**Principes fondamentaux du droit et application au secteur informatique**

**Le droit** = il ne définit pas la valeur des actes, le bien ou le mal mais il fait la distinction entre ce qui est permis et défendu dans une société humaine

**Au niveau de l’individu :**

•  Respect de l’éthique : adapter son comportement en fonction des valeurs que l’on juge essentielles

•  Respect du droit : adapter son comportement par peur de la sanction en cas de violation • « la démarche éthique permet de prendre en considération des attentes de la société qui souvent précèdent le droit ». Lulin, 2011

1. **Les sources du droit en France**

* **Hiérarchie des normes**

**•  La Constitution de la Ve République du 4 octobre 1958** et son Préambule de la constitution de 1946.

**• Les conventions et traités internationaux ratifiés par la France** = Le droit communautaire et européen : Conventions, Traités, directives (les Etats de l’UE doivent prendre des mesures de transposition en droit interne pour rendre les directives applicables) et règlements (directement applicables dans les Etats membres de l’UE / RGPD 25 mai 2018) des instances européennes comme Traité sur l'union européenne ou la Convention européenne de sauvegarde des Droits de l'Homme et des Libertés fondamentales du 4 novembre 1950

•   **La loi** votée par les députés et les sénateurs (Parlement), promulguée par le Président de la République et publiée au journal officiel (Ordonnance).

**•   Les règlements de l'autorité́ administrative : décrets, arrêtés ministériels**

**•  La Jurisprudence est l’œuvre de l’autorité judiciaire** = les décisions de justice rendues par les tribunaux et les cours qui appliquent une règle de droit à des situations de faits ou l’ensemble des décisions rendues par les tribunaux sur un point de droit litigieux.

Pour qu’il existe une jurisprudence, deux conditions doivent être réunies :

* La répétition c’est-à-dire l’habitude prise par les tribunaux de statuer dans un certain sens,
* La hiérarchie : ainsi, il arrive qu’une seule décision fasse jurisprudence lorsqu’elle émane d’une juridiction d’un très haut niveau dans la hiérarchie judiciaire. Les décisions rendues par la Cour de Cassation finissent donc par s’imposer à toutes les juridictions.

•  La Jurisprudence crée du droit dans le sens où :

* Elle interprète les lois (parfois obscures),
* Elle comble les lacunes de la loi (qui ne prévoit pas forcément tous les cas de figure). En effet, un juge ne peut pas refuser de juger (déni de justice). Donc, lorsque la loi est obscure ou incomplète, le juge se référera aux principes généraux du droit, à l’équité et au bon sens,
* Elle fait évoluer le droit.

Cependant, la Jurisprudence n’est pas définitive dans la mesure où les juges ont toujours la possibilité de changer d’avis.

**•  La coutume (usage)** : une pratique qui présente un caractère habituel et qui, de ce fait, tend à se poser en règle de droit. L’usage doit être ancien, constant, notoire et général et repose sur une conviction de tout le monde que c’est un comportement obligatoire

**• La doctrine** = l’ensemble des écrits des personnes qui sont autorité en matière juridique : professeurs de droit ou experts • La doctrine peut être considérée comme une source du droit car elle influence les autres sources du droit : • Le législateur dans la définition des lois • Les magistrats dans leur jugement en leur faisant infléchir la jurisprudence • Les influences :

* Le contrôle de la hiérarchie des lois = Le conseil constitutionnel vérifie que les lois sont conformes à la Constitution (QPC = question prioritaire de constitutionnalité).

A l'occasion de procès, les tribunaux, administratifs et judiciaires, vérifient l'application des traités prioritairement aux lois et règlements. La Cour de cassation est en ce sens très importante puisqu’elle vérifie toujours la bonne application du droit et qu’elle permet d’uniformiser les décisions (rôle unificateur de la Cour de cassation). •  Pour le droit européen, les tribunaux peuvent consulter la Cour de justice de l’Union européenne pour vérifier la conformité du droit interne au droit européen.

Le contrôle de la hiérarchie des textes réglementaires est assuré par les tribunaux administratifs et le Conseil d'État. Si un traité est incompatible avec la Constitution, celle-ci doit être modifiée. Enfin, pour les coutumes et usages qui sont des règles non écrites, ils peuvent compléter la loi ou combler un vide juridique mais ne peuvent jamais être contraire à une loi.

