la pertinence des traces.

Le contexte technique : les traces permettent d'identifier et de résoudre les problèmes rencontrés, de mesurer les performances… Les traces techniques sont habituellement utilisées par les développeurs ou les superviseurs du système.

Le contexte commercial : les traces permettent de suivre les relations commerciales, d'identifier la fraude, d'établir la confiance. La Politique de Traçabilité peut indiquer les contrats auxquels elle se réfère.

Le contexte organisationnel : les traces permettent de vérifier la conformité des procédures (réglementaire, qualité, sécurité) et de réaliser des audits.

> ***L'étape préalable au projet de traçabilité est l'analyse de l'ensemble de ces dimensions par les acteurs du projet et la synthèse de ces données. Cette étude permet de faire une première sélection des données à tracer pour chacun des contextes.***

Application à l'exemple de la validation des CGU

Contexte métier : Un utilisateur a créé son compte client, action qui doit elle-même être tracée. L'utilisateur ne doit pas pouvoir utiliser le site avant d'avoir validé les Conditions Générales d'Utilisation (CGU). En fonction du type de compte, les CGU à valider ne seront pas les mêmes. Par exemple, si un service met en relation des vendeurs et des acheteurs, les CGU correspondant au profil « acheteur » peuvent être différentes des CGU du profil « vendeur ». La trace doit donc contenir des informations précises sur les CGU qui ont été présentées à l'utilisateur.

Contexte juridique : La validation des CGU répond à des impératifs imposés par le droit de la consommation : les CGU doivent être présentées dans une fenêtre de type pop-up, à un format imprimable, etc. Il est impératif de recueillir le consentement de l'utilisateur aux CGU et de pouvoir le prouver. La trace est donc indispensable et il faudra valider une nouvelle fois les CGU à chaque évolution de celles-ci.
On notera notamment qu'un arrêt de la Cour de cassation du 31 octobre 2012 considère au sujet de l'opposabilité des CGU que : « la simple mise en ligne de ces dernières, accessibles par un onglet à demi dissimulé en partie inférieure de l'écran, ne suffit pas à mettre à la charge des utilisateurs des services proposés une obligation de nature contractuelle ». Les hauts magistrats estiment que *« l'accès à la page d'accueil des sites M6 replay et W9 replay, aux menus et aux programmes à revoir était libre et direct et ne supposait ni prise de connaissance ni acceptation préalable des conditions générales d'utilisation »*. **Dès lors, et en l'absence d'une acceptation non équivoque (case à cocher par exemple), il devient difficile à un commerçant de se prévaloir des conditions inscrites dans un contrat qu'il n'a pas fait lire à un utilisateur. La traçabilité prend toute sa signification pour ce type d'opération.**

Contexte commercial : Le nombre de validations de CGU sera employé comme indicateur du nombre de nouveaux clients. La trace doit permettre d'identifier les utilisateurs uniques, même en cas de nouvelle validation de CGU par le même utilisateur suite à une évolution.

Contexte organisationnel : Le support téléphonique ne doit pas répondre aux questions d'un utilisateur sans avoir vérifié préalablement qu'il avait validé les CGU. La trace de validation des CGU doit pouvoir être visualisée sur l'écran du support.

5.2 Organiser les données à tracer

L'analyse du contexte ayant permis d'identifier les données pertinentes pour la traçabilité, il convient maintenant de les trier et de les organiser.

Les traces doivent contenir les informations significatives permettant de reconstituer a posteriori l'historique des opérations effectuées dans le cadre du ou des processus sur lesquels porte la traçabilité.

Le triptyque constitutif de toute trace est :

- qui ?
- quoi ?
- quand ?

L'élaboration d'un système de traçabilité oblige à identifier trois natures de données :

- celles que l'on **doit** tracer (il existe une obligation) ;
- celles que l'on **peut** tracer (utiles pour les processus et dont la conservation n'est pas interdite, et possibles à générer) ;
- celles que l'on **ne doit pas** tracer (sauf autorisation ou déclaration) : on sera en particulier attentif aux données à caractère personnel.

Application à l'exemple de la validation des CGU

La traçabilité de l'acte de validation des CGU de l'utilisateur inclura par exemple les données suivantes :

- QUI ?
  > son identité (par exemple représentée par son identifiant unique, ou son adresse e-mail, l'adresse IP à partir de laquelle il était connecté) ;
- QUOI ?
  > l'action qu'il a réalisée (validation des CGU, cliquer sur « j'ai lu et j'accepte ») ;
  > la version des CGU sur laquelle a porté la validation (type de CGU, numéro de version, date de mise en ligne, empreinte électronique du document…) ;
- QUAND ?
  > la date et l'heure de la validation.

Aspect de fiabilité des identités

En général, les systèmes d'information ne gèrent pas correctement les orthographes de noms complexes : accents, apostrophes. C'est ainsi qu'il arrive que des usagers bénéficient de deux identités numériques, même dans les systèmes d'information officiels de l'État. Les identités multiples par erreur de traitement peuvent donc contrecarrer les effets de la traçabilité.

La gestion des homonymes pose le même problème d'usurpation involontaire d'identité qui peut priver de droits un usager par erreur de traitement logiciel.

La mise en place d'un système d'e-traçabilité doit permettre une interopérabilité entre systèmes d'information différents, et valider l'association de la trace au bon individu. Le référentiel de traitement des identités doit permettre de dédoublonner les informations liées à un individu unique, mais aussi d'éviter la confusion d'identité entre deux individus.

L'absence de ces deux points amène à un double risque :
- la contestation légitime d'usagers lésés ;
- la contestation de coupables de par l'incapacité à lier les traces à leur auteur réel de manière indubitable.

Aspects de confidentialité

Parmi les informations à tracer, certaines peuvent revêtir un caractère de confidentialité tel que leur nature même peut entrer en contradiction avec l'obligation de les tracer. C'est le cas, en particulier, de certaines données à caractère personnel, mais aussi de données touchant à la stratégie d'une entreprise.

Afin de répondre aux besoins de traçabilité sur de telles informations tout en préservant leur caractère confidentiel, il est nécessaire de procéder à leur anonymisation.

L'anonymisation consiste à rompre le lien entre l'identité d'une personne et la donnée qui la représente. On peut par exemple employer des identifiants non nominatifs, rendant impossible la reconstitution d'un tel lien.
Exemple : la traçabilité des dossiers médicaux peut être employée à des fins de statistiques et de recherche à condition que les données soient anonymisées.

On apportera une attention toute particulière à la façon de fabriquer les identifiants uniques. En l'occurrence, il ne doit pas pouvoir être possible de reconstituer l'information ainsi protégée à partir de cet identifiant. Le numéro de sécurité sociale (N.I.R.) est une illustration de ce principe.

L'utilisation conjointe de date et heure, de numéros de séquence et/ou d'empreintes (issues de calculs d'empreinte effectués sur les données confidentielles elles-mêmes) sont de bonnes méthodes pour générer de tels identifiants.

Aspects techniques

La conservation de toutes les traces relatives aux processus peut constituer un volume très important, pénalisant à la fois en termes de coût de stockage et de capacité de recherche effective.

La FNTC préconise de limiter la traçabilité aux seules informations réellement utiles.

5.3 Définir le cadre juridique de la traçabilité

5.3.1 Identifier le régime juridique applicable

Certains domaines techniques (banque, fournisseurs d'accès à Internet, hébergeurs, opérateurs de jeux en ligne…) sont soumis à des régimes juridiques ou des normes sectorielles particuliers qui leur imposent le respect de règles spécifiques en matière de traçabilité. ***Des exemples en sont donnés dans le chapitre « la traçabilité par l'exemple » page 24.***
En dehors de ces cas particuliers, les règles générales détaillées ci-dessous ont vocation à s'appliquer quel que soit le secteur économique.

5.3.2 Protection des données personnelles

En règle générale, la conservation de traces est soumise au respect des prescriptions de la loi « Informatique et libertés » du 6 janvier 1978 modifiée, si les traces peuvent être qualifiées de données à caractère personnel, autrement dit si elles contiennent des informations relatives à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.

Dans cette hypothèse, les traitements doivent faire l'objet de formalités préalables (dispense de déclaration, déclaration ou autorisation selon le caractère des données, les traitements réalisés et l'identité du responsable du traitement). En outre, leurs finalités doivent être déterminées et les personnes concernées doivent être informées de ces traitements.

Enfin, des durées de conservation des traces doivent être fixées et respectées. L'article 6.5 de la loi du 6 janvier 1978 modifiée, dispose que ces données « sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées ».

5.3.3 Valeur juridique des traces

En l'absence d'obligation légale ou d'exigence contractuelle, les traces constituent un faisceau d'éléments de preuve qui pourront être pris en compte lors d'un contentieux.

Dans le cas où il existe une obligation légale de conservation des traces (par exemple : fournisseurs d'accès, hébergeurs, jeu en ligne), la valeur juridique de ces traces découle naturellement de l'obligation de conservation mise en œuvre selon l'état de l'art ou selon la réglementation.

Lorsqu'elles sont relatives à un procédé de contractualisation électronique, la valeur des traces sera renforcée par l'existence d'une convention de preuve du fait de l'article 1316-2 du Code civil.

