LES CAHIERS TECHNIQUES DE **CELOG**

LA PREUVE NUMERIQUE

& COLLECTE PROBATOIRE

BONNES PRATIQUES EN CAS DE SITUATIONS PRÉ-CONTENTIEUSES OU CONTENTIEUSES

DATE D'EDITION : AVRIL 2019

CELOG
LA PREUVE DANS L'ENVIRONNEMENT NUMERIQUE

Dans un univers mouvant et incertain, les organisations sont aujourd'hui confrontées à de nombreux risques internes ou externes.

Départ d'un salarié indélicat avec des données stratégiques, violation des droits de propriété intellectuelle, non-respect du contrat par un fournisseur... sont autant d'atteintes graves à la bonne marche des affaires.

Dans ces situations, la question de la preuve est centrale car ne pas pouvoir prouver ses droits revient à ne pas en avoir. Ce problème est amplifié dans le monde numérique compte tenu de la volatilité de l'information. C'est pourquoi, il est primordial d'acquérir les bons réflexes dans ce type de situation.

C'est l'objectif premier de ce cahier technique.

CELOG est un centre d'expertises informatique indépendant spécialisé dans la preuve immatérielle.

Créé en 1976, CELOG est aujourd'hui un acteur majeur et reconnu dans les domaines de l'investigation, de la collecte et de la matérialisation de la preuve dans l'environnement numérique.

LA PREUVE NUMERIQUE & COLLECTE PROBATOIRE

BONNES PRATIQUES EN CAS DE SITUATIONS PRÉ-CONTENTIEUSES OU CONTENTIEUSES

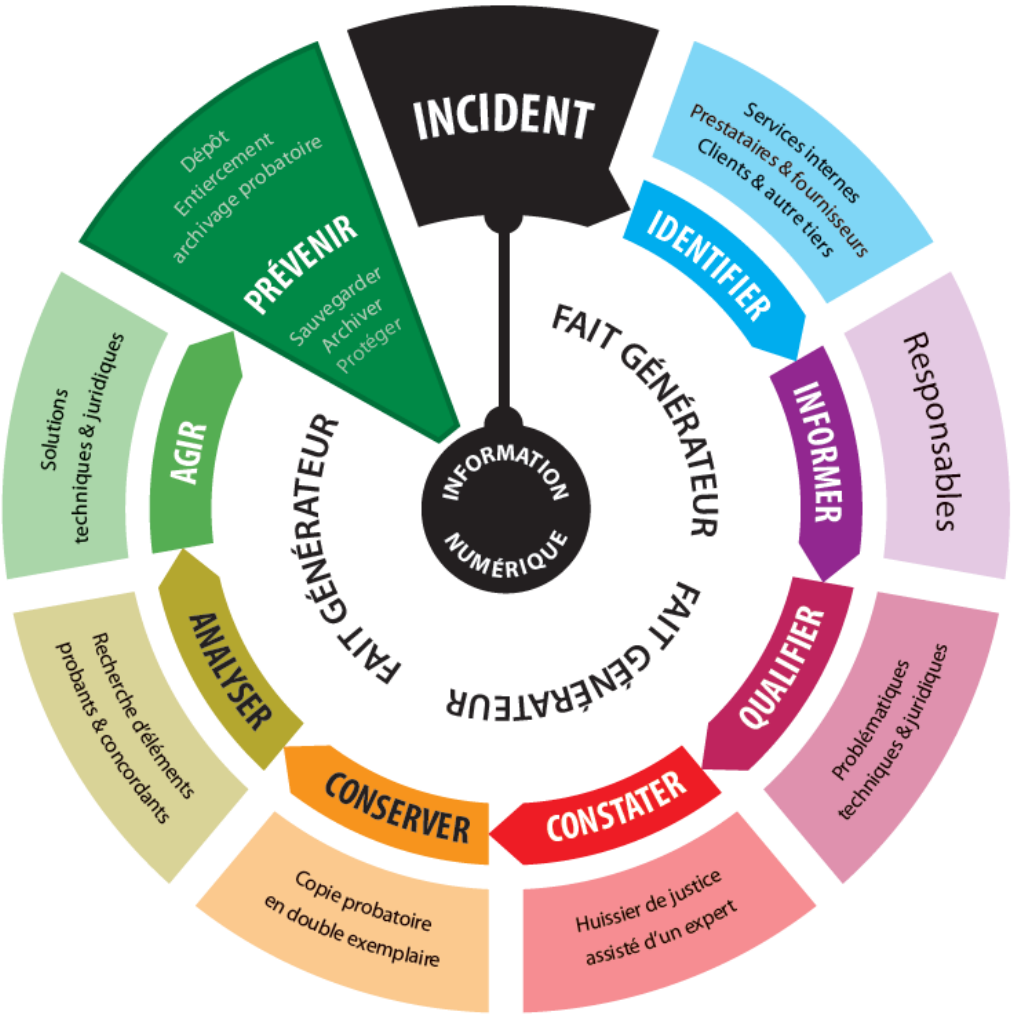


Schéma général de gestion de la preuve numérique

Depuis plusieurs années, l'informatisation et l'intégration constante des nouvelles technologies au monde de l'entreprise ont fait apparaître de nouvelles pratiques qui ont contribué à l'émergence de dérives inattendues.

Aujourd'hui, le « vol » des données informatiques constitutives du patrimoine informationnel (savoir-faire, informations confidentielles, bases de données, etc.), la suppression volontaire de fichiers ou de dossiers importants, l'utilisation non autorisée de la messagerie électronique ou de l'accès à internet, etc., sont des risques quotidiens pour les entreprises. La longue liste des agissements conduisant à ces dommages émaille désormais quotidiennement l'actualité.

