Le système de reconnaissance biométrique du FBI est opérationnel

Le système de reconnaissance biométrique du FBI est opérationnel

Grâce aux outils du système NGI, le FBI pourra retrouver des criminels dans tous les Etats-Unis grâce à une empreinte, un scan d'iris ou une photo.

Le système NGI sera disponible dans tous les Etats-Unis d'ici à la fin 2014.
Après trois années de développement, le nouveau système de reconnaissance biométrique Next Generation Identification system) du FBI est opérationnel a annoncé le Bureau le 15 septembre 2014. Il a été conçu pour améliorer les possibilités d'identification biométriques explique le FBI dans son communiqué.
Il comporte deux nouveaux outils qui viennent s'ajouter aux bases de données d'empreintes digitales et de scans d'iris. Le premier concerne la reconnaissance faciale, l'Interstate Photo System (IPS) et le second, Rap Back, fournit des notifications écrites.

La base contiendra à terme 52 millions de photos.

Rap Back permet à toutes les autorités habilitées de recevoir des informations sur l'historique criminel de toute personne occupant un poste de confiance : un professeur, un conseiller bancaire…, explique le FBI dans son communiqué. Plus question de passer sous silence une arrestation pour conduite en état d'ivresse à 19 ans. Quant à IPS, il permet d'accélérer la recherche de criminels grâce à une base de données qui comptera 52 millions de photos d'ici à 2015.

En avril dernier, l'ONG Electronic Frontier Foundation émettait déjà quelques réserves sur cet outil. En premier lieu, elle dénonçait le mélange des genres puisqu'en plus des photos de criminels, celles de citoyens lambdas se trouvaient dans cette base. Elle s'inquiétait également du risque de « faux positif » compte tenu du taux de fiabilité du système qui n'est que de 85 %.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.01net.com/editorial/626932/le-systeme-de-reconnaissance-biometrique-du-fbi-est-operationnel/#?xtor=EPR-1-NL-01net-Actus-20140916

Cécile Bolesse

Données personnelles : la Cnil épingle l'opacité des applis mobiles

Données personnelles : la Cnil épingle l'opacité des applis mobiles

Près de 15% de 121 applications examinées ne fournissent aucune information sur le traitement des données collectées et la moitié rendent ces infos peu accessibles.

La collecte de données personnelles par les applis mobiles téléchargées ne donne pas lieu à beaucoup d'informations de la part de leurs éditeurs. C'est le constat issu d'une démarche initiée, en mai 2014, par la Cnil et 26 de ses homologues dans le monde. Celles-ci ont mené un audit en ligne simultané de plus de 1 200 applications mobiles gratuites et payantes.
Leurs vérifications ont porté sur le type de données collectées par les applications, le niveau d'information des utilisateurs et la qualité des explications données par l'application concernant le motif de la collecte de ces données.
Pour la France, la Cnil a examiné 121 applications parmi les plus populaires pour les trois principaux systèmes d'exploitation mobiles (iOS, Android, Windows Phone). Ses conclusions ne diffèrent pas du constat général effectué à l'échelon mondial.
La CNIL a passé au crible 121 applications mobiles les plus populaires en France
Ainsi, 15% des applications examinées ne fournissent aucune information sur le traitement des données collectées. Et même lorsqu'une information est fournie sur la politique de collecte, près de la moitié des applications concernées ne la rendent pas facilement accessible.
La Cnil déplore qu'on impose à l'utilisateur une recherche active sur le site internet de l'éditeur ou dans les différents onglets de l'application : « Il a ainsi été constaté que les mentions d'information de certaines applications à destination d'utilisateurs français ne sont disponibles qu'en anglais. »
Fort des de constat, la Commission recommande aux utilisateurs d'être à la fois curieux, vigilants et exigeants. « Il existe un large choix d'applications offrant des services similaires, détournez vous de celles qui en demandent le plus et en disent le moins ! » conclut-elle.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.01net.com/editorial/626952/donnees-personnelles-la-cnil-epingle-lopacite-des-applis-mobiles/#?xtor=EPR-1-NL-01net-Actus-20140917
Frédéric Bergé 01net.le 16/09/14 à 19h50

La France nomme un « administrateur général des données », le 1er en Europe

La France nomme un « administrateur général des données »

Nous l'avions annoncé le 26 mai dernier :http://www.lenetexpert.fr/france-nome-chef-protection-donnees-personnelles-les-administrations-cdo-chief-data-officer/
Henri Verdier vient d'être nommé administrateur général des données, la première fonction de ce type créée dans un pays d'Europe, afin de faire entrer le service public dans l'ère des données, selon un décret publié vendredi.