**• La hiérarchie des sources du droit en France :**

* **La Constitution 1958 (Préambule constitution de 1946)**
* **Les Traités européens et internationaux**
* **La loi, l’ordonnance**
* **Le règlement (Décret, arrêté, circulaire)**
* **Usage / Jurisprudence**
* **Doctrine**

**Une norme supérieure prévaut sur une norme inférieure (sauf en matière de droit du travail).**

1. **La personnalité juridique**

**Définition** : une personne juridique est une personne qui est à la fois, titulaire de droits : droit de jouissance et droit d’exercice (droit de propriété par exemple) et soumis à des obligations (payer des impôts par exemple)

Deux catégories de personnes juridiques :

•  **Personne physique** : un être humain vivant sans distinction de sexe, d’ethnie et de religion (de la naissance au décès)

**•  Personne morale** : un groupement d’individus réunis dans un intérêt commun (de l’enregistrement à la fin) • de droit public : collectivités publiques, établissements publics • De droit privé : société, association, syndicat • À but lucratif : l’objectif est de réaliser des bénéfices • A but non lucratif : l’objectif premier n’est pas de réaliser des bénéfices.

1. **Identité numérique et protection**

L’identité numérique est l’ensemble des traces numériques qu’une personne ou une collectivité laisse sur Internet. Toutes ces informations, laissées au fil des navigations, sont collectées par les moteurs de recherche, comme Google, et sont rendues public. Une identité numérique, ou IDN, peut être constituée par : un pseudo, un nom, des images, des vidéos, des adresses IP, des favoris, des commentaires etc. Cette identité sur internet a donc une influence sur la [e-réputation](https://www.reputationvip.com/fr/guide/e-reputation), sur la façon dont les internautes perçoivent une personne. En résumé, l**’**identité numérique est l’image renvoyée sur internet, l’image virtuelle, dématérialisée.

Mais ces données, qui se retrouvent à la portée de tous, constituent un risque permanent pour les utilisateurs et pour la protection de leur vie privée. Aujourd’hui, les informations inscrites sur Internet sont très difficiles à effacer.

Même si Google a mis en place un formulaire pour adresser des demandes de droit à l’oubli, celui-ci reste très compliqué à remplir. Cependant, la plateforme en ligne Forget.me est un outil gratuit qui permet de remplir plus facilement puis d’envoyer les demandes de retrait des données. Dans cette continuité Reputation VIP propos un service dédié à la suppression des avis Google My Business. Des outils permettent donc de gérer son image et sa présence sur Google. Des lois sur l’identité numérique ont aussi été votées dans le but de protéger les utilisateurs. Récemment, la CNIL et le Conseil d’État ont interdit un dispositif qui permettait de connaître le parcours des piétons pour une utilisation commerciale. La CNIL, la Commission Nationale de l’Informatique et des Libertés a été créée pour assurer la protection des données personnelles. La commission veille à ce qu’internet ne porte pas atteinte à la vie privée des utilisateurs.

* **Les différents types d’identité numérique**

Il existe plusieurs types d’identités numériques qui répondent à différentes catégories d’informations, en fonction de la source, de son contenu et de son auteur. Ces informations circulent aussi parfois à l’insu de leur utilisateur, et peuvent avoir une influence néfaste sur l’intégrité de la personne ou de l’entité correspondante.

On peut facilement créer trois catégories distinctes d’identité numérique correspondant à l’origines des sources différentes et aux informations divulguées :

* **L’identité déclarative**

Ce type d’identité numérique correspond aux diverses informations qui ont été déclinées par la personne ou l’entité concernée, avec des renseignements variés, portant sur la nature du sujet, sur son état civil et sur d’autres éléments très objectifs.

* **L’identité calculée**

L’identité calculée résulte des différentes analyses menées à propos de l’identité agissante. Les conclusions permettent ainsi d’établir un profil de l’individu ou d’un service auquel il est affilié.

* **L’identité agissante**

L’identité agissante est déterminée par les différentes actions menées sur le web par l’utilisateur. Ainsi, on pourra effectuer une trace de ce dernier en observant ses attitudes et ses habitudes à partir de son compte personnel. Ses données seront ainsi récoltées. Le code bancaire et le mot de passe n’ont plus aucun secret pour ces sites web en guise d’illustration. Par ailleurs, ces informations sont une vraie mine d’or pour certaines entreprises, qui utilisent des données de masse en tant que statistiques très instructives au niveau commercial. Une question se pose alors : où se limite le droit à la vie privée et aux données privées ?

* **Pourquoi protéger son identité numérique ?**

Dans le monde d’hier, qui se développait sans internet, l’identité des personnes était protégée. Aujourd’hui, la connexion permanente empêche de gérer ses données personnelles correctement. Par exemple, le *cloud computing* ou information en nuage, est l’une des pratiques courantes qui met en danger l’identité virtuelle. Ce procédé consiste à stocker des fichiers sur des serveurs comme Youtube, Facebook, Dropbox ou Google Drive. Des données, parfois personnelles, se retrouvent sur le c*loud* qui peut être exposé à des risques comme des brèches de sécurité ou des piratages. Pourtant, maîtriser son identité numérique est primordial.