Comment réagir ? Comment agir ? Comment s'y préparer ou anticiper ?

De la prévention à la protection, il existe désormais de nombreux moyens techniques (gestion des accès, archivage électronique des données, de la messagerie électronique, des journaux de connexion, etc.) et juridiques (règlement intérieur, charte informatique, clause contractuelle, etc.) pour encadrer les différentes situations à risque. Malgré ces mesures, les entreprises doivent faire face à ces événements dommageables. Dans cette hypothèse et afin d'obtenir réparation, il est primordial d'en rapporter la preuve dans des conditions efficaces.

Ce manuel pratique a pour but de présenter une méthodologie fiable et rapide de collecte et de conservation de l'information numérique à des fins probatoires applicables à différents cas de figure. Il s'adresse à la fois aux dirigeants et cadres de l'entreprise mais également aux spécialistes du droit chargés de les assister dans leurs démarches (juristes, avocats) ou sollicités pour constater de telles dérives (huissiers de justice).

Ce document détaille les critères requis pour qu'une information numérique collectée puisse être utilisée à titre de preuve. En effet, sa collecte doit être réalisée dans des conditions particulières et sa conservation doit également répondre à des exigences connexes pour garantir sa valeur juridique.

I. L'INFORMATION NUMÉRIQUE COMME MODE DE PREUVE

Les risques préalablement évoqués (« vol » de données, utilisation non autorisée de fichiers, etc.) peuvent se rencontrer dans tout type de structure (TPE, PME, grandes entreprises), indépendamment du secteur d'activité ou de la situation géographique. Les grandes structures sont souvent mieux préparées et équipées (services informatiques dédiés, moyens humains et financiers) que les petites entités pour faire face à ces incidents, sans pour autant détenir toutes les clés pour les gérer.

Contrairement aux idées reçues, ce type de comportements n'est pas uniquement du fait des salariés. Toute personne travaillant dans et/ou pour le compte d'une entreprise est susceptible d'indélicatesse à son égard : qu'elle soit en activité (stagiaires, salariés, dirigeants ou tiers intervenant dans ses locaux), qu'elle soit sur le départ (démission, retraite) ou qu'elle n'appartienne déjà plus à l'entreprise (licenciement, préretraite).

Après avoir défini ce qu'est une information numérique et détaillé le régime qui lui est applicable en rappelant les principales évolutions en matière de preuve électronique, nous vous présenterons les quatre critères à réunir pour l'ériger au rang de preuve.

A. DÉFINITION ET CARACTÉRISTIQUES DE L'INFORMATION NUMÉRIQUE

Qu'entend-on par « information numérique » ? Adaptée du terme anglais « digital information », cette expression fait référence à toute information présentée de manière dématérialisée. Il peut s'agir à la fois des données constitutives de cette information (texte, image, son, vidéo, etc.) aussi bien que des informations propres à cette dernière (nom de fichier, de dossier, date et heure de création, de dernière écriture, de dernier accès, etc.).

Ainsi, un fichier bureautique ou un courrier électronique générés par l'utilisateur d'un système informatisé ou encore un fichier généré - automatiquement ou non - par ledit système (fichiers de journalisation d'événements, cookies internet, etc.) sont considérés comme des informations numériques au même titre que les métadonnées qui y sont attachées.

L'information numérique est donc par définition abstraite car immatérielle et volatile ; complexe car variée et qualitative. Elle est également riche car quantitative et évolutive, et vulnérable car modifiable et copiable à l'infini. Enfin, il existe un lien intime avec l'environnement dans lequel elle évolue.

Prenons un exemple concret : le cas d'un salarié démissionnaire qui quitte son entreprise en emportant une copie de la base de données des clients de son employeur.

Pour la détourner, le salarié a pu directement copier le fichier original, ou alors créer un nouveau fichier dans lequel les informations de celui-ci ont été ajoutées. Ensuite, ce fichier a pu être enregistré par le salarié de différentes manières : en utilisant par exemple la messagerie électronique de l'entreprise pour se l'envoyer (envoi en pièce jointe d'un message vers une boîte de messagerie électronique externe voire personnelle), en le gravant sur un support optique (CD, DVD, etc.) ou en le copiant sur un support numérique (clé USB, disque dur externe, etc.). Il faut savoir que peu importe le moyen d'appropriation utilisé, il est souvent possible de retrouver des traces de ces manipulations grâce à des moyens adaptés et une expertise adéquate.

B. QUALIFICATION DE L'INFORMATION NUMÉRIQUE

Avant de conférer la qualification de preuve à une information numérique, il est important de rappeler au préalable les règles générales applicables en la matière.

Ces règles ont pour objet de déterminer la charge de la preuve (qui doit rapporter la preuve), son objet (sur quoi elle doit porter), son mode d'admission (comment elle doit être établie) et sa force probante. Il n'est pas possible de donner une définition unique de la preuve en droit, tout comme il n'existe pas de régime légal unique. Le droit de la preuve est hétérogène. Il s'adapte et varie selon l'objet sur lequel il porte et la matière dans laquelle il intervient.