La fiabilité et la recevabilité des traces dépendent des conditions de leur génération et de leur conservation, de leur documentation (interprétabilité), et de la finalité de leur utilisation.
Le juge reste dans tous les cas souverain dans son appréciation.

On confèrera une valeur supérieure aux traces dès lors qu'elles sont couvertes par une convention de preuve (chaque partie acceptant en principe leur production), lorsqu'on les conserve dans un Coffre-fort électronique et/ou en faisant appel à un Tiers de confiance pour les certifier (horodatage, cachet serveur), pour garantir l'identification de l'émetteur ou pour les conserver (archivage à vocation probatoire).

L'identification de la personne dont émane la preuve par écrit comporte dans la traçabilité deux aspects :

- pouvoir prouver que la trace provient bien du système de traçabilité mis en œuvre (l'auteur de l'écrit) ;
- pouvoir prouver l'identité et l'authenticité des acteurs à l'origine de l'événement objet de la trace.

La FNTC préconise la mise à disposition des traces pertinentes pour les utilisateurs de manière à garantir la disponibilité de traces à vocation probatoire. La transparence ainsi offerte renforce la confiance et est de nature à réduire le risque de contentieux lié à l'usage des systèmes d'information.

La FNTC préconise également, dans les cas où la loi ne fixe pas de principe prédominant, l'établissement d'une convention de preuve entre les parties garantissant la nature, le contenu et l'interprétation à faire des traces établies.

5.3.4 La recevabilité des preuves provenant de la traçabilité

Il est parfois difficile de prouver l'équivalence de la force probante de l'écrit sous forme électronique et sous forme papier, telle qu'énoncée à l'article 1316-1 du Code civil. Dans ces conditions, l'appréciation du juge est souveraine. Il est donc d'autant plus important de pouvoir fournir des éléments de traçabilité convaincants : la jurisprudence offre des exemples d'écrits électroniques acceptés car démontrant une traçabilité satisfaisante.

En cas de contestation du document immatériel par la partie adverse dans le cadre d'un litige, il incombe à la partie se prévalant de ce document de fournir au juge la preuve de sa force probante. Dans ce contexte, un procédé fiable de traçabilité du document permettra de garantir l'identification de l'auteur et l'intégrité du document en cause.

Deux jurisprudences de la Cour de cassation permettent d'illustrer ce propos.

Jurisprudence 1

Dans le cadre d'un litige contre la CPAM, une copie informatique d'un courrier envoyé par papier a été considérée comme fiable, car *« faisant apparaître clairement l'auteur de ce document »*, émanant d'un système à la *« fiabilité technique nécessairement auditée par les autorités de tutelle »*, dont l'examen pouvait être corroboré par l'existence d'un accusé de réception de lettre recommandée portant les même références que celles du document informatique, et après présentation de la trace des opérations de gestion effectuées par la CPAM dans le cadre de l'instruction du dossier (Cour de cassation, 2ème civ. 17 mars 2011, n°10-14.850). Cf Vade-mecum juridique de la dématérialisation des documents, p. 14, 6ème éd. 2013).

► L'existence de la traçabilité, couplée à la fiabilité de sa mise en œuvre, a ici permis de régler le litige au bénéfice du gestionnaire des données. Une véritable Politique de traçabilité permet de réduire l'aléa afférent à la recevabilité de preuves issues de systèmes informatiques.

Jurisprudence 2

Dans le cadre d'un litige portant sur la résiliation d'un bail d'habitation, le juge a considéré que de simples mails, contestés par l'une des parties, ne pouvaient se voir conférer un caractère probant, sans avoir vérifié préalablement le respect de l'article 1316-1 [garantie de provenance et d'intégrité] et 1316-4 [signature électronique] du Code civil (Cour de cassation, civ. 1ère, 30 septembre 2010, n°09-68.555).

► La preuve de la fiabilité de l'échange incombe à celui qui s'en prévaut. La traçabilité permet de créer les conditions de recevabilité des preuves en justice.

Tous les domaines du droit sont concernés par les problématiques de traçabilité de documents immatériels. La mise en place d'une Politique de Traçabilité permet en principe d'accroître la fiabilité technique et par là la recevabilité juridique des éléments présentés au juge en cas de litige, et/ou de régler le litige en amont par la voie d'une transaction.

5.3.5 S'appuyer sur des Tiers de Confiance

Un Tiers de Confiance est un prestataire indépendant des parties à un potentiel litige, mettant en œuvre des mécanismes techniques, méthodologiques et organisationnels de nature à renforcer la valeur probante des éléments de traçabilité.

Le Tiers de Confiance n'est pas un Tiers de vérité : il ne prend pas d'engagement sur le contenu des données établies ou conservées, mais sur leur provenance, leur intégrité, leur disponibilité, leur pérennité.

La notion de tiers de confiance donne des obligations en termes de respect des normes, règlements et bonnes pratiques et règles d'éthique en vigueur. Dans certains domaines, il existe des labels, agréments et certifications qui viennent à l'appui du statut du Tiers de Confiance.

Les traces peuvent être établies et conservées entièrement ou partiellement par un Tiers de Confiance. Dans ce cas, l'article 35 de la loi Informatique et Libertés impose que les conditions de sécurité relatives à la conservation des données soient définies contractuellement entre le propriétaire des traces et le Tiers de Confiance.

Dans le domaine de la traçabilité, le Tiers de Confiance peut intervenir à plusieurs niveaux :

- garantie d'intégrité et de provenance des traces ;
- horodatage des traces ;
- conservation, disponibilité et confidentialité des traces ;
- identification des parties.

Eu égard au risque de voir une trace établie et conservée par les soins de son détenteur remise en cause par le juge, la FNTC préconise de faire appel à des Tiers de Confiance pour asseoir la fiabilité et la recevabilité de la Politique de traçabilité.

5.3.6 Application à l'exemple de la validation des CGU

Dans notre exemple de la validation des Conditions Générales d'Utilisation, le contexte juridique est celui de l'établissement d'un contrat entre l'utilisateur et le fournisseur du service : les CGU font partie intégrante de ce contrat et lient les parties par les obligations qui y figurent. Ainsi, les CGU contiendront la Convention de Preuve, au sein de laquelle s'intègre la Politique de Traçabilité.

On pourra avantageusement s'appuyer sur un Tiers de Confiance pour horodater et conserver la trace de la validation des CGU, qui devra impérativement être opposable en justice puisque c'est elle qui est garante de l'acceptation de la Convention de Preuve par l'utilisateur, et donc *a fortiori* de son opposabilité.

En ce qui concerne les données à caractère personnel, la trace servant à conserver la mémoire d'une action volontaire de l'utilisateur, deux options sont possibles :

- inclure les données d'identification de l'utilisateur dans la preuve ;
- inclure dans la preuve un identifiant anonyme de l'utilisateur, qui renvoie à ses données personnelles gérées dans la base de données du service.

Dans la seconde option, la traçabilité ne comporte pas explicitement de données à caractère personnel, et aucune contrainte de destruction ne s'impose donc. En revanche, elle n'est pas autosuffisante et nécessite, pour son interprétation, d'être croisée avec la base de données, qui doit elle aussi être conservée dans des conditions de nature à en garantir l'intégrité.

5.4 Définir le mode de conservation des traces

La conservation des traces doit être sécurisée et assurer l'intégrité de ces dernières dans le temps (notamment lorsqu'elles sont jointes à un acte électronique).

Ces conditions peuvent être remplies, selon le contexte, les enjeux, les volumes concernés, à l'aide de dispositifs techniques et organisationnels différents.

Le support de conservation des traces peut être une simple base de données ou, si l'on veut ajouter une garantie supplémentaire d'intégrité et de disponibilité, un coffre-fort électronique, exploité par le responsable du traitement lui-même ou par un Tiers Archiveur. La FNTC a développé un label « Tiers Archiveur » et un label « coffre-fort électronique », sur lesquels les concepteurs de systèmes de traçabilité pourront s'appuyer.

La périodicité de la sauvegarde des traces sur un système fiable est à arbitrer en fonction de la sensibilité des traces : un dépôt en temps réel dans un coffre-fort normalisé est exigé dans le cas du jeu en ligne, une conservation des traces par paquets quotidiens est souvent suffisante pour des applications moins sensibles.

Lorsque des traces sont déposées de manière asynchrone dans le système de conservation, une attention particulière doit être apportée à la conservation de l'horodatage : la date de l'événement, la date d'établissement de la trace et la date de dépôt de la trace ou du paquet de traces doivent être cohérentes entre elles et en adéquation avec la Politique de Traçabilité.

La garantie d'intégrité est la certitude que les données sauvegardées n'aient pas été altérées depuis le moment de leur établissement. Pour garantir l'intégrité, on pourra s'appuyer sur des mécanismes variés. La duplication des données de traçabilité sur plusieurs supports distincts ou sur des supports non réinscriptibles est un premier pas, mais la valeur probante offerte par ces mécanismes n'est pas avérée.

> La FNTC recommande fortement l'utilisation de mécanismes de nature cryptographique, à base de calcul d'empreinte et de signature cachet serveur. L'horodatage certifié offre également cette garantie.