Les recruteurs, les amis ou les collègues de travail n’hésiteront pas à Googliser le nom de la personne pour trouver des informations. Le risque est que l’identité numérique ait des répercussions directes sur la vie réelle. Une mauvaise identité numérique ou e-reputation, avec des informations compromettantes sur la toile, peut discréditer une personne lors d’une recherche d’emploi. C’est pour cette raison qu’il est préférable d’éviter de polluer une identité numérique professionnelle avec des informations trop personnelles.

Les plateformes de *microblogging* comme Facebook ou Twitter donnent la possibilité de publier tout ce qui vous passe par la tête : vos activités, vos envies, votre humeur, votre mécontentement. Cependant, ces courts textes peuvent être lus par votre patron qui peut donc se rendre compte de votre ennui au travail ou que votre arrêt maladie est un prétexte pour faire la fête. Dans les cas les plus extrêmes, certaines personnes payent les conséquences d’une mauvaise *e-reputation* toute leur vie. Avant de publier quelque chose sur internet, répétez-vous cette phrase de Warren Buffet : « Il faut 20 ans pour construire une réputation et cinq minutes pour la détruire ».

* **Comment gérer son identité numérique sur le web ?**

Les utilisateurs sont obligés de remplir leur profil avec le maximum d’informations pour pouvoir bénéficier d’une visibilité optimale sur la toile. Néanmoins, la divulgation de tous ces renseignements ne peut pas se faire sans précautions. Voici quelques reflexes à avoir pour éviter de prendre des risques liés à votre image et à votre e-notoriété :

* **Gérer ses paramètres de confidentialité sur les réseaux sociaux**

Trop de personnes oublient cette étape indispensable. Les réseaux sociaux sont une source d’informations conséquentes et les paramètres de base ne vous protègent pas assez. Sans certaines modifications, l’utilisateur s’expose à une usurpation d’identité numérique.

* **Se méfier de ce qui est gratuit**

« Si c’est gratuit, vous êtes le produit. » Lorsque vous naviguez, likez ou recherchez, vous dévoilez gratuitement vos choix de consommateurs. Pour les entreprises privées, ces données sont précieuses puisqu’elles permettent de mieux vous comprendre pour mieux vous vendre. De nos jours, naviguer sans donner d’informations, personnelles ou non, est quasiment impossible.

* **Changer de mot de passe**

Aujourd’hui, il existe des manières plutôt simples pour se procurer un mot de passe. Changer de mot de passe régulièrement rend cette tâche plus compliquée et sécurise un peu plus vos données personnelles et professionnelles. Idéalement, vous devez changer de mot de passe tous les trois mois.

* **Ne pas cliquer sur n’importe quel lien**

L’hameçonnage est une technique courante pour récupérer des informations. Le cybercriminel se fait passer pour une entreprise ou une personne de confiance soit par e-mail, soit par un faux site. Malgré la notoriété de cette anarque, encore beaucoup d’internautes cliquent sur des liens dangereux.

1. **La preuve informatique**

* **Définition de la preuve informatique**

Le régime de la preuve diffère selon les domaines. En droit pénal, commercial ou administratif, la preuve se fait par tous moyens. En droit civil, le nouvel article 1358 (issu de la réforme du droit des contrats du 10 février 2016) dispose que « hors les cas où la loi en dispose autrement, la preuve peut être apportée par tous moyens ».

La loi n° 2000-230 du 13 mars 2000 transposant la directive 1999/93/CE portant adaptation du droit de la preuve aux technologies de l’information et relative à la signature électronique a modifié les articles 1316 ancien et suivants du Code civil, fondant la recevabilité des preuves informatiques. Ces dispositions résident aujourd'hui aux articles 1363 et suivants du Code civil. Cette loi a conféré à l’écrit électronique la qualité de preuve légale.

**A. Conditions à la recevabilité de preuve informatique**

Deux conditions sont nécessaires à la recevabilité de l’écrit électronique (article 1366 du Code civil) :

* La personne dont elle émane doit pouvoir être dûment identifiée.
* Il doit être établi et conservé dans des conditions de nature à en garantir l’intégrité.

**B. Force probante de la preuve informatique**

L’article 1366 du Code civil dispose « l'écrit sur support électronique a la même force probante que l'écrit sur support papier » : les preuves informatiques ne souffrent pas de leur caractère immatériel en termes de force probante. Toutefois, la force probante peut être mise à mal par les doutes relatifs à l’intégrité de la preuve informatique.

