

DÉCRYPTAGE
La signature
électronique
est-elle
fiable ? P. 24

JO 2024
Quel
vidéoprojecteur
pour regarder les
jeux en grand P. 22

UN MAGAZINE
**FABRIQUÉ
EN FRANCE**
RÉDACTION
IMPRESSION
PAPIER

SÉCURISEZ VOTRE MAISON

P. 36



LES
**MEILLEURES
CAMÉRAS**
INTÉRIEURES
ET EXTÉRIEURES

NOTRE COMPARATIF
DES SOCIÉTÉS DE
TÉLÉSURVEILLANCE

LES KITS
D'ALARME
CONNECTÉE
À LA LOUPE

EN PRATIQUE
**APPRENEZ
À PARLER À
CHATGPT, GEMINI
ET MISTRAL AI**

P. 58

INTERVIEW Le coup de gueule
de **GILBERT MONTAGNÉ** contre
le manque d'accessibilité numérique P. 8

BANC
D'ESSAI **13 smartphones PREMIUM**
à moins de 700 euros P. 44

BEUX : 5,10 € - CH : 8,95 € - CAN : 8,99 \$ - MAR : 54 Dh - TUN : 8,9 Tnd - DOM : 5,7 €

L 13262 - 1022 S - F : 4,50 € - RD



CPPAP

DÉCRYPTAGE SIGNATURE ÉLECTRONIQUE QUE VAUT-ELLE VRAIMENT ?

De la tablette du livreur Colissimo ou UPS au contrat chez le notaire, c'est le genre d'outils que l'on utilise sans s'interroger, comme un passage obligé. Or toutes les signatures électroniques ne se valent pas, loin de là, tant sur le plan technologique que juridique.

Comme pour beaucoup d'outils juridiques, c'est quand les choses ne se passent pas comme prévu que l'on en saisit l'importance. La signature électronique est de ceux-là. Cependant, elle est très normée. Par le Code civil, par le règlement européen eIDAS... Et, pour sa mise en œuvre, elle est placée sous le haut patronage de l'Agence nationale de sécurité des systèmes informatiques (ANSSI). Attention cependant, il ne faut pas confondre la signature électronique avec la simple numérisation ou photographie d'une signature manuscrite transformée en image pour être copiée-collée sur des documents. La griffe ainsi numérisée s'avère être, en l'absence de tout contrôle ou même passage par un tiers, aisément falsifiable. Rien à voir avec la signature en per-

sonne, ou en « présentiel » comme l'on dit maintenant, dont la valeur juridique est établie depuis fort longtemps. C'est cette graphie originale que la signature électronique tente technologiquement de reproduire. « Lorsque vous dessinez votre signature sur un document, vous tracez quelque chose qui vous est propre, en usant de gestes dont les graphologues vont dire qu'ils sont uniques », explique François Devoret, fondateur de Lex Persona, un éditeur de logiciel basé à Saint-André-les-Vergers, dans l'Aube, spécialisé dans la signature électronique. « Les gouttelettes d'encre qui s'imbibent dans le papier créent un lien indissociable entre cette griffe personnelle et le document, ajoute l'expert. Les ingénieurs ont réfléchi à comment traduire ce processus de manière informatique. Pour ça, ils s'appuient sur les mathématiques, notamment les fonctions irréversibles et la décomposition des produits de très grands nombres

premiers. » Notre interlocuteur, usant de la métaphore du passager aérien qui n'a pas besoin de savoir piloter pour prendre l'avion, ne veut toutefois pas nous perdre dans « des questions de fonctions de hachage, d'empreinte, de chiffrements ». Pour autant, il semble légitime d'avoir une idée, sans là encore tout comprendre dans les moindres détails techniques, de la manière dont la sécurité et la fiabilité sont assurées. Ce qui vaut, convenons-en, tant pour l'avion que pour la signature numérique.

Des données chiffrées par des algorithmes

Pour assurer cette confiance entre les signataires d'un document juridique, contrat synallagmatique (vente ou bail, par exemple) ou acte légal réglementé, il faut respecter deux impératifs. Ainsi, Alban Sayag, PDG de la société Yousign, l'un des leaders du secteur, basée à

Caen, précise que cette « signature à valeur probante possède deux fonctions : elle doit garantir, d'une part, l'intégrité des données, et, d'autre part, l'identité des signataires ». Reprenons dans l'ordre. Pour le premier objectif, le processus technique mis en œuvre doit empêcher que les données soient hackées. Il serait en effet plus qu'embêtant que le prix d'achat (ou de vente) d'un appartement ou de tout autre bien soit modifié. « Cela nécessite l'utilisation d'algorithmes pour chiffrer les documents et éviter qu'ils ne soient modifiés pendant le processus de création de la signature », clarifie un expert de Yousign. Ici, c'est donc l'objet technique qui, intrinsèquement, produit sa propre vertu sécuritaire. Par analogie, on pourrait oser la comparaison avec les calculs des antiques Sumériens. ...