Application à l'exemple de la validation des CGU

Dans notre exemple de la validation des Conditions Générales d'Utilisation, il est souhaitable que la trace soit générée dès le moment de l'action, et immédiatement archivée dans un coffre-fort d'archivage sécurisé de nature à en garantir la provenance et l'intégrité.

5.5 Identifier les formes de traçabilité à appliquer

On distingue trois types de traces :

Les traces système (aussi appelées « logs applicatifs ») : il s'agit généralement d'une suite d'informations qui rendent compte des différentes opérations techniques réalisées par le système et des anomalies éventuellement rencontrées. Ces traces ont un haut niveau de technicité et sont destinées principalement à des informaticiens pour la maintenance du système.

Les traces fonctionnelles : il s'agit d'enregistrements systématiques des actions métier réalisées dans le système, avec ou sans intervention humaine. Ces traces sont destinées principalement à être présentées aux utilisateurs ou aux administrateurs fonctionnels du système (service clients, back-office…) pour assurer un suivi des opérations.

Les traces certifiées (aussi appelées « preuves ») : il s'agit d'enregistrements autonomes relatifs à une action particulière, destinés à faire foi de son déroulement dans le cadre d'une convention de preuve définie. Dans la pratique, il s'agit en général d'un fichier xml récapitulant l'événement, qui fait l'objet d'un scellement cryptographique (signature cachet serveur, horodatage). Ces traces sont destinées principalement à disposer d'éléments inaltérables faisant foi en cas de contentieux.

Le niveau de confidentialité des traces et leur conservation doivent être adaptés selon les informations qu'elles contiennent et leurs usages. En effet, celles contenant des informations hautement stratégiques pour une entreprise devront être traitées avec une grande rigueur en termes d'accessibilité et de conservation (cas des jeux en ligne pour lesquels les traces sont déposées en temps réel dans un Coffre-fort Électronique). Inversement, un tel niveau de sécurité peut s'avérer surdimensionné pour des traces peu sensibles.

Il est donc nécessaire de prendre en compte le degré d'importance de chaque trace afin d'adapter les moyens à mettre en œuvre pour leur sécurisation. Cela doit faire partie des choix de la Politique de Traçabilité.
Un procédé courant pour la sécurisation de la traçabilité est le chaînage des traces : chaque trace contient, a minima un numéro d'ordre croissant, ou de préférence une empreinte de la précédente. De cette manière, l'intégrité de l'ensemble du système de traçabilité peut être vérifiée en remontant cette chaîne. Le système peut encore être renforcé en ajoutant périodiquement une signature cachet serveur d'un paquet de traces (toutes les N traces ou à intervalles de temps réguliers).

Application à l'exemple de la validation des CGU

Dans notre exemple de la validation des Conditions Générales d'Utilisation, la preuve devant être opposable en justice, il est recommandé de générer une trace certifiée : la trace générée sous forme xml pourra ainsi être scellée par un cachet serveur et horodatée par un Tiers de Confiance.

5.6 Définir les accès aux traces

Le contrôle d'accès aux traces doit être strict et modulé en fonction de leur contenu, de leur finalité et de la réglementation applicable.

La FNTC recommande de restreindre l'accès aux traces aux seules personnes autorisées dans l'exercice de leur fonction.

Les traces système ne doivent être accessibles qu'aux seuls exploitants système.
Les traces métier ne doivent être accessibles qu'aux seuls utilisateurs directement concernés par leurs propres traces et aux superviseurs fonctionnels des services.
Les exploitants systèmes et les superviseurs fonctionnels doivent être astreints à une clause de confidentialité spécifique.

Le droit français impose que les traces soient accessibles sur demande par les autorités judiciaires et antiterroristes.
Dans certains cas, les traces doivent être mises à disposition d'autorités habilitées, comme par exemple l'ARJEL (l'Autorité de Régulation des Jeux En Ligne) pour le secteur des jeux d'argent et de hasard en ligne.

S'il est fait appel à un Tiers de confiance pour la constitution ou la conservation des traces, une attention particulière doit être apportée à certaines clauses contractuelles : accès, transmission, confidentialité, réversibilité des traces. Le client qui confie ses traces à un Tiers de Confiance doit pouvoir exercer un contrôle sur la gestion des traces par le tiers, en particulier disposer d'une traçabilité de l'accès aux traces.

Il est souhaitable que les traces soient systématiquement mises à disposition de l'utilisateur par le service, afin que chacun dispose en toute transparence de moyens équivalents de prouver sa bonne foi.
Une façon de faire est d'envoyer systématiquement des accusés de réception faisant foi des actions réalisées : attention toutefois à ne pas s'appuyer sur un simple mail, dont la valeur probante est incertaine au regard de la jurisprudence. Il sera préférable de permettre à l'utilisateur le téléchargement et la conservation des traces certifiées, comme décrit plus haut.

Application à l'exemple de la validation des CGU

Dans notre exemple de la validation des Conditions Générales d'Utilisation, la preuve cryptographique générée pourra être mise à disposition de l'utilisateur.
Elle sera par exemple déposée dans un coffre-fort d'archivage électronique opéré par un Tiers de Confiance, sous couvert d'un engagement de confidentialité.
Seuls les personnels habilités du fournisseur de service auront la possibilité de consulter les preuves hébergées chez le Tiers de Confiance, en cas de besoin.

5.7 Prévoir la fin de vie des traces

Si les traces contiennent des données à caractère personnel, il est impératif de définir la durée de conservation des traces et de les supprimer à l'issue de cette période.
Si les traces ne contiennent pas de données personnelles, deux cas se présentent : soit il existe une obligation légale relative à la durée de conservation, et il faut l'appliquer ; soit il n'existe pas d'obligation légale et la liberté est totale.

La suppression des traces correspond à plusieurs impératifs :

- le respect des obligations légales (notamment lorsqu'une action judiciaire peut être diligentée) ;
- la libération de l'espace de stockage.

La suppression des traces peut être difficile à mettre en œuvre concrètement en l'absence d'une politique exhaustive et stricte de gestion de la traçabilité. Il convient donc de la prévoir en amont.

Par ailleurs, la suppression d'une trace est susceptible de rompre le chaînage des traces, ce qui peut être problématique si toutes les traces n'ont pas la même durée de conservation.

La suppression des traces sera considérée comme une action à part entière, qui sera elle-même tracée.

La FNTC recommande de concevoir le système de suppression des traces en même temps que le système de traçabilité et de documenter systématiquement la politique de traçabilité et de gestion de preuves.

Application à l'exemple de la validation des CGU

Dans notre exemple de la validation des Conditions Générales d'Utilisation, les traces pourront par exemple être supprimées un an après la désactivation du compte de l'utilisateur.

5.8 Respecter les normes techniques applicables

Dans le domaine de la traçabilité, de nombreuses fonctions de sécurité et de confiance sont mises en œuvre. On peut citer notamment :

- l'horodatage ;
- la signature cachet serveur ;
- l'archivage électronique ;
- l'anonymisation ;
- le chiffrement ;
- le contrôle d'accès…

Tous ces mécanismes répondent à des normes ou standards, et doivent être employés conformément aux normes sectorielles correspondant au service dans lequel la traçabilité est mise en œuvre.

En France, le Référentiel Général de Sécurité (RGS) définit les niveaux de sécurité applicables pour les services des autorités administratives, auxquelles il s'impose. Il se veut également un guide de bonnes pratiques pour le secteur privé. On pourra s'y reporter pour les fonctions de signature, d'horodatage et de chiffrement, sur le site de l'ANSSI. On notera également qu'une proposition de Règlement « identification et services de confiance » a été publiée par la Commission Européenne, qui s'appuiera sur des normes techniques de sécurité (figurant dans des actes d'exécution). Les normes existent et il convient de s'y reporter. La FNTC recommande également de se reporter à sa collection de Guides de la confiance.

En ce qui concerne l'archivage électronique, les labels FNTC « Coffre-fort électronique » et « Tiers archiveur » rendent compte du respect de la norme AFNOR NF Z42-013 intitulée « Archivage électronique - Spécifications relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes ».

Application à l'exemple de la validation des CGU

Dans notre exemple de la validation des Conditions Générales d'Utilisation, les normes à respecter dépendront des choix opérés précédemment. On citera par exemple les normes de signature électronique (pour le cachet serveur, par exemple XAdES), d'horodatage (RFC 3161), d'archivage électronique (norme AFNOR Z42-013, transposée au niveau international dans la norme ISO FDIS 14641-1)…

5.9 Établir une Politique de Traçabilité

Pour renforcer la fiabilité de la traçabilité, il convient d'établir par écrit l'ensemble des règles et normes appliquées dans le cadre de la traçabilité mise en œuvre, et de les faire accepter par l'ensemble des parties prenantes au processus dans lequel cette traçabilité s'insère.