Le responsable, qui conserve ses fonctions de directeur d'Etalab, la mission chargée de l'ouverture des données publiques, est placé sous l'autorité du Premier ministre au sein du secrétariat général pour la modernisation de l'action publique.
« L'État doit savoir utiliser ses données pour s'améliorer, pour faire des économies, pour mieux piloter certaines politiques publiques », a expliqué Henri Verdier à l'AFP au cours d'une visite de start-up vendredi, avec Thierry Mandon, secrétaire d'État chargé de la Réforme de l'État.
« Il faut avoir des +data scientists+, des gens qui ont la culture de la donnée dans l'État, on va en recruter quelques uns pour faire de l'expérimentation. Il faut être sûr que celui qui prend une décision ait vraiment la donnée. Il faut être sûr qu'on les recueille bien », a-t-il poursuivi.
M. Verdier, membre fondateur en 2006 du pôle de compétitivité Cap Digital, sera chargé d'assurer l'ouverture des données, leur circulation et leur exploitation au sein de l'administration afin d'améliorer l'action publique. Il pourra aussi proposer au Premier ministre une position française dans les négociations internationales sur la politique de la donnée.
Thierry Mandon a souligné « l'intérêt économique » de l'ouverture des données publiques lors de sa visite dans les start-up Fivebyfive et Snips, spécialisées dans le traitement de la donnée.
Fivebyfive a mis au point des applications pour la SNCF lui permettant d'adapter son réseau de gares aux personnes à mobilité réduite, tandis que Snips a construit notamment un modèle permettant de prédire les risques d'accidents de la route à base de données comme la météo, la date, la topographie…

La France est le premier pays à mettre en place un administrateur général des données au niveau national, alors que cette fonction de « chief data officer » a été créée par certaines villes comme New York ou San Francisco ou entreprises comme Yahoo, CityGroup, Ogilvy.

Décret n° 2014-1050 du 16 septembre 2014 instituant un administrateur général des données

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://lentreprise.lexpress.fr/actualites/1/actualites/la-france-nomme-un-administrateur-general-des-donnees-le-1er-en-europe_1577573.html

---

Droit à l'oubli : des directives édictées par le G29 en préparation

Droit à l'oubli : des directives édictées par le G29 en préparation

Réunis en assemblée cette semaine, les différentes autorités de protections des données personnelles européennes ont commencé à travailler sur les directives d'applications du droit à l'oubli. Pour l'instant, chaque moteur de recherche interprète ce droit à sa manière.

Si la loi issue de l'arrêt rendu en mai par la CJUE ne fait plus débat, son application reste encore problématique. Dans les faits, cet arrêt met en place un droit à l'oubli, garantissant aux citoyens des moyens de recours afin de faire déréférencer des informations les concernant et qu'ils ne jugent plus valides ou discriminantes.
Mais si tout le monde s'accorde plus ou moins sur cette décision, la mise en place effective de ce droit fait débat. Google a ainsi rapidement proposé un formulaire afin de transmettre les demandes de déréférencement relatives au droit à l'oubli mais la Cnil voit d'un mauvais œil cette approche unilatérale, qui laisse à Google le soin d'interpréter à sa guise l'arrêt de la CJUE et de s'imposer comme intermédiaire unique.

Axelle Lemaire, secrétaire d'Etat au Numérique, expliquait d'ailleurs à ZDNet.fr que ce modèle « ne lui convenait pas » tout en plaidant pour une redéfinition du rôle de la Cnil.

Une réunion des différentes Cnil européenne avait lieu mercredi et jeudi. A cette occasion, les participants ont annoncé la préparation de directives afin de statuer sur les cas litigieux. Rien de définitif pour le moment, le projet est encore à l'étape de l'élaboration, mais le G29 promet qu'un document complet sera présenté pour le mois de novembre.