1. LA QUALIFICATION JURIDIQUE

L'article 1353 du code civil fait supporter la charge de la preuve à celui qui se prévaut d'un fait ou d'un droit. C'est donc au demandeur de prouver ce qu'il revendique. Néanmoins, le défenseur doit également apporter la preuve de ce qu'il invoque dès lors qu'il veut détruire la preuve de son adversaire. Celle-ci est alors soumise au juge qui se retrouve lié par les preuves parfaites qui sont requises pour la preuve des actes juridiques et qui doit apprécier les preuves imparfaites destinées à prouver les faits juridiques.

En droit civil, **le magistrat doit respecter un principe de neutralité**. Il doit apprécier la pertinence et la validité des preuves qui lui sont soumises sans en rechercher d'autres par lui-même. C'est le principe de la procédure dite inquisitoire. A l'inverse, en droit pénal, le juge doit rechercher des preuves et obéir ainsi au principe de la procédure accusatoire.

Le régime de la preuve est mixte en droit civil car il diffère selon qu'elle doit servir à établir l'existence d'un fait ou d'un acte juridique.

Un fait juridique concerne un événement, une action voulue - ou non - qui va produire des effets en droit de façon automatique, sans que ceux-ci n'aient été souhaités par ceux qui vont les subir. Par exemple, la perte de données informatiques par un salarié est un fait juridique. Il s'agit en effet d'un cas dans lequel un acte - volontaire ou non - risque d'exposer le salarié à des conséquences juridiques non recherchées.

A l'inverse, l'acte juridique est une manifestation de la volonté d'une ou plusieurs parties, destinée à produire des conséquences juridiques déterminées.

Par exemple, un contrat informatique est un acte juridique par lequel une société achète un bien ou un service technique auprès d'un prestataire, pour lequel elle s'engage à payer le prix en échange de la livraison du bien ou de la réalisation de la prestation. La vente est voulue et les conséquences juridiques sont clairement connues des parties. Le législateur ne peut donc pas exiger les mêmes conditions en matière d'admissibilité de la preuve selon qu'il s'agit d'un acte ou d'un fait juridique.

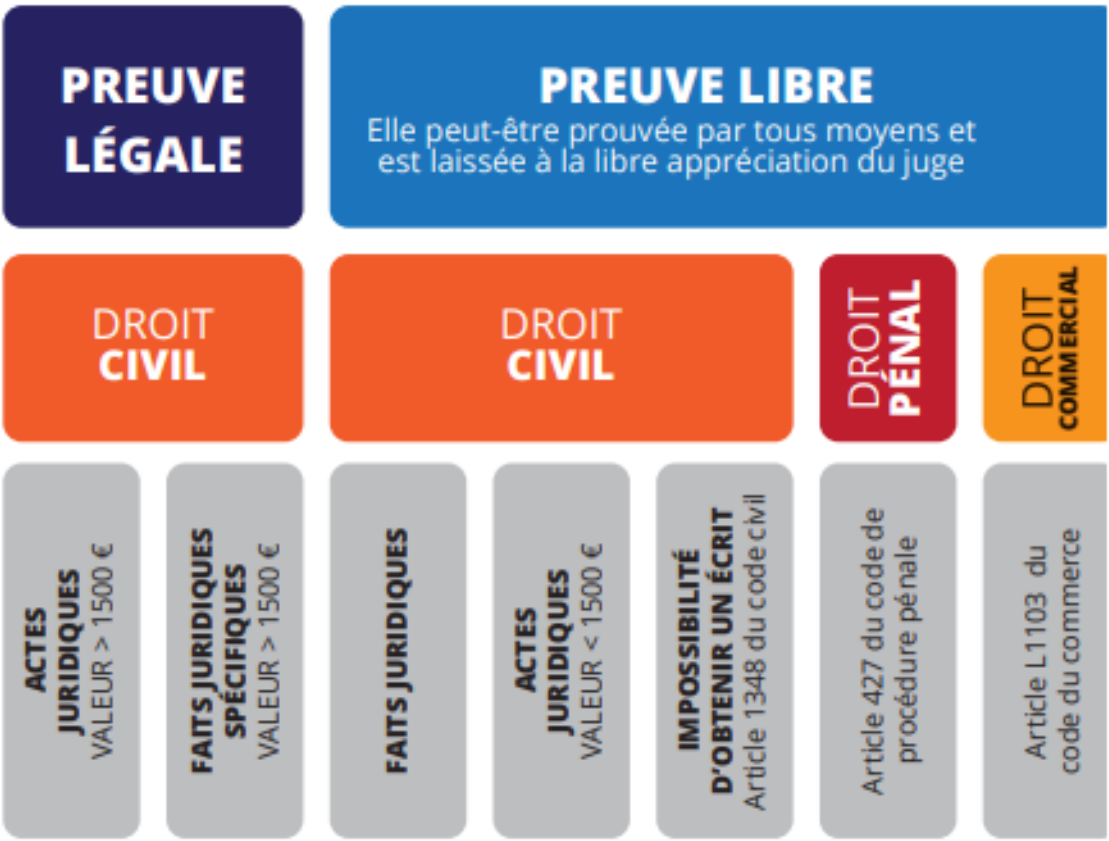
En matière d'actes juridiques, la preuve est dite « légale ». Cela signifie que l'acte doit être prouvé selon des moyens qui ont été préalablement fixés par un texte de loi. Il s'agit le plus souvent d'un écrit, d'un aveu judiciaire ou d'un serment (preuve parfaite). Néanmoins, il existe des exceptions selon le montant du litige ou l'impossibilité d'obtenir un écrit qui assouplissent cette obligation.

