

L'historique d'un fichier Word peut-il prouver la falsification d'un document RH ?

Réponse courte

Oui, et c'est même l'un des moyens les plus efficaces pour contester une pièce numérique. Les fichiers bureautiques conservent des données que leur auteur n'a pas toujours conscience de transmettre : date de création, date de dernière modification, identité du dernier utilisateur, parfois l'historique des révisions et les commentaires supprimés.

Ces éléments ne prouvent pas une intention frauduleuse, mais ils établissent des **faits vérifiables** : un document daté du 3 mars dont le fichier a été créé le 12 septembre, un rapport « rédigé le jour des faits » modifié la veille de l'audience. Le décalage suffit à ruiner la pièce, et le soupçon s'étend aux autres productions de la même partie.

Tout suppose de disposer du **fichier natif**. Une impression, une capture d'écran ou un PDF régénéré ne portent aucune métadonnée : c'est pourquoi il faut réclamer le fichier d'origine plutôt que la version que l'adversaire a choisi de produire.

Définition

Les **métadonnées** sont les informations techniques accompagnant un fichier sans figurer dans son contenu visible : dates, auteur, application, durée d'édition.

Le **suivi des modifications** est une fonction distincte, qui conserve les versions successives d'un texte. Lorsqu'il est activé, il restitue l'évolution du document et parfois des passages supprimés.

Questions fréquentes

Les métadonnées d'un fichier bureautique peuvent-elles révéler une manipulation ?

Oui, et c'est l'un des moyens les plus efficaces de contester une pièce numérique. Ces fichiers conservent la date de création, la date de dernière modification et l'identité du dernier utilisateur.

Pourquoi faut-il réclamer le fichier natif plutôt qu'une impression ?

Parce qu'une impression, une capture d'écran ou un PDF régénéré ne portent aucune métadonnée. Seul le fichier d'origine permet la vérification.

Que démontrent exactement les métadonnées d'un document ?

Des faits vérifiables, non une intention frauduleuse : un document daté du 3 mars dont le fichier a été créé le 12 septembre, ou un rapport modifié la veille de l'audience.

Quelle conséquence un décalage de dates a-t-il sur le reste du dossier ?

Il ruine la pièce concernée et étend le soupçon aux autres productions de la même partie.

Quelles autres traces un fichier de traitement de texte peut-il conserver ?

L'historique des révisions et les commentaires supprimés, que leur auteur n'a pas toujours conscience de transmettre.

Conditions d'exercice

Les métadonnées établissent des faits ; leur interprétation reste soumise au débat.

Élément	Portée
Date de création et de modification	Fait vérifiable, opposable à la date affichée sur le document
Identité du dernier utilisateur	Indice sur l'auteur réel de la dernière intervention
Historique des révisions	Restitue l'évolution du texte lorsque le suivi était activé
Fichier natif	Indispensable : impression et capture ne portent aucune métadonnée
Métadonnées modifiables	Elles peuvent être altérées ; leur cohérence d'ensemble reste révélatrice
Expertise	Le juge peut l'ordonner lorsque le doute technique persiste
Falsification caractérisée	Peut relever du faux et de l'usage de faux

Modalités pratiques

La démonstration se construit en réclamant le fichier, non en discutant l'impression produite.

Étape	Détail
Demande du fichier natif	Réclamer le document d'origine avec ses métadonnées, non un extrait imprimé
Lecture des propriétés	Comparer date de création, date de modification et date affichée
Cohérence externe	Confronter aux autres pièces : courriels, plannings, virements
Suivi des modifications	Vérifier si des révisions ou commentaires subsistent dans le fichier
Conservation en l'état	Ne pas ouvrir ni enregistrer le fichier reçu : cela modifierait ses métadonnées
Copie de travail	Travailler sur une copie, en conservant l'original intact
Expertise	La solliciter si le doute persiste après ces vérifications

Pratiques et recommandations

Ouvrir le fichier suffit parfois à le dégrader. Certaines applications actualisent la date de dernière modification à la simple ouverture, voire au seul enregistrement automatique. Conservez le fichier reçu tel quel et travaillez sur une copie : cette précaution évite de détruire l'élément que vous cherchez à exploiter.

Le raisonnement vaut dans les deux sens. Un employeur qui produit un rapport interne s'expose à ce que ses métadonnées révèlent une rédaction tardive ; c'est une raison supplémentaire de consigner les faits au moment où ils surviennent, plutôt que de reconstituer un dossier après la notification.

Les commentaires supprimés réservent des surprises. Un document ayant circulé entre plusieurs responsables conserve parfois des annotations effacées de la version visible mais présentes dans le fichier — et leur contenu, souvent plus direct que le texte final, se révèle décisif.

Cadre juridique

Référence	Objet
Art. 1315 du Code civil	Charge de la preuve pesant sur celui qui réclame l'exécution de l'obligation
Art. 1322-1 du Code civil	Signature électronique : garantie d'intégrité et identification du signataire
Art. 1322 du Code civil	Force probante de l'acte sous seing privé entre ceux qui l'ont souscrit
Art. <u>L.124-11</u>, paragraphe (3)	Charge de la matérialité et du caractère réel et sérieux des motifs pesant sur l'employeur
Loi du 25 juillet 2015	Copie certifiée par un PSDC présumée conforme à l'original
Code pénal	Faux en écritures et usage de faux : altération frauduleuse de la vérité

Les métadonnées d'un fichier établissent des faits vérifiables — dates réelles de création et de modification — qui peuvent contredire la date affichée. Réclamez le fichier natif et ne l'ouvrez pas directement : certaines applications actualisent ces données à la simple ouverture.

Les contenus sont rédigés et mis à jour régulièrement à partir de sources officielles. Leur usage ne remplace pas une consultation juridique et doit être validé par un professionnel du droit.