Dura lex, sed lex
L'objet de ces directives sera de donner une « boite à outils » pour jauger les cas jugés complexes, c'est-à-dire les cas refusés par Google. Pour l'instant en effet, Google est seul à juger de la validité des demandes de déréférencement qui lui sont adressées. Ces outils se présenteront sous deux formes : d'une part une classification des cas en différentes catégories et d'autre part une compilation des différents arbitrages rendues par les autorités nationales, afin de donner des références pour l'application des jugements futurs.
Au total, 90 réclamations ont été déposées auprès des différentes autorités nationales suite à un refus de déréférencement de la part de Google, dont une vingtaine en France. Google avait annoncé en juillet avoir reçu plus de 90.000 demandes de déréférencement mais ce chiffre progresse et Reuters rapporte que Google aurait déjà traité plus de 120.000 demandes.Nous avons contacté les porte-paroles de Google France à propos de ces chiffres mais nous n'avons pas encore reçu de réponse de leurs part.
Les membres du G29 ont également rencontré différents éditeurs de presse, inquiets des conséquences du déréférencement de leurs articles vis-à-vis du droit à l'information. Outre l'opposition entre Google et les différentes autorités européennes autour de l'application de ce nouveau droit, le débat reste ouvert afin de trouver le « bon équilibre » entre protection des données personnelles et droit légitime à l'information pour le grand public.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.zdnet.fr/actualites/droit-a-l-oubli-des-directives-edictees-par-le-g29-en-preparation-39806625.htm
Par Louis Adam | Vendredi 19 Septembre 2014

Droit à l'oubli : Google continue ses discussions, la

Cnil veut traiter des refus

Droit à l'oubli : Google continue ses discussions, la Cnil veut traiter des refus

Google continue son tour des capitales européennes et mène des discussions autour de l'application du droit à l'oubli pour tous. De son côté, le groupement des autorités chargées de la protection des données personnelles édite un registre commun des demandes de déréférencement refusées par les moteurs.

Le G29, le groupement européen de l'ensemble des autorités chargées de la protection des données personnelles (en France la Cnil) avance sur le dossier du droit à l'oubli. Le collectif annonce avoir mis en place des référents, dans chaque pays, dont la tâche sera de dresser des pratiques communes pour traiter les demandes de déréférencement, en particulier les refus des moteurs de recherche.

Le réseau mis sur pied par le G29 aura la charge d'éditer un registre commun des suites données aux plaintes. Il devra ainsi mettre en place un tableau de bord destiné à coordonner leurs actions en cas de refus des moteurs de recherche. La Cnil indique par exemple avoir déjà reçu « plusieurs dizaines de plaintes ».
Pour rappel, cette procédure de déréférencement est née suite à la publication en mai dernier d'une décision de la Cour de justice de l'Union européenne. La juridiction estimait qu'une personne peut être fondée à demander à ce qu'un moteur de recherche déréférence des liens dirigeant vers des informations la concernant.
La Cour ne consacrait toutefois pas un droit absolu à l'oubli. Elle relevait l'importance de « rechercher un juste équilibre entre cet intérêt et les droits fondamentaux de la personne concernée, en particulier le droit au respect de la vie privée et le droit à la protection de données à caractère personnel ». Le déréférencement peut donc être refusé si le public justifie d'un « intérêt prépondérant » à accéder à ces informations.
De son côté, Google mène actuellement des réunions publiques dont le but est de trouver un « équilibre entre le droit des personnes à l'oubli et le droit à l'information du public ». Après Madrid et Rome, ce rendez-vous doit atteindre Paris à la fin du mois.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://pro.clubic.com/entreprises/google/actualite-728183-droit-oubli-google-discute-cnil.html

Au Delaware, les héritiers auront accès à la vie numérique du défunt

Au Delaware, les héritiers auront accès à la vie numérique du défunt

L'Etat américain du Delaware est le premier à adopter une loi qui autorise les héritiers et/ou exécuteurs testamentaires à accéder à la vie numérique d'une personne décédée ou incapable d'y accéder par elle-même. Mais pour le moment, les services numériques (Google, Facebook et consorts) refusent de coopérer.

« A mes enfants je lègue ma maison, mes documents numériques, mon compte Facebook, mon blog et mes achats iTunes ».