Ces règles seront regroupées au sein d'une Politique de Traçabilité, à laquelle on donnera une valeur contractuelle, soit en l'incluant directement dans un contrat (par exemple contrat commercial ou contrat de travail), soit en l'incluant dans une Convention de Preuve au sein

des Conditions Générales d'Utilisation du service (CGU).
Il est important que les parties prenantes soient tenues par les règles d'établissement et d'interprétation de la traçabilité. La façon d'en imposer le respect dépendra beaucoup du contexte :

- dans le cadre d'un téléservice de l'administration, les conditions d'utilisation du service s'imposent à l'utilisateur et doivent juste être portées à sa connaissance ;
- dans le cadre d'un service privé, les CGU doivent être validées et explicitement acceptées par l'utilisateur ;
- dans un cadre interne à une entreprise, la charte informatique, un avenant au contrat de travail, voire le Document Unique d'Evaluation des Risques instauré par le décret n° 2001-1016 du 5 novembre 2001 peuvent être des supports utiles.

Remarque : La FNTC recommande que la Politique de Traçabilité inclut une justification de la gestion des traces afin :

- d'éviter la constitution de bases de données illicites au regard du respect de la vie privée et des recommandations de la CNIL ;
- de protéger les identités numériques et en garantir l'intégrité ;
- de limiter la conservation des traces à la durée nécessaire (cf. droit à l'oubli numérique en fonction du contexte juridique associé).

6 LA TRAÇABILITÉ PAR L'EXEMPLE

L'importance de la traçabilité peut être illustrée dans divers secteurs économiques, tels que le secteur bancaire (6.1) et le secteur des jeux en ligne (6.2). La traçabilité peut être également mise en œuvre par différents services dématérialisés, et notamment la lettre recommandée (6.3) et le vote électroniques (6.4). Enfin, des entreprises sont particulièrement exposées aux exigences de traçabilité, comme en témoignent les opérateurs de communications électroniques en général (6.5) et les fournisseurs d'accès à internet et hébergeurs, en particulier (6.6).

6.1 La traçabilité dans le secteur bancaire

Une traçabilité nécessaire… Et utile !

Le secteur bancaire « traditionnel » est une profession réglementée, encadré par différentes autorités de tutelles et de contrôle. Les principales en France sont la Banque de France, l'Autorité de Contrôle Prudentiel (ACP), l'Autorité des Marchés Financiers (AMF).

La confiance dans la monnaie est une préoccupation permanente et historique des États. La sécurité de la monnaie scripturale, avec la généralisation de la bancarisation et des offres de services à la clientèle sur internet, nécessite une approche d'encadrement des risques de la part des gouvernements, du législateur et de ces autorités de contrôle.

Le déploiement des systèmes informatiques dans les banques avait provoqué une première vague de prévention des risques avec pour certaines plates-formes techniques des certifications délivrées par des services spécialisés, pour encadrer notamment le secteur de la monétique et les services en ligne.

Il faut distinguer et classer la traçabilité sur les plates-formes bancaires de la manière suivante :

- la gestion de preuve relative aux ordres des clients ;
- la gestion de preuve relative aux actions des collaborateurs et au respect des procédures de séparation des fonctions ;
- l'historique des procédures ;
- la gestion de preuve relative aux fraudes ou aux tentatives de fraude, d'attaques de hacker ou d'intrusion délinquante sur les plateformes.

Les données et les traces doivent être techniquement protégées pour en assurer la confidentialité afin de ne pas permettre des usages frauduleux.

La généralisation de l'authentification forte et/ou de la signature électronique sécurise les échanges financiers entre les banques et leurs clients. Elles permettent de valoriser les traces électroniques et de responsabiliser les acteurs.

Une bonne gestion de preuve, s'appuyant sur une traçabilité à valeur probatoire, permet d'enrichir l'offre de service métier des banques : en effet, pour des raisons de risque, en l'absence d'opposabilité de la preuve, les offres sont bridées (limitation de montants, etc.).
Ainsi, une meilleure traçabilité permet l'innovation dans les services et la contrainte liée à la traçabilité devient une opportunité.

Un contexte juridique riche et vivant

Le contexte juridique et normatif du secteur bancaire est extrêmement contraint, comme le montrent les principales grandes évolutions depuis une dizaine d'années, dont nous faisons la liste ci-dessous :

■ le Comité de Règlementation Bancaire et Financière (CRBF) a mis en place en 1997 le règlement 97.02 sur les « Conditions d'exercice du contrôle interne des établissements bancaires ». Il impose aux banques la mise en place d'un contrôle interne. La dimension d'un contrôle interne recouvre la lutte contre la fraude, l'exactitude des comptes (qui a été complétée par Sarbane Oxley), la mise en place de procédures assurant une bonne organisation ou en cas d'externalisation, une contractualisation couvrant bien les risques ;

■ la réglementation édictée par le Comité de Bâle dite Bâle II, publiée en 2004, a imposé aux banques d'intégrer et d'évaluer les risques opérationnels pour le calcul de leurs fonds propres à partir de 2008 ;

■ la Banque de France a publié en 2000 un livre blanc intitulé « Internet, quelles conséquences prudentielles » et destiné à préciser un certain nombre de recommandations pour les grandes familles de sites internet bancaires et notamment transactionnels ;

■ le 15 novembre 2001, avec la Loi sur la Sécurité Quotidienne, le législateur a confié la mission de la surveillance de la sécurité des moyens de paiements scripturaux à la Banque de France. A cette occasion, un observatoire de la fraude a été mis en place. Toutes les fraudes sur des cartes bancaires sont tracées et consolidées. Cette loi a également précisé un certain nombre de règles et limité la responsabilité financière des particuliers lorsqu'il ne peut leur être opposé de la négligence de leur part ;

■ le Secrétariat Général de la Banque de France, sur la base des recommandations du Livre Blanc de la Banque de France, a confié au CFONB (Comité Français d'Organisation et de Normalisation Bancaires) la mission d'élaborer un référentiel de sécurité pour les sites bancaires et /ou financiers sur Internet. La version 7 de ce profil de protection inspiré des standards Critères Communs, a été publiée en 2004. L'analyse des risques, de la traçabilité et des recommandations des différents métiers doit être prise en compte dès le début du projet. Le contrôle de sa prise en compte doit être réalisé à la fin du projet ;

■ le PCI Security Council encadre la norme de sécurité PCI-DSS (Payment Card Industry-Data Security Standard) promue par les grands réseaux monétiques Visa et Mastercard, rejoints par tous les grands réseaux mondiaux (American Express, JCB, etc.). PCI-DSS s'applique aux partenaires et clients de ces sociétés de cartes bancaires, c'est-à-dire à la fois les commerçants gérant des transactions, les acteurs du e-commerce ou du commerce de proximité, mais aussi les hébergeurs des systèmes de paiement, dont les banques. Le consortium s'est fixé pour objectif d'établir des bonnes pratiques en matière de protection des données stockées sur les cartes bancaires. Les commerçants sont répartis en 4 catégories en fonction de l'importance des risques potentiels, des audits par des Cabinets labellisés étant effectués périodiquement pour les plus exposés ;

■ pour la banque électronique de bourse/titres en ligne, il est nécessaire de prendre en compte la directive MiFID (Markets in Financial Instruments Directive), publiée par l'Union Européenne au mois d'avril 2004. Cette directive uniformise au niveau européen les règles de fonctionnement des marchés financiers et renforce la protection des investisseurs, notamment en ce qui concerne l'obligation d'information que doit la banque à son client, notamment aux particuliers épargnants dont on peut penser qu'ils n'ont pas suffisamment

de connaissances sur leur prise de risque. Les plates-formes internet doivent donc prendre en compte le niveau de connaissance du client, l'information qui lui est faite en fonction de son profil, la vérification de la couverture des ordres et filtrer les ordres inhabituels ou anormaux ;

■ depuis 2008, pour les commerçants de vente à distance, les banques françaises ont progressivement déployé le protocole de sécurité 3D Secure qui permet d'authentifier l'identité du porteur de carte bancaire lors des paiements. Ce contrôle d'identité s'ajoute aux contrôles d'opposition et de capacité financière du porteur. Les traces des différents contrôles doivent bien sûr être conservées et archivées ;

■ depuis 2010, la Banque de France a exigé des banques le déploiement de systèmes d'authentification forte pour les transactions par Carte Bancaire pour le commerce électronique et pour les transactions de banques ou de bourse effectuées sur les sites de banque électronique sur internet. Le procédé doit être non copiable et non rejouable avec par exemple un mot de passe à usage unique ;

■ avec la disparition du réseau X25 en 2012, le CFONB, dès 2008, a recommandé pour les échanges EDI entre les clients entreprises et les banques deux protocoles en remplacement d'ETEBAC 3 et 5 : Swiftnet et Ebics (Electronic Banking Internet Communication Standard). Ces protocoles utilisent des certificats serveurs pour authentifier et chiffrer les échanges. Les ordres d'exécution joints ou disjoints (par un canal séparé) à l'échange des données doivent permettre la validation des instructions par la banque sous réserve des contrôles prudentiels ou juridiques ;

■ depuis 2012, dans le cadre de la mise en place de la signature électronique personnelle pour l'exécution des ordres par Ebics TS, le CFONB a mis en place la « Politique d'Acceptation Commune » (PAC) pour les certificats numériques X509 conformes au RGS. Les Autorités de Certifications doivent impérativement se faire référencer auprès de la commission du CFONB. Par ailleurs, il faut noter que la FNTC publie sur son site www.fntc.org l'annuaire ComPAC recensant les banques pratiquant l'acceptation des certificats conformes à la PAC et Ebics TS.