En matière de faits juridiques, la preuve est dite « libre » ou « morale ». Cela signifie qu'un fait juridique peut être prouvé par tous les moyens, qu'ils soient parfaits ou imparfaits (témoignage, présomption du fait de l'homme, aveu extrajudiciaire et serment supplétoire). Ainsi, un simple courrier électronique en relation avec les faits litigieux peut être produit à titre de preuve.

Dans notre exemple concernant le salarié indélicat, des courriers électroniques de clients, figurant dans la base de données et qui ont été démarchés pour le compte d'une entreprise concurrente par l'ancien salarié, peuvent être utilisés à titre de preuve.

En droit français, le régime de la preuve doit **respecter certains principes fondamentaux** comme la loyauté et la proportionnalité.

Le principe de loyauté, issu de l'article 9 du code de procédure civile, est une déclinaison du principe de bonne foi. Il s'attache aux conditions et circonstances dans lesquelles la preuve a été collectée. Celles-ci doivent être transparentes ce qui suppose une publicité des moyens de collecte utilisés.



Le régime de la preuve : preuve légale et preuve libre

Par exemple, en droit du travail, les techniques de contrôle et de surveillance des salariés dans les entreprises doivent avoir été préalablement portées à leur connaissance soit directement ou soit par le biais de leurs représentants.
La mise en place d'un système de vidéosurveillance doit donc être signalée aux salariés de manière individuelle, mais également collective au moyen d'un panneau d'affichage visible les informant de l'existence dudit dispositif, du nom de son responsable et de la procédure à suivre pour demander l'accès aux enregistrements visuels les concernant.

Le principe de proportionnalité est quant à lui un corollaire au principe de loyauté. En effet, la collecte de la preuve ne doit pas porter atteinte aux libertés individuelles et/ou collectives.

Ainsi, un dispositif de vidéosurveillance ne doit pas filmer les salariés sur leur poste de travail, sauf exceptions, ou encore filmer les espaces de détente. Les salariés ont en effet droit au respect de leur vie privée même sur leur lieu de travail. Un juste équilibre doit donc être trouvé entre le respect de ces libertés et la légitimité de se constituer une preuve.

Au-delà de la qualification juridique, il est nécessaire de se conformer à des critères techniques précis pour rendre opposable l'information numérique sur le plan probatoire.

2. LA QUALIFICATION TECHNIQUE

Pour être opposable, l'information numérique doit tout d'abord être accessible (exploitabilité) et compréhensible (intelligibilité). Elle doit également répondre à quatre critères techniques : le critère d'authenticité, celui d'intégrité, de traçabilité et le critère de pérennité.

Le critère d'authenticité s'intéresse à l'origine de l'information numérique c'est-à-dire son imputabilité, de qui elle émane. C'est de loin l'un des critères les plus importants mais aussi le plus problématique car il est souvent sujet à discussion. Ainsi, afin de garantir l'authenticité d'une information numérique, il est indispensable de procéder à sa collecte en suivant un « modus operandi » bien établi.

Le critère d'intégrité est également déterminant d'autant plus que l'information numérique peut se dupliquer à l'infini. Il permet de s'assurer que l'information numérique collectée est bien conforme à l'information originale.

Le procédé technique de calcul d'empreintes électroniques (MD5, SHA, etc.) de l'information source et de l'information copiée est un moyen incontestable de respecter ce critère car il permet de démontrer que celle-ci n'a pas pu être altérée au moment de cette opération et que le contenu est resté strictement identique.

Le critère de traçabilité fait référence à la chaîne de traitement de l'information numérique depuis sa création. Celle-ci a pu être créée automatiquement par un système informatique (historique de consultations internet) ou manuellement par un individu (différentes versions d'un fichier bureautique), d'où l'importance des métadonnées.

Lors de sa collecte, ce critère permet également de s'assurer que l'information a été copiée dans les règles de l'art en conservant un historique de toutes les manipulations réalisées : quoi et à qui ? Par qui ? Quand et où ? Avec quoi ? Sur quoi ? D'où l'importance du respect des règles de bonnes pratiques en la matière qui peuvent impacter l'interprétation qui sera faite de l'information a posteriori.

Le critère de pérennité permet de s'assurer que la preuve collectée résistera à l'épreuve du temps et que sa valeur n'en sera donc pas affectée.

On retrouve également dans ce critère les notions d'**exploitabilité** et d'**intelligibilité** de la donnée qui doivent perdurer dans le temps.

La réunion de l'ensemble de ces critères confère à l'information numérique le statut de preuve numérique et conditionne sa validité et sa force probante en résistant à la contestation. En contribuant à obtenir une interprétation fiable de l'information, ces critères facilitent sa qualification juridique.

Dans notre cas d'espèce, le courrier électronique contenant la copie de la base de données de l'entreprise envoyé par le salarié constitue un élément probant des faits qui lui sont reprochés. Ceci est également vrai pour les fichiers de son système informatique qui permettent de démontrer la copie ou la gravure sur un support externe.

Mais comment appréhender ces éléments pour leur donner une valeur juridique ? Que faire, si vous ne disposez pas de données suffisantes pour confirmer de tels agissements ? Comment, dans ces conditions, conférer aux données informatiques collectées une force probante suffisante ?

La mise en place d'une méthodologie adaptée et conforme aux règles de l'art en la matière lors de l'appréhension de ces éléments répond à ces impératifs.

Les critères de qualification

II. LES BONNES PRATIQUES EN MATIÈRE DE PREUVE NUMÉRIQUE

La richesse de l'information numérique collectée est souvent un facteur déterminant dans le processus probatoire. En effet, la copie d'un courrier électronique litigieux, d'une boîte de messagerie électronique contenant ledit message ou du disque dur contenant la boîte de messagerie électronique susvisée dans son environnement informatique n'a pas du tout les mêmes conséquences au niveau probatoire. Cela influe sur la qualité de la preuve collectée d'une part, sur sa force probante d'autre part mais surtout sur sa résistance à la contestation.

