archimag
[STRATÉGIES & RESSOURCES DE LA MÉMOIRE & DU SAVOIR]

PAYS : France
PAGE(S) :30-31
SURFACE :141 %
PERIODICITE : Mensuel

DIFFUSION :(8000)
JOURNALISTE : Christophe Dutheil

► **1 juillet 2022 - N°356**

sécuriser et renforcer la confiance

Plusieurs experts sont revenus sur les questions de validation et de sécurisation des échanges et des identités numériques lors d'un séminaire *Archimag* d'une journée, le 10 mai 2022. Tour d'horizon des évolutions en cours et des enjeux à relever.

Les êtres humains ont besoin de confiance : « *Sans la confiance des hommes les uns envers les autres, la société tout entière se disloquerait* », écrivait le sociologue Georg Simmel dès 1900. Mais celle-ci est « *une denrée en voie de disparition* », estimait récemment une journaliste du *Monde*, citant entre autres la perte de confiance des Français dans leurs élus, leur système judiciaire, voire leurs concitoyens... La confiance s'est en outre particulièrement étiolée sur le Web, sous l'effet d'une multiplication des usurpations d'identité et des actes de piratage.

garantie d'authenticité

« *Les sites doivent mettre en place un climat de confiance pour que les consommateurs puissent échanger et consommer* », observe Pascal Daisnée, président de Certilane (application permettant d'établir une relation de confiance entre les consommateurs et les acteurs du Web). Il souligne les questions qui se posent actuellement pour les internautes : « *Comment être sûr d'être au bon endroit ? Comment savoir s'il s'agit bel et bien du site d'un revendeur officiel ? Est-il risqué de laisser des données sur ce site ?...* ». L'application de cet éditeur, disponible en téléchargement gratuit, indique aux utilisateurs s'ils sont au bon endroit, c'est-à-dire sur un site reconnu comme un site de confiance par la marque. « *Les entreprises peuvent labelliser très rapidement leurs réseaux de revendeurs officiels et lutter contre la vente de leurs produits — éventuellement contrefaits — par des tiers non autorisés* ».

mise en conformité

« *La conformité (compliance, en anglais) est le corollaire de ce besoin de confiance* », souligne l'avocat Sylvain Staub, PDG de Data Legal Drive, une plateforme de mise en conformité vis-à-vis du RGPD ou des lois anticorruption. « *L'État ne peut pas aujourd'hui contrôler l'ensemble des problématiques* », relève ce spécialiste. « *La notion de compliance a donc induit une modification de la charge de la preuve. Pour une entreprise, il ne suffit plus de se défendre lorsqu'une faute a été commise, comme c'était le cas auparavant. Elle doit aujourd'hui pouvoir prouver qu'elle a mis en place tous les processus visant à éviter que cette faute puisse se produire* ». Or, en matière de gouvernance de l'information, les risques à surveiller et éviter sont nombreux. « *Ils peuvent être liés à la cybercriminalité, à la dégradation des infrastructures, à l'obsolescence des outils, à la perte ou au détournement de fichiers ou de données, à la négligence humaine, et dans certains cas à la non-complétude de documents engageants* », observe de son côté Caroline Fiscal, directrice de Serda Conseil.

signatures électroniques et dossiers de preuve

Pour Serda Conseil, les parapheurs électroniques « *gages de la traçabilité du processus de validation* » sont désormais la clé de voûte d'une bonne gouvernance. Leur succès repose sur la capacité des organisations à relever des enjeux de « *confiance numérique* », résume Richard Lamy, responsable de produit chez Docaposte. Avec la signature électronique, l'identité du signataire peut être vérifiée par le biais d'un certificat (un petit fichier infalsifiable et au contrôle exclusif), tandis que la signature est horodatée et le contenu protégé de toute modification par un chiffrement dit asymétrique : « *Il calcule une empreinte du document avec la clé privée du signataire* » (tout changement viendrait casser cette signature).