Des bonnes pratiques en croissance

Les conséquences pratiques de toutes ces dispositions, sont entre autres de favoriser les bonnes pratiques pour les offres télématiques des banques à leur clientèle. La traçabilité et la confidentialité des données et des ordres électroniques passés sur les différentes infrastructures techniques sont encadrées, doivent pouvoir être auditées dans de bonnes conditions de prévention des risques et assurer une gestion de preuve intègre.

Et de fait, sous l'impulsion de la Banque de France, les déploiements par les banques ou les établissements de paiement d'authentification forte, par One Time Password (OTP) et par certificats numériques X509, se généralisent depuis fin 2010 pour les transactions effectuées par la clientèle des particuliers et des entreprises pour la banque à distance et les paiements sur internet.

Les équipements retenus sont principalement par OTP à l'aide de Carte EMV, d'OTP par téléphonie mobile à l'aide de SMS, de certificat numérique téléchargeable, ou de certificat numérique conforme au RGS et délivré en face en face.

Une volumétrie qui entraîne des obligations particulières

Les efforts à faire sont très importants et les quelques chiffres ci-après donnent une bonne idée du périmètre :

- 99 % des français possèdent un compte en banque (source : FBF) ;
- il y a en circulation 88 millions de cartes de paiement à fin 2010 (source : Observatoire de la Fraude BDF), dont 60 millions de cartes bancaires en 2010 (source Groupement CB) ;
- 7 milliards de transactions CB tracées et archivées en 2010 (source : Groupement CB) ;
- 74 % des français ont acheté sur internet en 2010 (source : FEVAD) ;
- il y avait 38 millions d'internautes en France début 2011 (Source : Médiamétrie) dont 44 % réalisent des virements sur leur sites de banque à distance (source : IFOP), qu'il faut tracer et archiver.

Avec un chamboulement en cours qui laisse dubitatif : il y a 67 millions d'abonnements de téléphonie mobile au troisième trimestre 2011 dont 45 % sont actifs en multimédia mobiles (source : ARCEP) et déjà plus de 6 millions de cartes SIM « non voix » fin 2011. Il n'est donc pas étonnant que le commerce mobile, ou « m-commerce », accélère la croissance du commerce et de la banque à distance… Encore d'autres motifs de traçabilité.

Afin de gérer une telle dimension, les directives européennes sur les moyens de paiements permettent d'ouvrir le marché à de nouveaux acteurs comme les Etablissements de Paiement, agréés par les Banques Centrales européennes. Ces nouveaux acteurs ont développé des offres originales, innovantes et qui intègrent pour certaines la téléphonie mobile. Sans pouvoir être exhaustif, on peut citer les sociétés Buyster, Limonetik, Cardsoff, Slimpay, Kwixo, etc., qui prennent en charge en France la traçabilité et assurent les sécurités transactionnelles. Ces acteurs sont ou seront concurrents des grands acteurs de l'internet comme Paypal, Facebook et bien d'autres.

De nouveaux protocoles pour sécuriser la traçabilité

Les nouveaux protocoles bancaires sur Internet améliorent les services de traçabilité, de bouclage et réconciliation comptable. Dans le cadre de cette migration, l'infrastructure de la signature électronique et la gestion de preuve utilisées dans ETEBAC 5 depuis 1992 par un certain nombre d'entreprises françaises a arrêté son activité le 31 décembre 2011 au soir. Le stock de cartes à mémoire vierges et les clés ont été détruites et le Groupement des Cartes Bancaires a assuré la gestion de preuve jusqu'au 30 mars 2012 pour les opérations transmises jusqu'au 31 décembre 2011.

La signature électronique ETEBAC 5, fondée sur des technologies propriétaires, a été transposée dans les nouveaux protocoles Swiftnet et EBICS TS avec des certificats numériques X509.

Pour compléter le dispositif, le CFONB a mis en place la PAC (Politique d'Acceptation Commune). Il s'agit d'un cadre pour une interopérabilité technique et juridique pour permettre une multi-acceptance des certificats conformes au RGS et référencés par le CFONB. Le but est de couvrir les 100 000 entreprises qui effectuent des échanges informatisés et la totalité des entreprises françaises qui effectuent des opérations sur les sites de banques en ligne.

La FNTC s'est impliquée pour cette migration en publiant le guide « Au-delà de la migration ETEBAC », qui a été notamment diffusé par les banques à leurs clients conformément à une

recommandation du CFONB. Ce guide a été suivi par la mise en place de l'annuaire « ComPAC » (COMpatilité PAC), destiné à enregistrer et publier en ligne les déclarations d'usages par les opérateurs de services bancaires et non bancaires. Il s'adresse principalement aux entreprises afin de les guider dans leur choix d'équipement de leurs collaborateurs.

6.2 Le secteur français des jeux en ligne

La loi française 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne, impose à toute société voulant devenir Opérateur de jeux en ligne sur le marché français d'obtenir un agrément auprès de l'Autorité de Régulation des Jeux En Ligne (ci-après l'ARJEL). L'agrément ARJEL nécessite notamment la mise en œuvre d'un « Frontal », dont la fonction première est de tracer toutes les activités de jeu sur le site de l'Opérateur. Le Frontal de l'ARJEL constitue un exemple de solution de traçabilité imposée par la loi, rendant transparentes les activités de jeux en ligne afin d'en contrôler la régularité.

Les joueurs et parieurs français jouaient et pariaient déjà sur des sites enregistrés dans d'autres pays européens, avant la promulgation de la loi. Prenant en considération ces plates-formes de jeu déjà en place à l'étranger, l'ARJEL a conçu un dispositif dit « Frontal », c'est-à-dire une solution additionnelle à l'application de jeu, à travers laquelle le joueur français passe pour pouvoir jouer. Pour garantir l'exhaustivité des flux de jeux pris en charge par le Frontal, l'Opérateur de jeux agréé doit réorienter sur le Frontal tous les flux de jeu venant des joueurs français, même s'ils se connectent sur un site de jeu étranger (contrôle par l'IP de connexion), et même s'ils se connectent depuis un pays étranger (contrôle lors de l'identification du joueur). Afin que les Opérateurs agréés ne soient pas déloyalement concurrencés par les Opérateurs non agréés en France, l'ARJEL met en place les actions judiciaires pour faire fermer l'accès à ces derniers (mise en demeure des Opérateurs étrangers acceptant les joueurs français, demande aux fournisseurs d'accès internet de fermer l'accès à des sites précis). Le Frontal peut ainsi tracer la totalité de l'activité de jeu des joueurs français.

- Pourquoi tracer ? Pour assurer l'intégrité, la fiabilité et la transparence des opérations de jeu, et ce sous le contrôle de l'autorité nationale compétente, l'ARJEL.
- Que tracer ? Toutes les activités des joueurs en ligne dès leur authentification sur le site de l'Opérateur.
- Comment tracer ? L'ARJEL a publié un cahier des charges précis décrivant techniquement le Frontal. En voici un résumé présenté sous l'angle de la traçabilité probante. Le site de l'ARJEL [www.arjel.fr] détaille davantage les exigences techniques requises en la matière.

L'ARJEL décrit le Frontal comme composé d'un « Capteur » et d'un « Coffre-fort électronique ». Le Capteur est la partie qui se place en interruption du flux joueur-application de jeu, qui duplique la totalité de ce flux pour en envoyer un doublon dans le Coffre-fort : le Capteur fabrique les traces. Le Coffre-fort conserve les traces de façon à les rendre accessibles à l'ARJEL et à en garantir la valeur probante.

Parce que l'objectif de la régulation est surtout de protéger le joueur, le flux pris en charge par le Frontal est celui venant du joueur et non pas celui venant de l'application de jeu. Il n'y a donc pas de risque que le Coffre-fort contienne des informations envoyées par l'application de jeu et jamais reçues par le joueur. Toutefois, souvent, dans les jeux de table, il arrive que le protocole d'échange joueur-application de jeu ne soit pas du http mais soit propriétaire, et que certaines actions du joueur apparaissent comme effectuées directement par l'application de jeu. Dans cette situation, la plate-forme de jeu peut envoyer de l'information au Capteur. Dans ce type de situation, il y a un risque de fraude sur l'intégrité du contenu déposé dans le Coffre, car c'est l'Opérateur de jeu qui envoie l'information, celle-ci étant générée par l'application de jeu, qui peut ne pas être en France et ne pas être auditable. L'ARJEL n'accepte a priori pas cette situation. Elle peut toutefois l'accepter exceptionnellement si l'Opérateur démontre qu'il ne peut pas faire autrement pour fournir les données désirées et que de plus il fournit une documentation précise sur ce flux émis.

Les traces viennent du Capteur. Avant de les déposer dans le Coffre-fort, le Capteur doit formater les traces en respectant un format de fichier (en l'occurrence XML), défini par l'ARJEL. Ainsi, lorsque l'ARJEL récupèrera ce fichier XML elle pourra le traiter facilement.
Le Capteur doit déposer dans le Coffre en temps réel, pour augmenter la certitude qu'il n'y a pas eu de modification de la trace avant sa mise au Coffre. Le temps réel est un élément de confiance. En cas de souci technique, si le Capteur ne peut pas déposer en temps réel, alors le service de jeu en ligne doit s'arrêter. Ainsi, en l'absence de traçabilité en temps réel, la confiance doit être maintenue par un arrêt du service.