**C. Risques et doutes portant sur la preuve informatique**

Les risques de falsification de la preuve ne sont pas l’apanage des supports informatiques. La notion de faux apparue dans le droit romain a été successivement reprise par le droit d’Ancien régime et le code pénal de 1810.

Toutefois, la preuve informatique peut être facilement altérable et difficilement traçable, c’est pourquoi des obligations entourant la collecte de cette preuve incombant aux experts et huissiers permettent d’en garantir l’authenticité.

C’est le cas des huissiers de justice qui doivent se conformer à une série de mesures techniques lors d’un constat électronique. Ainsi, une capture d’écran nécessite par exemple que l’huissier mentionne l’adresse IP, vide les mémoires caches, vérifie l’absence de connexion à un serveur proxy, décrive le matériel utilisé…

Des normes AFNOR encadrent la collecte des preuves électroniques. En matière de preuve électronique, droit et technique s’associent afin de garantir une efficience procédurale.

Dans les relations commerciales, en propriété intellectuelle ou pour défendre son e-réputation, le recours à la preuve électronique est devenu à la fois commun et indispensable.

1. **La signature électronique**

La loi du 13 mars 2000 instaure une présomption de fiabilité pour les solutions de signature électronique qui répondent à certaines contraintes spécifiques, étant précisé que les Prestataires de certifications électroniques (PSCE) jouent un rôle déterminant dans ce dispositif.

Conformément à l’article 1367 du code civil (anc.1316-4), la signature électronique revêt une double fonction : elle manifeste le consentement au contenu du document sur lequel elle est apposée et elle sert également de moyen d’identification du signataire, en ce qu’elle est supposée être personnelle et unique.

Dans ce système, l’identité du signataire repose sur l’utilisation d’un certificat électronique dit « qualifié » qui est délivré au signataire par un prestataire de service de certification électronique qualifié.

Le recours à la signature électronique consiste « en l’usage d’un procédé fiable d’identification garantissant son lien avec l’acte auquel elle s’attache. La fiabilité de ce procédé est présumée, jusqu’à preuve contraire, lorsque la signature électronique est créée, l’identité du signataire assurée de l’intégrité de l’acte garantie dans les conditions fixées par décret en Conseil d’Etat (art 1367 CC).

1. **Les prestataires de services de certifications électroniques (PSCE)**

Ces PSCE sont accrédités par le Comité français d’accréditation (Cofrac), et l’Agence nationale de sécurité des systèmes d’information (Anssi qui a remplacé la Direction centrale de la sécurité des systèmes d’information en juillet 2009).

Le rôle des PSCE est déterminant puisqu’ils doivent assurer l’authentification par l’usage d’un certificat électronique. Conformément à un arrêté du 26 juillet 2004, « la vérification de l’identité d’une personne à laquelle le certificat électronique qualifié est destiné, est effectuée en sa présence sur présentation d’un document officiel d’identité comportant une photographie par le prestataire de services de certification électronique ou par un mandataire qu’il désigne et qui s’engage auprès de lui par contrat ».

De plus, les PSCE ont également l’obligation de conserver, éventuellement sous forme électronique, toutes les informations relatives aux certificats électroniques qui pourraient s’avérer nécessaires pour faire la preuve en justice de la certification électronique ou d’utiliser des systèmes de conservation de certificats qui garantissent que l’introduction de la modification des données est réservées aux seules personnes autorisées à cet effet par le prestataire et que toute modification de nature à compromettre la sécurité du système puissent être détectées.

1. **Certificat électronique éphémère**

Pratique désormais courante : ce certificat est délivré en ligne par l’intermédiaire de plateformes de signatures électroniques utilisant des certificats électroniques dits éphémères ou encore à la volée. Il n’est valable que pour une seule signature pour l’acte auquel il est destiné. Il est ensuite automatiquement détruit. Souvent pour être activé, un code d’activation du certificat est adressé au signataire par SMS.

Le règlement 910/2014 sur l’identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, dit eIDAS, adopté le 23 juillet 2014 vise à garantir un haut niveau d’harmonisation des règles sur la signature électronique de l’Union européenne.

1. **Le règlement eIDAS**

La réglementation eIDAS fixe les règles d’utilisation et de reconnaissance légales des procédés de signature électronique des pays membres de l’Union Européenne. Un prestataire de service de confiance doit être en conformité avec ce règlement.  
La Commission Européenne identifie et liste par pays les prestataires de services de confiance certifiés reconnus sur l’ensemble du territoire européen.

Le règlement eIDAS établit également le principe de non-discrimination. La recevabilité juridique d’une signature ne peut donc être refusée au motif que celle-ci est au format électronique. Toute signature électronique dispose donc d’une valeur probatoire au sein de l’Union Européenne.