François Devoret
Fondateur et président
de Lex Persona

“Le plus grand défi de la signature électronique, c'est son interopérabilité.”

Aujourd'hui, tout le monde bricole des tas de trucs souvent non conformes aux bonnes pratiques, aux bons standards.”

67%
des décideurs recourent
à la signature électronique.

Mais aussi...

57%
des TPE

89%
des PME

83%
des ETI et GE

Source : Les Persona Yousign





Alban Sayag
Président
de Yousign

“L'identité numérique européenne aura un impact important non pas sur la vérification de l'intégrité des données, mais sur la vérification d'identité qui sera rendue beaucoup plus simple.”

■ ■ ■ Pour assurer la sécurité des transactions commerciales, ces jetons en argile enserrés dans des enveloppes-bulles aussi en argile désignaient et quantifiaient la marchandise, avant la naissance de l'écriture. À l'arrivée, l'acheteur vérifiait que l'inscription gravée sur l'argile correspondait bien au contenu. Et qu'aucun déstasage n'avait été opéré en route. C'est presque pareil ici. Avec l'utilisation d'empreintes numériques, la plus infime modification d'un document numérique doit se voir immédiatement.

Différents niveaux de contrôle d'identité

La vérification de l'identité, puisqu'un contrat est conclu entre des parties qui doivent y consentir, est tout aussi primordiale. Mais pour des raisons d'efficacité, le niveau de contrôle le plus haut (voir tableau ci-contre) n'est pas toujours requis. Ici, c'est la propension de l'acte à être contesté, ainsi que le niveau d'engagement qu'il implique, qui sont les maîtres-mots. On ne signera pas avec les mêmes exigences formelles l'achat d'un bien immobilier

et l'adhésion à des conditions générales d'utilisation d'un service de streaming qu'on ne lit généralement pas. « Il existe des contrôles d'identité plus ou moins forts, selon la criticité du document, qui découlent de normes réglementaires, résume Alban Sayag. Pour un acte notarial, on parle de signature électronique qualifiée. Il faut scanner la pièce du signataire et la faire correspondre avec un contrôle physique, c'est-à-dire voir la personne et vérifier qu'il s'agit bien de sa pièce d'identité. Mais il y a des niveaux de contrôle plus bas. Pour une signature dite « avancée », on scanne juste la pièce d'identité et on s'assure que le nom correspond bien. Et pour une signature « simple », on se contente d'envoyer un code par mail ou par SMS, que le signataire doit rentrer avant de pouvoir signer. » L'ANSSI met à disposition du public un guide très bien fait qui détaille les différentes variantes des signatures électroniques simples, avancées ou qualifiées (bit.ly/3Q2vTaT). La reconnaissance d'empreinte digitale ou faciale de nos smartphones sécurise bien sûr un peu plus la signature électronique, notamment dans sa variante « simple ». Et elle est donc logiquement, pour des raisons de coût et de praticité, la plus répandue. Pour les niveaux les plus élevés, Alban Sayag ajoute que « si l'intelligence artificielle est mise à contribution à des fins de vérification de pièce d'identité, il n'est pas possible d'automatiser tout le processus. Il y a une obligation réglementaire de faire participer les humains au contrôle ».

63%

des dirigeants privilégient les solutions françaises.