Un courrier électronique isolé ne constitue en général qu'un faisceau d'indices voire un commencement de preuve. Seule la richesse des éléments collectés pourra offrir, notamment par son exhaustivité, la possibilité de corréler ce faisceau d'indices avec d'autres éléments numériques.

Plus on dispose de matière à analyser, plus on a de chance d'identifier des éléments concordants probants. Ainsi, le cumul des faisceaux d'indices augmente la véracité de ce que l'on veut prouver. Encore faut-il que la collecte de ces derniers soit réalisée dans de bonnes conditions pour ne pas nuire à leur efficacité.

Les étapes d'identification et de qualification de la problématique sont des préalables indispensables à la mise en place d'une méthodologie probatoire adaptée au cas d'espèce, appliquée par des acteurs spécialisés avec des moyens dédiés.

A. LA COLLECTE DE LA PREUVE

La collecte d'informations numériques peut avoir deux finalités :
- la première se pratique à titre conservatoire c'est-à-dire en absence de toute problématique, en prévention d'une disparition ou d'une érosion de l'information dans le temps et donc de la preuve ;
- la seconde s'effectue lors de la survenance d'un fait dommageable pour lequel il est important de se pré-constituer la preuve.

Techniquement, matérialiser une preuve consiste à enregistrer, selon une procédure particulière, une information numérique sous une forme écartant toute altération possible en lui assurant une durée de vie suffisante pour atteindre la prescription.

1. L'IMPORTANCE D'UNE MÉTHODOLOGIE ADAPTÉE

Dans notre exemple, il se peut que ce soit le service informatique qui ait alerté sa hiérarchie de l'envoi par courrier électronique de la base de données sur une adresse de messagerie externe.

C'est à partir de cette remontée d'informations identifiée via l'interface d'administration du serveur de messagerie par exemple, qu'une méthodologie probatoire doit être déterminée. Pour cela, il est important que les principaux acteurs de l'entreprise : la direction générale, la direction informatique, la direction juridique et la direction des ressources humaines se concertent et déterminent ensemble l'opportunité d'effectuer des investigations complémentaires.

Attention aux données personnelles !

Certaines règles doivent être respectées concernant la collecte et la conservation de données non ciblées qui pourraient contenir des données personnelles des salariés. Il faut rappeler que les « preuves » établies en interne restent acceptables devant un tribunal si elles sont considérées comme fiables.

Même si la jurisprudence, constante en la matière, présume du caractère professionnel des données présentes sur les postes de travail des salariés, il n'en demeure pas moins que ces derniers ont droit au respect de leur vie privée sur leur lieu de travail. Dans certains cas, il peut être alors opportun d'agir sur ordonnance ou en présence du salarié ou celui-ci dûment appelé pour réaliser cette opération.

1A. ÉVITER L'ALTÉRATION DES INFORMATIONS

Ace stade, il est d'usage de vouloir les réaliser soi-même pour asseoir davantage son propos avant de prendre une décision. Or, les services informatiques sont rarement spécialisés en investigation numérique. Ainsi, l'accès à des dossiers ou encore la consultation de fichiers qui peuvent vous paraître anodins sont en fait autant d'actions qui dégraderont la force probante de ces éléments.

Par exemple, la connaissance des métadonnées (nom de fichier, de dossier, date et heure de création, de dernière écriture, de dernier accès, etc.) peut permettre de découvrir des informations importantes. Mais si celles-ci - en particulier de nature temporelle - sont altérées avant constatation, comment démontrer vos affirmations ?

Il est donc déconseillé d'effectuer des recherches directement sur le système suspect sans constatations et dispositifs techniques préalables. Pour éviter cela, il est conseillé d'isoler la machine suspecte en amont de toute procédure. L'opportunité d'enclencher une action avec les éléments déjà identifiés doit donc être mise en balance avec la possibilité de rechercher de nouveaux éléments au risque d'affecter la force probante des premiers. Corréler une information probante avec d'autres éléments se révèle parfois difficile, il est donc important de figer les éléments de la machine sans les altérer à l'aide d'une méthodologie adaptée.

1B. LE NÉCESSAIRE RECOURS À UN TIERS

Il est toutefois possible de procéder à des recherches annexes sur des éléments pour lesquels la force probante est d'ores et déjà discutable. Par exemple, la mise en place d'une politique de sauvegarde informatique en interne permet de réaliser des enregistrements quotidiens, hebdomadaires, mensuels de certaines données importantes : messageries électroniques, partages réseaux, fichiers de journalisation, etc. Or, à titre probatoire, leur utilisation souffre du fait d'une part que l'entreprise a un contrôle total dessus et d'autre part, que la collecte de ces éléments se fait par et pour l'entreprise.

Or, selon le principe « nul ne peut se constituer une preuve à soi-même », toute preuve fiable nécessite l'intervention d'un tiers afin d'attester de la véracité de celle-ci. L'intervention d'un tiers spécialisé lors de la collecte d'informations permet de répondre à cette exigence.

Le recours à un tiers de confiance pour la mise en place, par exemple, d'une politique d'archivage probatoire, respectueuse des exigences du législateur, ayant pour objet la collecte d'informations numériques spécifiques, offre également une chance supplémentaire d'identifier des éléments probants. Au-delà de la méthodologie appliquée pour la recherche et la collecte de ces éléments, la qualité du constatant influe également sur l'efficacité de la preuve.