* **Application en France**

Le règlement européen eIDAS a été retranscrit en droit français dans le code civil aux articles 1366 « L'écrit électronique a la même force probante que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité. »

et 1367 **«**La signature nécessaire à la perfection d'un acte juridique identifie son auteur. Elle manifeste son consentement aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte. 

Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat. »

Ces articles établissent la valeur juridique de la signature électronique en France. Ils reprennent les règles d’utilisation et le principe de non-discrimination établis par le règlement eIDAS. En France, l’ANSSI est l’organisme référent en matière de signature électronique. Il identifie et contrôle les prestataires de services de confiance afin de s’assurer de leur conformité avec le règlement eIDAS. Il est également en charge des certifications des prestataires de services de confiance, reconnus ensuite au niveau européen.

1. **LES CERTIFICATIONS AFNOR**

ISO 27001 est une certification adaptée aux prestataires qui souhaitent rassurer leurs clients sur la gestion de la sécurité des informations qui leur sont confiées par la pertinence des mesures mises en place. C’est un gage de confiance pour la préservation de la confidentialité, la disponibilité et l’intégrité des données.

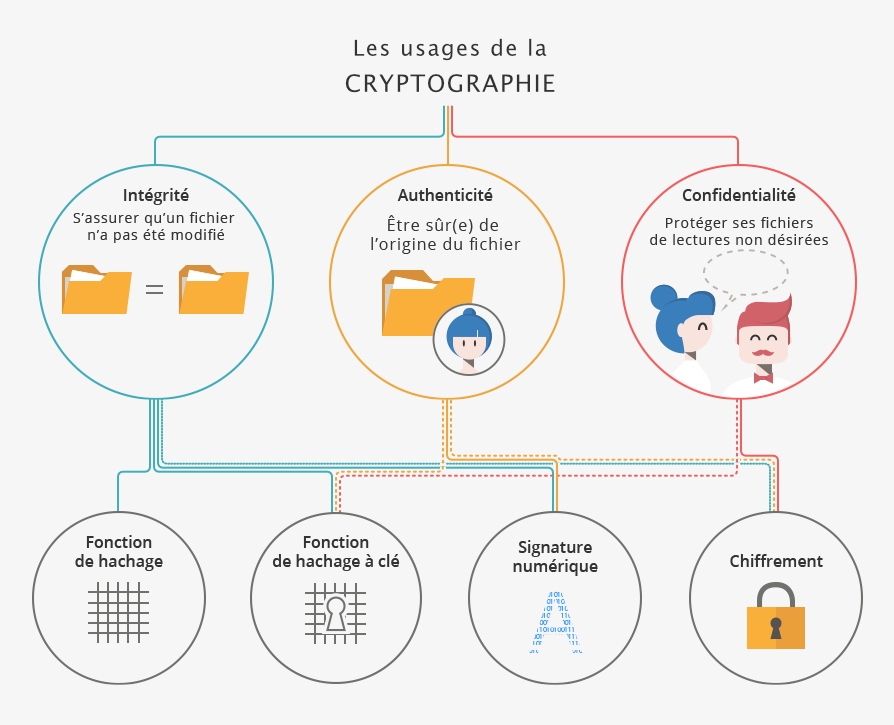
De nombreux fournisseurs de cloud appliquent ces règles. ISO 22301 est une certification de la continuité d’activité, qui apporte des garanties sur la disponibilité des données et qui est également adaptée à l’activité des fournisseurs de cloud. La qualification « SecNumCloud » de l’ANSSI est depuis peu disponible et dédiée aux acteurs du cloud voulant valoriser leur fort investissement en moyens organisationnels et techniques. Le niveau de service attendu à délivrer par le fournisseur de cloud est exigeant et notamment adapté à la sensibilité des données des OIV et de l’administration. Par ailleurs, certains secteurs réglementés, tel que celui de la santé par exemple, sont soumis à des obligations légales. Les hébergeurs de données de santé à caractère personnel, dont une grande partie est fournisseur de cloud, mais également les info géreurs associés, doivent être certifiés selon les exigences du référentiel HDS (Hébergeur de Donnée de Santé), basé à 80 % sur l’ISO 27001.

1. **La cryptologie**

Le moyen de cryptologie désigne « tout matériel ou logiciel conçu ou modifié pour transformer des données, qu’il s’agisse d’informations ou de signaux, à l’aide de conventions secrètes ou pour réaliser l’opération inverse avec ou sans convention secrète. Ces moyens de cryptologie ont principalement pour objet de garantir la sécurité du stockage ou de la transmission des données en permettant d’assurer leur confidentialité, leur authentification ou le contrôle de leur intégrité ».