Sources : Lex Persona / YouSign

LES SIGNATURES NUMÉRIQUES		LES TROIS NIVEAUX DE SIGNATURE ÉLECTRONIQUE		
	SCAN DE SIGNATURE MANUSCRITE	SIMPLE	AVANCÉE	QUALIFIÉE
Valeur juridique en cas de contestation	TRÈS FAIBLE Sans intervention d'un tiers de confiance, ce copier-coller est aisément falsifiable.	MOYENNE	MOYENNE À ÉLEVÉE Association optionnelle d'un certificat qualifié de signature numérique	TRÈS ÉLEVÉE Certification par un tiers de confiance approuvé par l'ANSSI
Conditions réglementaires à respecter (eIDAS)	Aucune	Pas d'exigence légale établie mais utilisation, en général, de la double authentification (mail + code OTP) + Dossier de preuve (intégrité des données, horodatage) + Identité déclarative	Double authentification (mail + code OTP) + Dossier de preuve (intégrité des données, horodatage) + Émission d'un certificat numérique qualifié associé au signataire (optionnel) + Vérification simple de la pièce d'identité	Double authentification (mail + code OTP) + Dossier de preuve (intégrité des données, horodatage) + Émission d'un certificat numérique qualifié associé au signataire + Vérification de l'identité du signataire en présence + Clé cryptographique
Charge de la preuve en cas de contestation	Indéfini, la signature numérisée n'entre dans aucun cadre légal	Repose sur le professionnel qui propose la signature à ses clients	Repose sur le professionnel qui propose la signature à ses clients	Incombe à celui qui conteste sa validité, car elle est présumée fiable
Nature des documents concernés	Tout type de document non contractuel	Document ou contrat de la vie courante présentant des facteurs de risques limités	Contrat impliquant des transactions financières importantes ou document juridique	Document, contrat à fort risque ou acte juridique exigeant le plus haut niveau formel
Exemples	Courrier, plaquette, brochure...	Adhésion à des CGU/CGV Contrat de bail et de travail Mandat de prélèvement SEPA Contrat d'assurance de complémentaire santé État des lieux d'entrée ou de sortie d'un logement...	Assurance vie Contrat de crédit Contrat de prévoyance Compromis de vente immobilière Facture électronique à destination des services fiscaux...	Acte authentique Acte d'avocat Acte produisant des effets hors de la France et dans l'UE (produits financiers européens, opérations bancaires intra UE...) Passation de marché public...

Source : ANSSI (2020)

Toujours dans cet esprit de paranoïa réglementée, on peut aussi se poser la question du stockage des données, par définition personnelles puisque l'identification des signataires implique le recueil d'informations sensibles. Là encore, des obligations drastiques s'imposent aux prestataires de services. Nos deux interlocuteurs, Lex Persona et Yousign, opèrent eux-mêmes leurs serveurs. « On a poussé la notion de souveraineté très loin, affirme François Devoret, puisque nos serveurs ne sont pas seulement basés dans des data centers en France. Nous sommes propriétaires de toute notre infrastructure : switches (commutateurs, NDRL), firewalls (pare-feu), disques archivage. Toute la chaîne, y compris l'envoi des codes que vous

recevez par SMS ou par mail, met à contribution des prestataires de nationalité française et qui opèrent en France. » Lex Persona pousse l'intégration de ses solutions d'autant plus loin que les données de certains de ses clients – « qui ont de gros centres informatiques internes », indique François Devoret, comme le centre national de la recherche scientifique (CNRS) ou les centres hospitaliers universitaires – sont stockées sur des serveurs maison. « Cela leur permet d'être totalement en maîtrise de leur système d'information, explique-t-il. Lorsqu'un collaborateur du CNRS signe, il signe sur la plateforme de signature du CNRS et non sur la plateforme de Lex Persona. » À l'avenir, parions que la signature électronique tendra à être à la fois de mieux en mieux intégrée, donc plus transparente, tout en fournissant un niveau de sécurité toujours plus élevé. L'émergence d'une « identité numérique » d'État ou établie au niveau européen (bit.ly/446CDdL) devrait aussi rebattre les cartes, ouvrant de nouvelles possibilités et posant d'autres problèmes techniques. ● David Namias

(1) Code One Time Password, soit un mot de passe à usage unique.
(2) La signature électronique n'est pas reconnue en France pour les actes relatifs au droit de la famille ou aux successions.

PAS À PAS EXPRESS

SIGNER UN PDF SUR SON TÉLÉPHONE AVEC FILL & SIGN

Pour des signatures sans exigence juridique particulière, Adobe Fill & Sign (Remplissage et Signature) fait parfaitement l'affaire.

01. REMPLISSEZ VOTRE FORMULAIRE
Téléchargez l'application depuis le Play Store (bit.ly/3Qh21JL) ou l'App Store (apple.co/49J426A), connectez-vous via Facebook, Google ou votre adresse mail, puis importez le document concerné.

02. CRÉEZ SIGNATURE ET PARAPHE
Ouvrez votre document puis entrez dans le menu Plume. Lors de la création d'une signature, le smartphone passe en affichage horizontal pour vous laisser plus de place et bien tracer votre griffe.

03. INSÉREZ VOTRE GRIFFE
Pour apposer votre signature (ou paraphe), retournez dans le menu Plume et sélectionnez-la. Vous pouvez la déplacer où bon vous semble sur la page et en changer la taille grâce aux flèches à droite du cadre.