2. APPLIQUÉE PAR DES ACTEURS SPÉCIALISÉS

L'huissier de justice est un officier ministériel chargé de constater des faits et de les consigner dans un procès-verbal de constat qui fait foi.

Or, l'huissier de justice n'est pas un technicien. C'est la raison pour laquelle il est indispensable, dans ce type d'opération, qu'il soit accompagné d'un homme de l'art (sachant) indépendant du requérant et habitué à ce type d'intervention (technicien d'un cabinet d'expertise, expert judiciaire).

Celui-ci a alors pour principale mission d'assister l'huissier dans ses constatations en l'éclairant sur les points techniques qui échappent à sa compétence. A cet effet, il doit avoir connaissance de l'architecture informatique de l'entreprise mais également des procédés de protection en place (cryptologie par exemple).

Ainsi, l'intervention d'un huissier va permettre de consigner le ou les faits reprochés et de matérialiser les opérations techniques réalisées pour identifier les éléments informatiques qui y sont liés. Un historique, de l'identification de ces éléments à leur mise sous scellés, sera dressé.

L'huissier va tout d'abord relater la problématique telle qu'exposée par le requérant avant de consigner le matériel sur lequel les opérations seront réalisées (notamment marque et modèle de la machine, utilisateur de la machine, qualité de l'utilisateur, etc.). Assisté de l'expert, il pourra illustrer ses constatations par le biais de captures d'écran des éléments litigieux avec mise en avant de certaines informations importantes (principalement des dates et des chemins d'accès) avant de procéder à la copie papier et/ou électronique sur support(s) optique(s) ou numérique(s) de ces derniers.

Il est préférable d'utiliser pour les copies des supports optiques non réinscriptibles de type WORM (CD, DVD, etc.) car les informations collectées sont définitivement figées après gravure ce qui n'est pas le cas sur des supports numériques de type USB (clé, disque dur). Cela a notamment son importance dans les affaires où les dates et plus largement les métadonnées sont en cause. Cette procédure permet donc de mettre en avant la provenance des éléments en répondant au critère d'authenticité posé par le législateur mais aussi au critère sous-jacent de traçabilité.

Dans notre exemple précédent, si le courrier électronique se situe toujours dans les éléments envoyés de la boîte de messagerie électronique professionnelle du salarié, il est en effet difficile de contester l'envoi de ce message surtout lorsque l'expéditeur est clairement identifié (compte individualisé et sécurisé) et que le destinataire est externe à l'entreprise.

Ce message peut également être mis en relation avec d'autres informations notamment des fichiers de journalisation du serveur de messagerie. Ceci est également vrai lors de l'identification d'un fichier se retrouvant dans la session utilisateur d'un salarié alors que celui-ci n'a théoriquement pas accès à cette information, en l'espèce la base de données.

En cas de doute sur le caractère probant d'une information numérique, il est nécessaire de procéder à des recoupements d'indices en provenance d'autres supports d'informations pour corroborer vos allégations. Dans cette hypothèse, il est tout aussi important de faire constater ces indices connexes par huissier.

3. AVEC DES MOYENS DÉDIÉS

Au cours des constatations, il est possible de mettre en œuvre différents modes de copie pour constater et conserver les éléments informatiques litigieux. En effet, il faut distinguer **la copie simple dite « logique » de la copie-image dite « physique ».** La première permet de figer uniquement le ou les informations numériques intéressantes indépendamment de leur environnement informatique. Par exemple, un courrier électronique, le contenu d'un dossier ou un fichier bureautique. La seconde permet de réaliser une copie de l'intégralité du contenu d'un support, il s'agit d'**une copie « bit-à-bit ».**

Afin de se réserver la possibilité d'effectuer des recherches complémentaires par le biais d'une expertise inforensique, il est vivement recommandé avant toute constatation de faire procéder, en présence d'un huissier et par un tiers sachant, à une copie-image du disque dur de la machine suspecte (source) sur un disque dur vierge et neuf (destination). Cette copie-image peut être réalisée de deux manières : soit en utilisant un logiciel de copie spécialisé (FTK Imager, Encase Forensic, etc.), soit en utilisant un matériel de duplication dédié (Logicube, Tableau, etc.).

Cette dernière solution dispose d'un avantage indéniable : elle ne nécessite pas que l'ordinateur soit allumé pour procéder à cette opération car le disque dur est extrait physiquement de la machine. Attention toutefois au matériel de duplication utilisé, il ne s'agit pas de copieurs standards comme ceux destinés à faire de la copie de sauvegarde. Il s'agit en effet de dispositifs dit « forensic » équipés d'un bloqueur en écriture garantissant l'intégrité du support original et de sa copie. Ainsi, les éléments copiés sont figés à la date de dernière extinction du système d'exploitation. Aucune altération du contenu des deux supports n'est donc possible au moment de la copie, le bloqueur en écriture étant chargé d'assurer un confinement parfait des informations lors de cette opération. **La copie ainsi réalisée est dite « parfaite ».**

Autre avantage de ce type de procédé, certains matériels permettent de calculer des empreintes numériques individuelles ou collectives du contenu des supports (source et destination) avant, pendant et après la copie. Si les empreintes obtenues entre la source et la destination sont identiques, cela signifie que les données présentes sur chaque support sont identiques et que leur contenu n'a pas été altéré au cours de cette opération. **La copie est alors dite « pure et parfaite »**.