Dès leur mise en forme, les traces vont du Capteur vers le Coffre-fort, comme un passage de relais, de façon à ne pas avoir de risque de pertes de données. Puis, le Coffre-fort renvoie un accusé de réception. Celui-ci est pour le Capteur la garantie que la trace est prise en compte. Le Coffre-fort ne doit donc le délivrer que lorsqu'il a effectué toutes ses actions d'enregistrement.
Le Coffre-fort scelle cryptographiquement chaque trace à l'aide d'un cachet (équivalent pour un serveur de la signature électronique), réalisé par un composant matériel externe pour augmenter le niveau de sécurité : Hardware Security Module (HSM).
Chaque trace est chiffrée avec une clé de chiffrement délivrée par l'ARJEL. Chaque trace est aussi chaînée par le Coffre avec la trace précédente. La continuité du chaînage permet de garantir que les traces ne sont ni perdues ni modifiées depuis leur mise au Coffre. Il n'est pas possible de modifier, d'ajouter ou de supprimer des traces sans que cela se voie dans la cohérence du chaînage. Et il serait visible de supprimer toutes les traces précédant celle que l'on veut altérer, car la première trace est consignée lors du démarrage de la plate-forme, lors de « la cérémonie des clés ».
La cérémonie des clés est un jalon important du projet : c'est la mise en production du Frontal et donc l'ouverture réelle du site de jeu. Lors de la cérémonie des clés, l'ARJEL remet les certificats nécessaires à la signature électronique et au chiffrement, et consigne la première trace.

Les données contenues dans le Coffre-fort ne sont accessibles que par authentification forte. Les certificats permettant l'accès sont seulement ceux de l'ARJEL : l'Opérateur et l'exploitant du Frontal ne peuvent pas accéder au contenu du Coffre-fort. L'ARJEL peut accéder aux données à tout moment, grâce à une interface de requêtes avec accès distant

sécurisé, permettant de télécharger des lots de traces sur des périodes. L'ARJEL n'a donc pas à demander une autorisation ou même à prévenir de ses contrôles sur les données.
Un autre niveau d'accès de l'ARJEL est l'accès physique à la plate-forme Frontal, à sa demande. Pour des raisons d'organisation humaine, cet accès peut être donné dans les 48 heures. C'est pour cette raison que la plate-forme Frontal doit être localisée sur le territoire français, alors que la plate-forme de jeu peut, elle, être localisée à l'étranger.
Enfin, pour délivrer l'agrément autorisant à être Opérateur de jeux d'argent en ligne en France, l'ARJEL exige un dossier technique complet, de plusieurs centaines de pages. Avec ce dossier technique, l'Opérateur montre que tout a été mis en œuvre pour répondre aux exigences de l'ARJEL susmentionnées. L'ARJEL délivre donc un agrément sur la base de la documentation remise par l'Opérateur et pourra contrôler que la réalité y correspond lors de la cérémonie des clés, lors des requêtes au Coffre-fort, et lors de l'accès physique au Frontal, puis six mois après la mise en service par le biais de la certification à six mois effectuée par un tiers agréé par l'ARJEL, dénommé certificateur.
Le dossier technique indique également tout ce que ne peut pas directement contrôler l'ARJEL. En effet, il contient le code source du Frontal, celui de l'application de jeu, un descriptif de l'organisation de l'exploitation, une copie de tous les contrats signés avec les différents prestataires intervenant sur le Frontal ou l'application de jeu, et surtout la Certification de Sécurité de Premier Niveau (CSPN) que le Coffre-fort a dû obtenir auprès de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), garantissant son niveau de sécurité. La documentation doit être intégralement en français, les contrats en langue étrangère devant être traduits.
Dans tous ces éléments mis en œuvre pour obtenir l'agrément de l'ARJEL, les changements doivent être documentés et l'ARJEL doit en être informée.
Le Coffre-fort doit conserver 12 mois glissant d'activité en ligne pour l'ARJEL. Ensuite les données doivent être conservées pendant 5 ans, ce qui correspond à la durée de validité d'un agrément ARJEL, et peuvent être remises à l'ARJEL à sa demande.

L'ARJEL a conçu un système de traçabilité organisant une transparence technique à plusieurs facettes : (i) transparence permanente sur l'activité des joueurs par le Frontal, (ii) transparence sur l'utilisation de produits non frauduleux par la remise des codes sources, (iii) transparence sur les droits d'accès par la cérémonie des clés, (iv) transparence sur les modifications par la déclaration et la possibilité de contrôler sur site géographique.
Toute l'infrastructure de l'Opérateur de jeux est transparente pour l'ARJEL. Le Frontal est un véritable outil de traçabilité à valeur probante alliant l'état de l'art en matière de signature électronique, de chiffrement et de conservation.

Ce contrôle des opérations de jeu par la traçabilité est complété par un certain nombre d'obligations de reporting quotidien mis à la charge des opérateurs de jeux en ligne agréés, et surtout de certifications de nature technique, juridique et comptable fréquentes. Outre la certification technique à six mois (unique), une certification est effectuée chaque année après la délivrance de l'agrément afin de contrôler le respect des obligations non plus seulement techniques, mais également légales et comptables.

6.3 Prouver des échanges : la traçabilité de la lettre recommandée électronique

Suite à la publication du décret 2011-144 du 2 février 2011 sur la lettre recommandée électronique (LRE), il est désormais possible d'utiliser ce moyen pour obtenir la traçabilité d'un échange numérique. Ce décret vient compléter l'article 1369-8 du Code civil qui encadre l'envoi d'une LRE relative à la conclusion ou à l'exécution d'un contrat par courrier électronique, à condition que ce courrier soit acheminé par un tiers selon un procédé permettant :

(i) d'identifier le tiers,
(ii) de désigner l'expéditeur,
(iii) de garantir l'identité du destinataire et
(iv) d'établir si la lettre a été remise ou non au destinataire.

Le destinataire a en effet un délai de 15 jours pour décider d'accepter ou de refuser de recevoir la lettre. Le contenu de cette lettre, au choix de l'expéditeur, peut être imprimé par le tiers sur papier pour être distribué au destinataire ou adressé à celui-ci par voie électronique. Dans ce dernier cas, si le destinataire n'est pas un professionnel, il doit avoir demandé l'envoi par ce moyen ou en avoir accepté l'usage au cours d'échanges antérieurs. Des conventions de preuves avec les usagers particuliers peuvent donc être mises en place pour l'usage fréquent d'envoi en recommandé électronique, les deux parties ayant intérêt à utiliser ce nouveau moyen (accessibilité améliorée, délais réduits, coûts réduits pour l'expéditeur).

Les bénéfices en termes de traçabilité

Un tiers postal proposant un service conforme au décret :

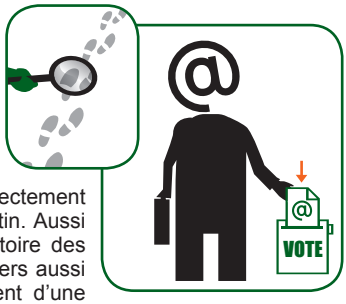
- garantit que le dépôt a bien été effectué auprès du tiers (date et identification de la lettre). En pratique, cette exigence sera le plus souvent satisfaite par l'utilisation d'un service d'horodatage du dépôt, conforme aux exigences du décret 2011-434). Il faut noter qu'alors le tiers postal garantit plus que la LRAR (Lettre Recommandée avec Accusé de Réception) papier actuelle, puisque l'intégrité du contenu du dépôt est alors également garantie et démontrable ;
- en cas d'option d'accusé de réception :
  - ► garantit, si le courrier est remis, que le destinataire a accepté de le recevoir (un délai de 15 jours est donné pour obtenir l'acceptation ou le refus de la part du destinataire),
  - ► garantit, si le courrier est remis, la date et l'heure à laquelle le destinataire a accepté de recevoir le courrier ;
- garantit que la preuve d'envoi est conservée pendant une durée d'un an. Il n'est pas exigé que le tiers conserve la preuve de réception par le destinataire ; toutefois, le service d'accusé de réception n'a que peu d'intérêt si l'acceptation par le destinataire ne peut être prouvée par l'expéditeur. En pratique, il convient de conserver la preuve de réception, soit au niveau du tiers, soit au niveau de l'expéditeur à qui le tiers l'aura fournie. Le décret précise tout de même que l'accusé de réception doit pouvoir être adressé à l'expéditeur de telle manière qu'il puisse le conserver.

Il faut noter que le décret ne contient aucune exigence explicite concernant la vérification d'identité du destinataire par le tiers postal en cas de demande d'accusé de réception. Toutefois, l'article 1369-8 du Code civil, que le décret vient préciser, requiert de garantir l'identité du destinataire : « Une lettre recommandée relative à la conclusion ou à l'exécution d'un contrat peut être envoyée par courrier électronique à condition que ce courrier soit acheminé par un tiers selon un procédé permettant d'identifier le tiers, de désigner l'expéditeur, **de garantir l'identité du destinataire et d'établir si la lettre a été remise ou non au destinataire**. ».