La prestation de cryptologie s’entend quant à elle de « toute opération visant à la mise en œuvre, pour le compte d’autrui, de moyens de cryptologie ».

*Historiquement, la cryptologie correspond à la science du secret, c'est-à-dire au chiffrement. Aujourd'hui, elle s’est élargie au fait de prouver qui est l'auteur d'un message et s'il a été modifié ou non, grâce aux signatures numériques et aux fonctions de hachage.*



Étymologiquement, la cryptologie est la science (λόγος) du secret (κρυπτός) . Elle réunit la cryptographie (« écriture secrète ») et la cryptanalyse (étude des attaques contre les mécanismes de cryptographie).

La cryptologie ne se limite plus aujourd’hui à assurer la **confidentialité** des secrets. Elle s’est élargie au fait d’assurer mathématiquement d’autres notions : assurer l’**authenticité** d’un message (qui a envoyé ce message ?) ou encore assurer son **intégrité** (est-ce qu’il a été modifié ?).

Pour assurer ces usages, la cryptologie regroupe quatre principales fonctions : le hachage avec ou sans clé,  la signature numérique et le chiffrement.

Pour expliquer la cryptologie, nous utiliserons dans nos exemples les personnages traditionnels en cryptographie : Alice et Bob.

**Pourquoi la cryptologie existe-t-elle ?**

1. **Pour assurer l’intégrité du message : le hachage**

La cryptologie permet justement de détecter si le message, ou l’information, a été involontairement modifié. Ainsi, une « **fonction de hachage** » permettra d’associer à un message, à un fichier ou à un répertoire, une empreinte unique calculable et vérifiable par tous. Cette empreinte est souvent matérialisée par une longue suite de chiffres et de lettres précédées du nom de l’algorithme utilisé, par exemple « SHA2» ou « SHA256 ».

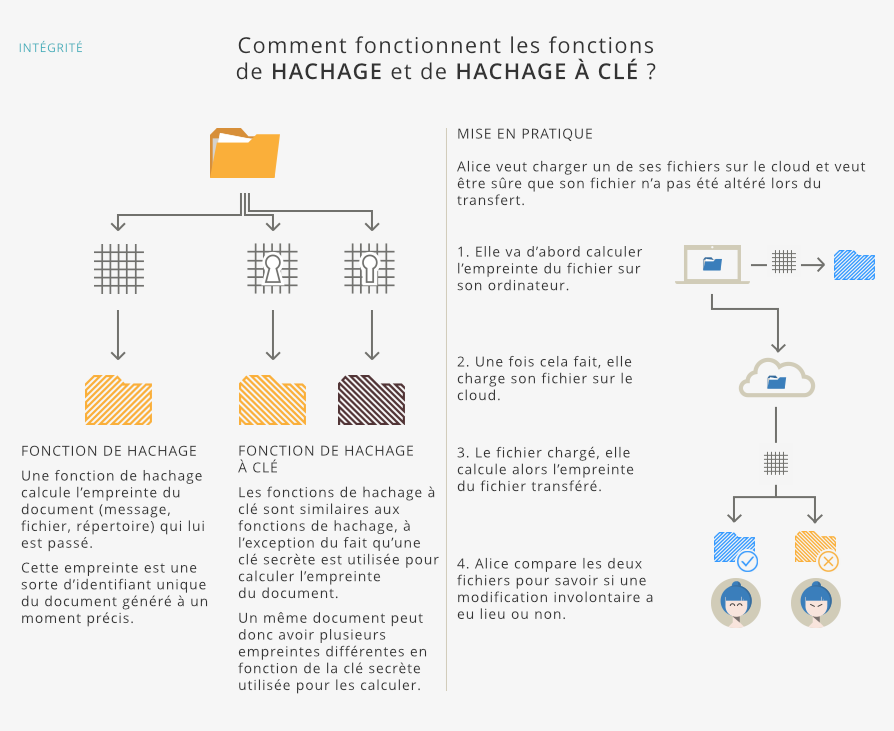
Il ne faut pas confondre le chiffrement, qui permet d’assurer la confidentialité, c’est-à-dire que seules les personnes visées peuvent y avoir accès, et le hachage qui permet de garantir que le message est intègre, c'est-à-dire qu’il n’a pas été modifié.

**Le hachage, pour quoi faire ?**  
Pour sauvegarder vos photos sur votre espace d’hébergement (de type « cloud » par exemple) et vérifier que votre téléchargement s’est bien déroulé ?Pour synchroniser vos dossiers et détecter ceux qu’il faut sauvegarder à nouveau et ceux qui n’ont pas été modifiés ?