Le critère d'intégrité de l'information collectée est donc pleinement respecté grâce à ces dispositifs techniques. Il est important de consigner dans le procès-verbal de l'huissier, les éléments d'identification des disques durs (source et destination), les caractéristiques du matériel utilisé, les options configurées pour réaliser cette opération ainsi que le nombre de copies effectuées.

D'un point de vue technique, il est recommandé de copier en double exemplaire le support source. Celui-ci sera alors mis sous scellés par l'huissier de justice et conservé soit à son étude, soit par le requérant de préférence dans un coffre-fort. La première copie pourra alors être replacée dans la machine pour procéder aux constatations et la seconde copie remise à un technicien aux fins d'analyse ou conservée par l'huissier jusqu'à nouvel ordre. Ce mode opératoire a pour principal intérêt d'isoler totalement le support original de la recherche de la preuve. Celui-ci pourra alors servir de base, en cas de contestation, pour une expertise diligentée au fond par un magistrat.

Il est également possible de mettre sous scellés une copie du support original car le critère d'intégrité est assuré par le mode de copie utilisé ; les constatations pouvant être réalisées directement sur le disque dur original après copie. Il est d'ailleurs tout à fait envisageable de ne procéder qu'à une seule copie du disque dur suspect. Le but premier des copies multiples est de garantir que la preuve originelle ne puisse être altérée de quelque manière que ce soit.

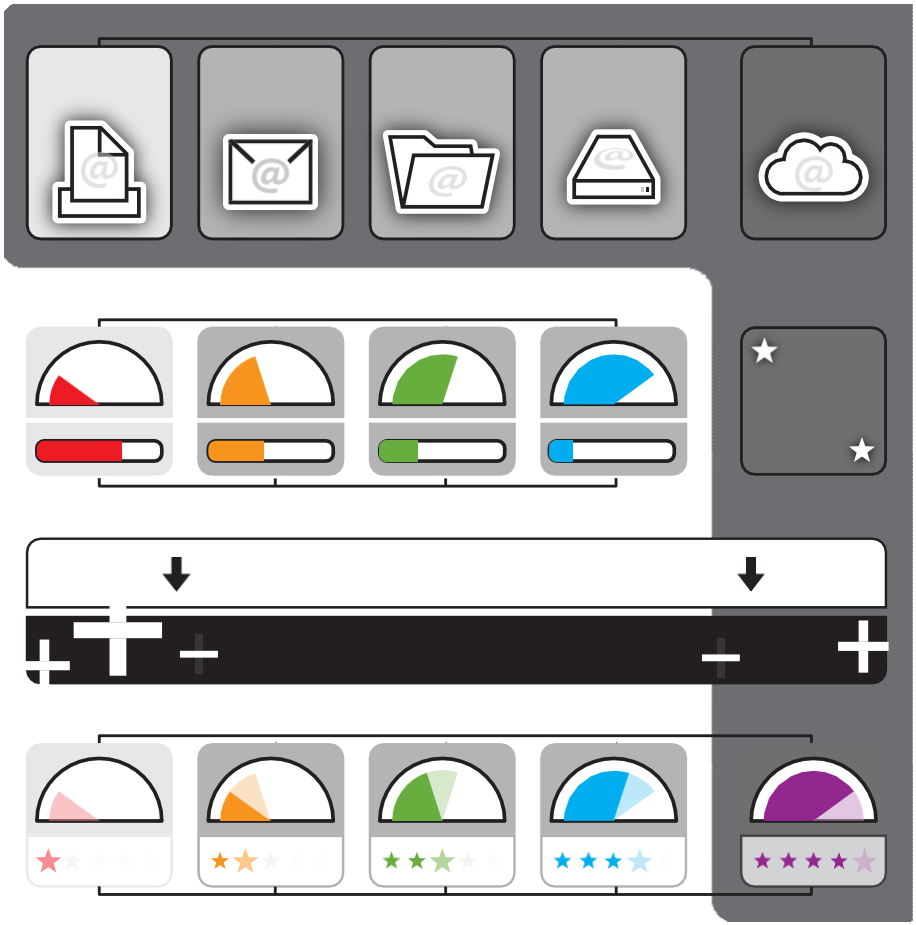
Cette méthodologie probatoire à deux niveaux est applicable à tout type de problématique et doit juste être adaptée au cas d'espèce et au(x) support(s) d'informations concerné(s) (smartphones, tablettes numériques, etc.).

Elle s'applique effectivement à notre exemple. Après concertation, la constatation des éléments déclencheurs - ceux identifiés par le service informatique via l'interface d'administration de la messagerie électronique - et la recherche de ces mêmes éléments dans la messagerie électronique du poste de travail du salarié peuvent être suffisants.

Les éléments générateurs de cette procédure sont donc constatés en amont, tout comme les éventuelles traces des agissements du salarié sont figées en aval. Toutefois, si cette solution est retenue, seuls les éléments consignés dans le procès-verbal de l'huissier auront une force probante suffisante pour résister à la contestation ; la fiabilité des autres informations numériques pourra être remise en cause. Si vous optez pour une copie-image préalablement aux opérations de constat, les éléments ainsi figés pourront être exploités dans un second temps lors d'une expertise indépendante ou judiciaire.

Pour reprendre notre exemple, n'oubliez pas que ce message n'est peut-être que la face visible de l'iceberg. Il est éventuellement possible d'identifier des traces d'autres agissements litigieux.