Un service n'offrant aucune garantie dans ce domaine a de fortes chances d'être invalidé juridiquement et n'atteindrait donc pas son but de protection juridique de l'échange, puisqu'un tel service est destiné à la conclusion ou à l'exécution d'un contrat par courrier électronique. En pratique, un service de LRE avec AR devra mettre en place un dispositif permettant d'avoir un bon niveau de confiance et de preuve, notamment dans l'authentification du destinataire.

On peut noter que les textes définissent les exigences minimales permettant de donner au service de LRE une valeur juridique. Il est possible de fournir un service à plus forte valeur ajoutée, en incluant un niveau supérieur de traçabilité tant pour l'émetteur que pour le destinataire.

6.4 Vote électronique et traçabilité



Cadre général

En matière de vote électronique, la notion de traçabilité est directement liée à la capacité de garantir la sincérité et l'intégrité du scrutin. Aussi longue est l'histoire de la démocratie, aussi longue est l'histoire des tentatives de fraude, que cette démocratie concerne des univers aussi disparates que les élections politiques, l'élection du président d'une association de joueurs de boules, les élections professionnelles (CE/DP), la démocratie actionnariale ou l'élection dans les ordres professionnels.
Le vocable « vote électronique » recouvre à la fois les dispositifs de lecture par code barre, le vote à distance par internet ou par téléphone, et le vote présentiel par machine à voter ou boîtier de vote.
Le point commun entre tous ces scrutins, quels que soient l'outil ou la population de votants concernée consiste en ce que, par principe, tout résultat électoral est susceptible d'être contesté pendant une période de recours défini par la loi ou les règlements statutaires. Le juge électoral devra alors pouvoir contrôler a posteriori la régularité des opérations de vote et la sincérité du scrutin. En cas de vote électronique, ce contrôle s'opérera principalement à partir d'une e-traçabilité de l'ensemble des procédures organisationnelles et techniques.
En plus du juge électoral éventuellement saisi, la CNIL, dans le cadre de sa mission de contrôle du traitement de données à caractère personnel, est habilitée à effectuer des inspections sur le déroulement de n'importe quelle opération de vote. Elle a émis deux recommandations explicitant la mise en œuvre de la traçabilité des opérations de vote électronique :

- la délibération n°98-041 du 28 avril 1998 concernant les systèmes de vote par code barre ;
- la délibération n° 2010-371 du 21 octobre 2010 concernant le vote électronique par internet, qui abroge l'ancienne recommandation de Juillet 2003.

Dans beaucoup de cas, la traçabilité des opérations de vote est encadrée par un texte administratif, législatif ou réglementaire. On citera par exemple et de façon non exhaustive :

- le Code électoral ;
- le Code du travail pour les élections professionnelles ;
- le Code de la Santé pour les élections à l'ordre des infirmiers ;
- le Code de commerce…

Le vote à bulletin secret.

Lorsque le scrutin électronique requiert l'anonymat des votants, la production d'éléments à valeur probante tout au long du processus est le seul moyen pour protéger chacune des parties (électeurs, candidats, organisateurs, prestataires) de l'accusation d'avoir contribué à frauder le scrutin, et donc pour assurer la sincérité de celui-ci.

Dans la pratique :

Les e-traces seront constituées par :

- *le scellement (empreinte numérique) des différents éléments constituant le système de vote électronique au sens large : liste électorale, logiciel, urne électronique, liste d'émargement, configuration des serveurs, etc. ;*
- *l'horodatage de la liste d'émargement ;*
- *l'utilisation de procédés cryptographiques (authentification forte, signature électronique, cachet serveur) permettant de tracer précisément l'historique de l'ensemble des accès au système.*

Ces traces seront conservées sur un support non réinscriptible pendant toute la durée de la période de recours.

Mais ces traces ne devront pas pouvoir remettre en cause la sincérité du scrutin qu'elles sont supposées garantir, en permettant de lever l'anonymat ou la confidentialité du vote, dans le cas d'un scrutin à bulletin secret. La traçabilité ne doit pas comporter de lien entre le votant et l'expression de son vote, ni comporter de date pour certaines opérations, comme le dépôt du bulletin dans l'urne électronique : le principe d'une urne étant de mélanger les bulletins, il ne faut pas pouvoir les ranger dans un ordre chronologique.

On comprend bien que dans ce cas, aucun lien ne pourra être établi entre la liste d'émargement et l'urne électronique. Ainsi, les bulletins de vote ne comporteront pas d'horodatage qui permettrait de faire un lien direct ou indirect avec la date et l'heure du vote stockée dans la liste d'émargement.

De même, la possibilité éventuelle pour le votant de pouvoir vérifier son vote, offerte par certains systèmes, ne doit pas se transformer en preuve de vote rendant possible l'achat de vote ou la contrainte.

D'une façon générale, les dispositifs destinés à renforcer l'intégrité et la traçabilité du scrutin peuvent comporter l'inconvénient de renforcer le risque de corruption du scrutin. Ce risque sera à chaque fois, éliminé par des procédés organisationnels dont on gardera, à leur tour, une trace irréfutable.

En matière de vote électronique à bulletin secret, il est donc tout aussi important de s'assurer de la non conservation de certaines données que de la conservation de certaines autres.

Le vote des assemblées générales d'actionnaires

Le cas est tout à fait différent pour les votes pour lesquels, à l'inverse, l'identification du votant et le lien avec l'expression de son vote sont essentiels à la perfection de la régularité du processus.

Il en est ainsi dans le cas du vote lors des assemblées générales d'actionnaires. Le vote y est de nature censitaire, c'est-à-dire que ce sont les actions qui votent et non, stricto sensu, les individus qui les détiennent.

Il devient impératif de s'assurer et de garder trace de l'identité de l'actionnaire, et du nombre exact d'actions détenues au moment du vote. En outre tout actionnaire pourra demander à consulter le détail des votes des résolutions soumises à l'approbation des actionnaires, lors de l'assemblée.

En ce qui concerne l'identité de l'actionnaire le Code de commerce dispose (article R. 225-77, alinéa 2, 3°, 2e phrase) que le formulaire de vote doit comporter une signature électronique.

Un aspect important est celui du moment de détention des actions prenant part au vote. L'extrême réactivité du marché des actions et les impératifs financiers interdisent un quelconque « blocage » de la propriété des actions. L'article R225-85 du Code de commerce dispose une date d'arrêté des positions, ou « record date », fixée à J-3 à 0 heures. Autrement dit, le propriétaire détenteur des droits de vote à l'assemblée est celui qui détient les actions antérieurement à cette « record date ». En cas d'usage du droit de vote lié à des actions vendues antérieurement à cette « record date », les votes correspondants seront invalidés.

Pour prévenir les contestations, voire les risques d'annulation de l'assemblée générale par le juge, ces deux points spécifiques, concernant la signature électronique et l'horodatage des bulletins de vote, sont deux éléments essentiels de traçabilité à mettre en œuvre.

En ce qui concerne les actionnaires inscrits au registre nominatif de l'Émetteur des actions, la mise en œuvre ne pose pas de difficultés particulières ; il en va autrement des actionnaires au porteur en raison du grand nombre et de la dispersion des teneurs de compte.

6.5 Opérateurs de communications électroniques

L'article L.34-1, II. du Code des postes et des communications électroniques pose le principe que « les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, **effacent ou rendent anonyme** toute donnée relative au trafic ». Cette obligation s'impose à toutes les personnes qui, « au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit ». Les fournisseurs d'accès à Internet ne sont donc pas les seuls concernés : cette obligation s'impose également aux entreprises offrant un accès Internet à leurs clients, aux cybercafés, etc.

Par exception à ce principe, l'article L.34-1, III. du même Code prend des dispositions pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales ou des infractions au droit d'auteur. Dans le seul but de mettre, si nécessaire, les traces de connexion à disposition de l'autorité judiciaire ou de la Haute Autorité pour la Diffusion

des Œuvres et la Protection des droits sur Internet (HADOPI), « il peut être **différé pour une durée maximale d'un an** aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques ». Ces exceptions, ainsi que la liste des données à conserver, figurent aux articles R.10-13 et R.10-14 du Code des postes et des communications électroniques (décret du 24 mars 2006).

6.6 Fournisseurs d'accès à Internet et hébergeurs

Aux termes de l'article 6, II. de la loi du 21 juin 2004 pour la confiance dans l'économie numérique, les fournisseurs d'accès à Internet (ci-après FAI) et les fournisseurs d'hébergement de contenus « **détiennent et conservent les données** de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires ».
Citons quelques exemples de contenus concernés par ce dispositif :

- les sites web ;
- les blogs ;
- les fichiers placés en téléchargement, par exemple par ftp ;
- les sauvegardes et stockages en ligne…

La durée de conservation de ces données a été fixée à un an par l'article 3 du décret du 25 février 2011. Les données à conserver sont déterminées par l'article 1er de ce même décret, qui distingue entre les fournisseurs d'accès et les hébergeurs.