Il existe aussi des « **fonctions de hachage à clé**» qui permettent de rendre le calcul de l’empreinte différent en fonction de la clé utilisée. Avec celles-ci, pour calculer une empreinte, on utilise une clé secrète. Pour deux clés différentes l’empreinte obtenue sur un même message sera différente. Donc pour qu’Alice et Bob calculent la même empreinte, ils doivent tous les deux utiliser la même clé.

C’est parmi ces fonctions de hachage à clé que l’on trouve celles utilisées pour stocker les mots de passe de façon sécurisée.

**Le hachage à clé, pour quoi faire ?**  
Votre service préféré reconnait votre mot de passe quand vous vous connectez ?Vous voulez pouvoir détecter si quelqu’un modifie des documents sans vous le dire ?



1. **Pour assurer l’authenticité du message : la signature**

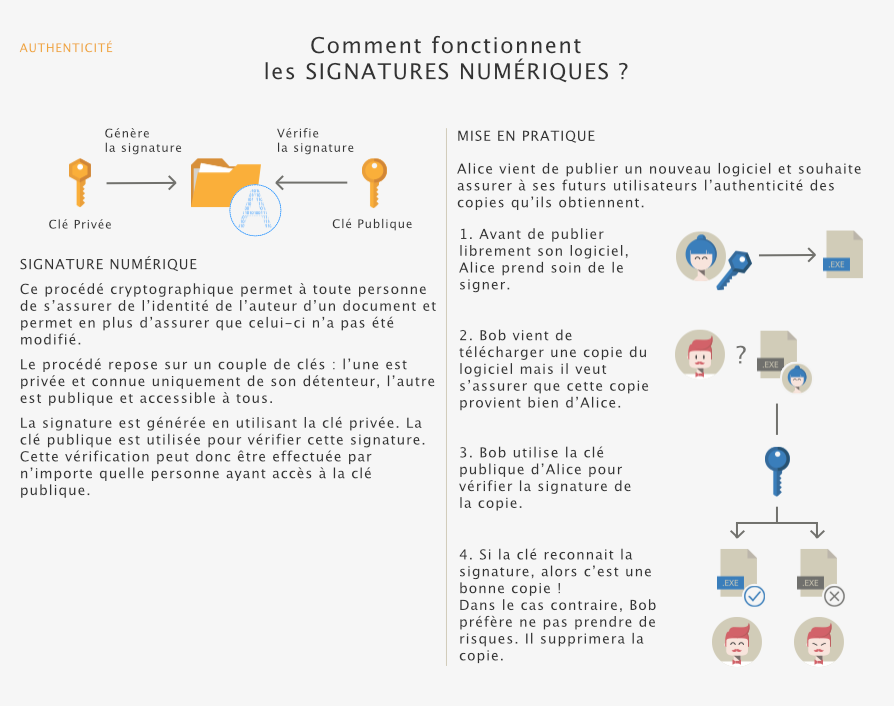
Au même titre que pour un document administratif ou un contrat sur support papier, le mécanisme de la « **signature**» - numérique - permet de vérifier qu’un message a bien été envoyé par le détenteur d’une « clé publique ». Ce procédé cryptographique permet à toute personne de s’assurer de l’identité de l’auteur d’un document et permet en plus d’assurer que celui-ci n’a pas été modifié.

**La signature numérique, pour quoi faire ?**  
*Vous voulez garantir être l’émetteur d’un courriel ?  
Vous voulez vous assurer qu’une information provient d’une source sûre ?*

Pour pouvoir signer, Alice doit se munir d’une paire de clés :

* L’une, dite « publique », qui peut être accessible à tous et en particulier à Bob qui est le destinataire des messages qu’envoie Alice ;
* L’autre, dite « privée », qui ne doit être connue que d’Alice.

En pratique, Alice génère sa signature avec sa clé privée qui n’est connue que d’elle. N’importe quelle personne ayant accès à la clé publique d’Alice, dont Bob, peut vérifier la signature sans échanger de secret.



### Pour assurer la confidentialité du message : le chiffrement

Le chiffrement d’un message permet justement de garantir que seuls l’émetteur et le(s) destinataire(s) légitime(s) d’un message en connaissent le contenu. C’est une sorte d’enveloppe scellée numérique. Une fois chiffré, faute d'avoir la clé spécifique, un message est inaccessible et illisible, que ce soit par les humains ou les machines.

**Le chiffrement, pour quoi faire ?**  
Vous voulez vous assurer que seul le destinataire ait accès au message ?Vous souhaitez envoyer ces informations sous enveloppe numérique et non lisible par tous comme sur une carte postale ?