La richesse des informations collectées - de la machine suspecte mais également en provenance d'autres supports d'informations (logs de serveurs par exemple) - peut donc être déterminante dans la qualification juridique des faits reprochés. Enfin, les moyens de recherche de la preuve dans l'environnement numérique doivent toujours être proportionnés aux enjeux poursuivis.



Intérêt de la copie probatoire

B. LA CONSERVATION DE LA PREUVE

Les éléments constatés doivent être appréhendés et conservés de manière à pouvoir être ultérieurement présentés au magistrat.

Au-delà de sa qualification et de sa collecte, l'information numérique doit également répondre aux contraintes et exigences posées en matière d'archivage probatoire. On retrouve ainsi les critères précédemment abordés à savoir : l'authenticité, l'intégrité, la traçabilité et la pérennité. Les données collectées doivent être intelligibles et exploitables c'est-à-dire que le contenu doit rester lisible et compréhensible.

Par exemple, les éléments chiffrés ne répondent pas totalement à ces impératifs car leur consultation est subordonnée à l'utilisation de procédés techniques spécifiques. Ceci a son importance notamment en matière de copie-image car l'exploitabilité des données copiées est directement liée à celle des données originales. Sans information technique préalable, il sera alors difficile, voire impossible de les utiliser.

Cela est également vrai pour les formats de fichiers dits « exotiques ». Un format générique permet d'assurer davantage l'intelligibilité et l'exploitabilité des informations copiées dans le temps. Il s'agit donc d'une limite technique, propre aux données informatiques, à laquelle il est difficile de pallier eu égard aux conditions dans lesquelles elles sont collectées.

L'imputabilité et la traçabilité de l'information numérique sont ainsi assurées par le procès-verbal de constat dressé par l'huissier de justice. Le juge peut ainsi prendre connaissance de toutes les opérations réalisées sur et à partir de ce support depuis sa création. L'intégrité est garantie par le scellé apposé par l'huissier sur ledit support et par les modalités de conservation (coffre-fort, armoire sécurisée, etc.). Sur certains supports optiques, l'intégrité est double car par nature ils interdisent toute modification post gravure.

Les informations ainsi conservées sont donc à l'abri de la destruction, de toute modification ou altération que ce soit de manière intentionnelle ou accidentelle. Au-delà de la contrainte liée aux formats des données, le critère de pérennité est quant à lui fonction du support utilisé pour les conserver.

La durée de vie des supports numériques est en moyenne comprise entre 5 et 10 ans suivant le type et la qualité des médias utilisés. Il s'agit donc d'une période au cours de laquelle l'intelligibilité et l'intégrité des données enregistrées sont censées être garanties.

Il est difficile de se prononcer sur la durée de vie réelle de ces supports car celle-ci dépend des conditions dans lesquelles ils sont conservés.

Il est évident qu'un support optique aura une durée de vie plus longue s'il est rangé dans son boîtier à l'abri de l'humidité, de la lumière et de la poussière que s'il est laissé sans protection sur une étagère.

Ainsi, la multiplication des types de supports de stockage utilisés et du nombre de copies réalisées peut permettre de ralentir l'érosion de la preuve dans le temps.

C. LA MISE EN PLACE D'UNE POLITIQUE PRÉVENTIVE

Les principales faiblesses de l'information numérique restent sa volatilité, sa capacité de reproduction infinie, et sa facilité de falsification. Ces caractéristiques, la multiplication des risques d'atteinte au patrimoine immatériel des organisations, le respect des grands principes énoncés supra permettent de tracer à grand trait les lignes d'une politique préventive.

Si la pré constitution de preuve en matière de droits de propriété intellectuelle est une évidence pour la plupart des organisations, les autres données constitutives du patrimoine informationnel de l'entreprise sont généralement peu ou mal protégées.

En amont, il est souvent nécessaire d'identifier dans la masse des données, celles qui pourront constituer un enjeu probatoire futur : messagerie des personnels sensibles, fichiers journaux des systèmes clés, base de données, etc.

D'une manière générale, le dépôt préventif de données sensibles auprès de tiers de confiance et/ou la mise en place de politiques techniques dédiées comme le « Log Protection » contribuent efficacement à l'établissement et à la conservation des preuves électroniques dans le temps.

Le principal intérêt de ces dernières réside dans la possibilité d'identifier des éléments informatiques probants susceptibles de corroborer d'autres éléments et donc de confirmer vos allégations. En aval, l'encadrement lors de la découverte d'un fait dommageable est un moment déterminant pour la protection de vos droits.

Ainsi, **la méthodologie précédemment détaillée qui fait appel à la copie probatoire s'inscrit dans cette logique de « bonnes pratiques » et reste un moyen simple, fiable et rapide de collecter et de conserver des données suspectes**.

Elle permet en outre, par le biais d'une expertise technique, de confirmer les premières constatations réalisées en offrant l'opportunité de découvrir de nouveaux faisceaux d'indices, voire de nouvelles preuves.

LA PREUVE DANS L'ENVIRONNEMENT NUMERIQUE

Ce cahier technique par
le Centre d'Expertise CELOG
sous la direction de :

Raphaël d'Assignies
Directeur du CELOG

Alexandre Drevet,
Responsable du pôle expertises de CELOG

Retrouvez ce cahier technique et bien plus d'informations sur ***celog.fr***

CELOG - T. +33(0)143596061 / F. +33(0)143596064 54 rue de Paradis 75010 PARIS - SIREN : 308950260

LES CAHIERS TECHNIQUES DE **CELOG**

CELOG

LA PREUVE DANS L'ENVIRONNEMENT
NUMERIQUE