À titre d'exemple, ce décret prévoit la conservation, lors de la souscription d'un contrat chez un FAI ou un hébergeur, de :

- au moment de la création du compte, l'identifiant de cette connexion ;
- les nom et prénom ou la raison sociale ;
- les adresses postales associées ;
- les pseudonymes utilisés ;
- les adresses de courrier électronique ou de compte associées ;
- les numéros de téléphone ;
- le mot de passe ainsi que les données permettant de le vérifier ou de le modifier, dans leur dernière version mise à jour.

Pour chaque opération sur un contenu, l'hébergeur doit conserver les éléments suivants :

- l'identifiant de la connexion à l'origine de la communication ;
- l'identifiant attribué par le système d'information au contenu, objet de l'opération ;
- les types de protocoles utilisés pour la connexion au service et pour le transfert des contenus ;
- la nature de l'opération ;
- les date et heure de l'opération ;
- l'identifiant utilisé par l'auteur de l'opération lorsque celui-ci l'a fourni.

FAI et hébergeurs doivent assurer en sus la sécurité des données conservées : l'obligation de sécurité prévue à l'article 34 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique à ces données.

Les données doivent être conservées de manière à permettre une extraction dans les meilleurs délais à la demande des autorités judiciaires.

7 GLOSSAIRE

Archivage électronique sécurisé (ou Archivage à vocation probatoire)
Ensemble des modalités de conservation et de gestion de données électroniques ayant une valeur juridique lors de leur établissement ; cet archivage garantissant la valeur juridique jusqu'au terme du délai durant lequel des droits y afférents peuvent exister (« Politique et pratiques d'archivage », version du 24 juillet 2006, § 1.1, disponible sur le site de l'ANSSI).

Authentification
L'authentification a pour but de vérifier l'identité dont se réclame une personne ou une machine. Généralement, l'authentification est précédée d'une identification, qui permet à cette entité de se faire reconnaître du système au moyen d'un élément dont on l'a doté (un identifiant). En d'autres termes, s'identifier consiste à communiquer une identité préalablement enregistrée, s'authentifier consiste à apporter la preuve de cette identité (art. 3.2 du Référentiel Général de Sécurité).
Processus électronique qui permet de valider l'identification électronique d'une personne physique ou morale, ou l'origine et l'intégrité d'une donnée électronique. (Art. 3.4 de la Proposition de Règlement Identification et services de confiance.)

Cachet
Données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données électroniques pour garantir l'origine et l'intégrité des données associées (art. 3.20 de la Proposition de Règlement Identification et services de confiance).

Certificat Électronique
Document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire (Décret 30 mars 2001).

Confidentialité
Propriété d'une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés. (Source http://www.securite-informatique.gouv.fr)

Convention de preuve
Accord exprès écrit par lequel les parties modifient les règles normales de la preuve judiciaire soit quant à la charge de la preuve, soit quant à la détermination des faits à prouver, soit quant à l'emploi des procédés de preuve.

Données à caractère personnel
Toute information relative à une personne physique identifiée ou qui peut être identifiée directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne (Source : Loi Informatique et Libertés – Article 2)

Horodatage
Information permettant de démontrer qu'une donnée (par exemple, un document, un enregistrement d'audit, ou une signature électronique) existait à un instant donné (Norme NF Z42-013 «Spécifications relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes»).

Intégrité
Caractéristique d'une information qui n'a subi aucune destruction, altération ou modification intentionnelle ou accidentelle. (Source : norme AFNOR NF Z 42-013)

Pérennité
Aptitude que doit avoir l'information à traverser le temps durant tout son cycle de vie en préservant son intégrité. (Source : norme AFNOR NF Z 42-013)

Preuve
Démonstration de l'existence d'un fait ou d'un acte (contrat, testament) dans les formes admises par la loi (Vocabulaire juridique Gérard Cornu).

RGS (Référentiel Général de Sécurité)
Émis par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), le RGS définit des niveaux de sécurité standard applicables aux autorités administratives.

Scellement
Procédé permettant de garantir l'intégrité d'un document par l'utilisation de fonctions cryptographiques.

Signature électronique
Donnée sous forme électronique, qui :
• est jointe ou liée logiquement à d'autres données électroniques (l'acte signé) ;
• identifie le signataire ;
• garantit le lien du signataire avec l'acte signé.
La signature électronique est réalisée à l'aide de certificats en utilisant les méthodes de cryptographie asymétrique.

Traçabilité
Au sens général, la traçabilité est : « l'aptitude à retrouver l'historique, l'utilisation ou la localisation d'une entité au moyen d'identifications enregistrées » (selon la norme ISO 8402 : Management et assurance de la qualité).

Appliquée aux Systèmes d'Information et/ou aux échanges numériques, la traçabilité d'un système peut être définie comme l'aptitude à reconstituer a posteriori un historique fidèle des événements qui se sont déroulés au sein du système.

Trace
Une suite d'empreintes ou de marques que laisse le passage d'un être ou d'un objet ; marque laissée par une action quelconque ; ce à quoi on reconnaît que quelque chose a existé ; ce qui subsiste d'une chose passée. (Dictionnaire Robert, V° « Trace »).

8 PARTICIPANTS

Ont participé à l'élaboration de ce guide :

- Pascal Agosti (Cabinet Caprioli & Associés)
- Olivier Normand (Cleona)
- Etienne Billet (DataSyscom)
- Denis Bourdillon (Pitney Bowes Asterion)
- Eric Caprioli (Cabinet Caprioli & Associés)
- Régis Chevalier (Docapost DPS)
- Frédéric Connes (Hervé Schauer Consultants)
- Thibault de Valroger (Keynectis)
- Jean-Pierre Doussot (Esopica)
- Alexandre Foucher (Cecurity.com)
- Pierre Lecomte (Docapost DPS)
- Pauline Le More (LeMore Avocat)
- Dimitri Mouton (Demaeter)
- Didier Renauld (MiaXys)
- Bernard Starck (Bernard Starck Conseil)

FÉDÉRATION DES TIERS DE CONFIANCE
19, rue Cognacq-Jay
75007 – Paris
Tel. 01 47 50 00 50
info@fntc.org - www.fntc.org

A PROPOS DE LA LA FÉDÉRATION DES TIERS DE CONFIANCE

La Fédération des Tiers de Confiance (FNTC) est un acteur majeur de la sécurisation des échanges électroniques et de la conservation des informations, maillons essentiels à la maîtrise de l'ensemble de la vie du document électronique.
Créée en 2001, la FNTC regroupe les professionnels de la dématérialisation, à savoir : les prestataires et éditeurs de confiance (acteurs de l'archivage électronique, de la certification, de l'horodatage et des échanges dématérialisés); les experts et les représentants des utilisateurs ainsi que les institutionnels et les professions réglementées.
La FNTC a pour but d'établir la confiance dans l'espace numérique, de promouvoir la sécurité et la qualité des services et de veiller au respect d'une charte d'éthique de la profession.

LES ADHÉRENTS FNTC*:

Accelya ; ACN ; ACOSS ; Actradis.fr ; Adminium ; AFCDP ; Alexandre Diehl ; AllPerf ; Almerys ; Alphacode ; APECA ; Argus DMS ; Ariadnext ; Asterion ; Bernard Starck ; Bruno Couderc Conseil ; Bull ; Cabinet Caprioli & Associés ; Cecurity.com ; Cedricom ; Celtipharm ; CertEurope ; ChamberSign ; Chambre des Huissiers de Justice du Québec ; Chambre Nationale des Huissiers de Justice ; Chambre Nationale des Huissiers de Justice et Agents d'Exécution du Cameroun ; Cleona ; Compagnie Nationale des Commissaires aux Comptes ; Conex ; Conseil National des Greffiers de tribunaux de commerce ; Conseil Supérieur de l'Ordre des Experts-Comptables ; Corus ; Cryptolog ; DARVA ; Darwin Consulting & Finance ; Data One ; Data Syscom ; Demaeter ; Digimedia Interactivité ; Docapost BPO ; Docapost DPS; Document Channel ; DPII Telecom ; Ecosix ; Edificas ; Edokial ; EESTEL ; eFolia ; Elcimai Financial Software ; Election Europe ; ESI ; Esker ; Esopica ; Forum Atena ; G.L.I. Ingénierie et Services ; Gdoc Lasercom ; Hervé Schauer Consultants ; Imprimerie Nationale ; IN Continu et Services ; Interb@t ; Isilis ; Issendis ; jedeclare.com ; Kahn & Associés ; Keynectis-OpenTrust ; Legalbox ; LeMore Avocats ; Locarchives ; Maileva ; Marc Chédru Conseil ; MIPIH ; Notarius ; Novapost ; Novarchive ; Odyssey Services ; Office des Postes et Télécommunications Polynésie Française ; OFSAD ; OPUS Conseils ; Perfect Memory ; PPI ; Primobox ; Provigis ; Sagemcom ; Scala ; SealWeb ; Sogelink/DICT.fr ; Stocomest ; Syrtals ; TESSI Ged ; UIHJ ; Univers Monétique ; ViaStorage ; Voxaly Electionneur ; Wacom ; Worldline ; Xeonys.

** Liste arrêtée au 1er octobre 2013*

Conception graphique et illustration : www.idsg.fr