Il existe deux grandes familles de chiffrement : le chiffrement symétrique et le chiffrement asymétrique.

Le **chiffrement symétrique** permet de chiffrer et de déchiffrer un contenu avec la même clé, appelée alors la « clé secrète ». Le chiffrement symétrique est particulièrement rapide mais nécessite que l’émetteur et le destinataire se mettent d’accord sur une clé secrète commune ou se la transmettent par un autre canal. Celui-ci doit être choisi avec précautions, sans quoi la clé pourrait être récupérée par les mauvaises personnes, ce qui n’assurerait plus la confidentialité du message.

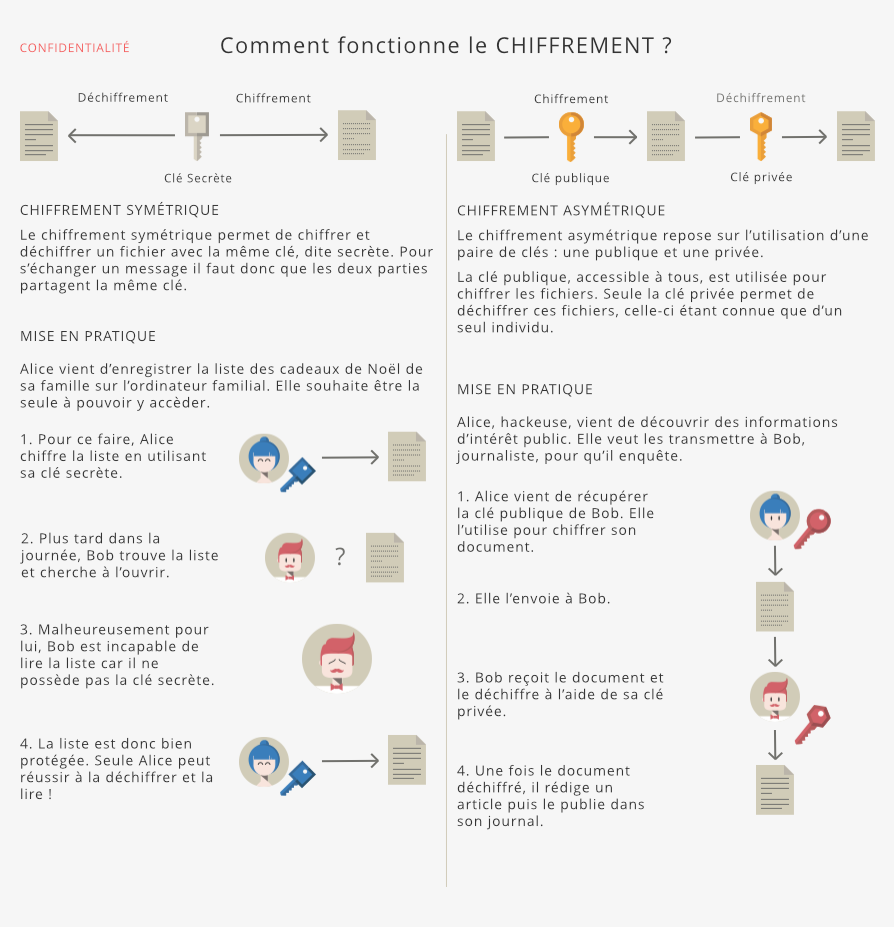
Le **chiffrement asymétrique** suppose que le (futur) destinataire est muni d’une paire de clés (clé privée, clé publique) et qu’il a fait en sorte que les émetteurs potentiels aient accès à sa clé publique. Dans ce cas, l’émetteur utilise la clé publique du destinataire pour chiffrer le message tandis que le destinataire utilise sa clé privée pour le déchiffrer.

Parmi ses avantages, la clé publique peut être connue de tous et publiée. Mais attention : il est nécessaire que les émetteurs aient confiance en l’origine de la clé publique, qu’ils soient sûrs qu’il s’agit bien de celle du destinataire.

Autre point fort : plus besoin de partager une même clé secrète ! Le chiffrement asymétrique permet de s’en dispenser. Mais il est malheureusement plus lent.

Pour cette dernière raison, il existe une technique combinant chiffrements « symétrique » et « asymétrique », mieux connue sous le nom de « **chiffrement hybride** ».

Cette fois, une clé secrète est déterminée par une des deux parties souhaitant communiquer et celle-ci est envoyée chiffrée par un chiffrement asymétrique. Une fois connue des deux parties, celles-ci communiquent en chiffrant symétriquement leurs échanges. Cette technique est notamment appliquée lorsque **le site visité débute par « https ».**



Source : Cnil.fr