Les entreprises ne doivent pas pour autant négliger « *le dossier de preuves* », rappelle ce spécialiste. Même son de cloche du côté d'Adrien Torregrosa, responsable marketing de Lex Persona (spécialiste français de la signature électronique) qui ajoute que ce fichier garantissant la valeur probatoire des signatures électroniques « *doit être lisible et récupérable rapidement* ».

archivage électronique

Pour Hervé Streiff, directeur de la stratégie digitale chez Helians, il est d'ailleurs conseillé d'envoyer en bout de chaîne l'ensemble des documents en archivage : « *En général, on récupère à ce stade les empreintes numériques qui ont été versées dans la signature, via un bordereau de dépôt traditionnel. Ces éléments de calcul d'empreinte numérique vont se retrouver dans les éléments de journalisation chaînée, conformes à la norme NF Z 42-013. Cela nous permet de préserver la sécurité de ces journaux chaînés en cas de disparition des services producteurs situés en amont* ».

Reste que « *cet archivage électronique est encore souvent considéré comme secondaire par les entreprises* », déplore Fabrice Aressi, PDG de LuxTrust, un prestataire de services de confiance numérique. « *Elles se focalisent sur la signature et nous avons encore beaucoup d'évangélisation à faire sur le reste, et en particulier l'archivage* ».

archimag
PAYS :France
PAGE(S) :30-31
SURFACE :141 %
PERIODICITE :Mensuel
DIFFUSION :(8000)
JOURNALISTE :Christophe Dutheil
► 1 juillet 2022 - N°356

Pascal Baisnée (Certilane) et Sylvain Staub (Data Legal Drive) en ouverture du séminaire animé par les journalistes *Archimag* Eric Le Ven et Fabien Carré-Marillonnet. DR

intelligence artificielle

Pineappli, une plateforme de dématérialisée présentée comme *« hyper sécurisée »*, s'intéresse quant à elle à l'intelligence artificielle (□A) et au développement de règles qui vont permettre d'automatiser le traitement des archives entrantes □ *« une tâche qui embête tout le monde actuellement »*, explique □ean-□arc Rietsch, son fondateur. Des technologies comme la recherche sémantique devraient permettre à cette plateforme de réduire la quantité de métadonnées utiles pour chaque archive : *« L'utilisateur pourra effectuer des recherches directement dans tous les termes contenus dans chaque document »*.

Chez □essi, Romain Le Formal, responsable mar□eting pour les offres EC□ et SAE, considère pour sa part que l'un des grands défis est de *« faciliter le travail caché de mise en archive, de façon quasi automatique, et le typage des documents afin qu'ils puissent être versés au bon endroit »*. Et ce, à l'appui de nouveaux outils d'□A et d'extraction de données.

certification PVID

Pour Romain Le Formal, la certification en cours des prestataires de vérification d'identité à distance (PV□D) par l'Agence nationale de la sécurité des s□stèmes d'information (Anssi) *« constitue aussi une évolution importante sur le marché »* : □essi est l'un des premiers candidats à l'obtention de ce label qui *« pose un cadre pour obtenir une identité substantielle ou élevée à distance »* (utilisation de la vidéo pour la détection du caractère vivant de l'utilisateur, l'acquisition de données ou l'enregistrement de certaines données biométriques...). *« La principale menace lors d'une vérification d'identité, qu'elle ait lieu en face à face ou à distance, est l'usurpation d'identité »*, justifie l'Anssi.

un monde sans mots de passe ?

Pour l'avenir, *« l'une des grandes révolutions réside dans les identités décentralisées ("decentralized identities" ou* "self-sovereign identities□ en anglais) □ selon □arim □ouami, directeur identité digitale et services de confiance chez Devoteam. La particularité de ces identités souveraines, que les éditeurs de logiciels de confiance pourraient s'approprier, est de donner aux utilisateurs le contr□le de leur identité numérique. Si possible en supprimant les mots de passe, considérés comme le maillon faible des cha□nes d'authentification. C'est ce que propose l'Alliance Fido (Fast □dentit□□nline), un consortium de fournisseurs de services, d'institutions financières, de processeurs de paiement et de grandes entreprises technologiques (Google, Faceboo□ Amazon, □hales...). Fido2, le dernier protocole issu des travaux de ce groupe, utilise deux protocoles d'identification (□ebAuthn et C□AP) pour permettre aux utilisateurs de s'identifier sur un site ou une application compatibles avec des données biométriques, des codes Pin ou des authentificateurs Fido externes. Les clés privées et les données biométriques ne quittent jamais l'appareil de l'utilisateur. Ce qui devrait réduire considérablement les risques de fuites de données. ■

Christophe Dutheil