Peut-être pourrons-nous un jour lire ce genre de phrase dans les testaments. Dans l'état du Delaware aux Etats-Unis, c'est même déjà le cas, et c'est une première. A noter que les états de l'Idaho ou du Nevada proposent déjà d'accéder à des fichiers numériques, mais de manière plus limitative.
La loi (baptisée « Fiduciary Access to Digital Assets and Digital Accounts Act » dite UFADAA) adoptée outre-Atlantique va même plus loin puisqu'elle donne de fait le droit aux familles d'accéder aux fichiers numériques d'une personne disparue. Concrètement, elle confère le droit aux héritiers et exécuteurs testamentaires de prendre le contrôle de ces fichiers comme ils le feraient pour des biens matériels.
Mais la réalité est bien différente. Car ceci impose une coopération des fournisseurs de services numériques. Ceci est un changement majeur car aujourd'hui, lorsqu'une personne disparaît, ses droits numériques disparaissent avec elle. Actuellement sur Facebook par exemple, le site consent à transformer la page d'un utilisateur décédé en « page de commémoration ». Il précise : « nous ne pouvons pas communiquer les informations de connexion d'un compte de commémoration. Se connecter au compte d'une autre personne constitue une violation de notre règlement ».

Bataille juridique en vue
« Nos lois n'ont pas évolué en même temps que nos technologies », estime Daryl Scott, membre de la chambre des députés du Delaware, militant pour que les fournisseurs de service coopèrent. Mais la bataille est loin d'être gagnée. « Cette loi ne tient pas compte de l'intrusion dans la vie privée que cela représente pour les personnes tierces qui ont communiqué avec la personne disparue », souligne Jim Halpert, avocat de DLA Piper, qui travaille notamment pour Google, Facebook, Yahoo et d'autres entreprises du numérique.
Il continue et explique que « cela comprend donc les communications potentiellement confidentielles entre une personne disparue et d'autres encore de ce monde – les patients d'un docteur, d'un psychiatre ou d'un homme d'église décédé par exemple – qui seraient alors très surpris qu'un exécuteur testamentaire ait accès à leurs conversations privées. La loi en tant que telle peut créer beaucoup de confusions car, comme la loi elle-même le reconnaît, la loi fédérale peut interdire la divulgation de certaines communications ».
Enfin, il estime encore qu'une lettre manuscrite et un mail n'ont pas la même valeur et ne doivent donc pas être traités de la même manière. « Le volume de mails est beaucoup plus gros et les gens sont généralement beaucoup plus prudents lorsqu'ils écrivent une lettre », termine-t-il.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.linformaticien.com/actualites/id/33954/au-delaware-les-heritiers-auront-acces-a-la-vie-numerique-du-defunt.aspx

Nouveau vol de données : Home Depot victime d'une cyberattaque et d'un vol massif de données ?

Nouveau vol de données : Home Depot victime d'une cyberattaque et d'un vol massif de données ?

Après Target, auprès de qui des pirates avaient dérobé des millions de données bancaires de clients, Home Depot pourrait bien être le dernier sur la liste. Les informations des clients de ses 2200 magasins aux US auraient été exposées pendant plusieurs mois.

Home Depot pourrait bien être la dernière enseigne américaine de la distribution à avoir fait l'objet d'une attaque informatique de grande envergure avec pour conséquence le vol de données bancaires de ses clients.
Toutefois, pour l'heure, l'entreprise ne confirme pas une telle menace. Le commerçant se borne pour le moment à faire savoir qu'il a identifié une « activité inhabituelle » en lien avec ses données de clientèle.
Néanmoins, plusieurs éléments semblent attester d'une fuite de données sensibles, dont l'ampleur reste à évaluer. D'après Brian Krebs, un spécialiste de la sécurité, Home Depot collabore avec les forces de police et « plusieurs banques » soupçonnent l'enseigne d'être la source de l'utilisation illicite de données bancaires vendues au marché noir.

Dernier naufrage d'une enseigne de distribution ?
« Protéger les données de nos clients est pour nous un sujet de très grande importante et nous faisons actuellement tout notre possible pour réunir des faits tout en nous efforçant de protéger les clients » commente auprès de la presse une porte-parole de Home Depot, qui admet la possibilité d'une faille.
« Si nous confirmons qu'une fuite s'est produite, nous nous assurerons que nos clients sont prévenus immédiatement » précise-t-elle ainsi. Et pour Brian Krebs, il y a bien eu fuite. Celle-ci aurait débuté en avril dernier et concernerait les 2.200 magasins de Home Depot aux US.
La faille pourrait ainsi s'avérer de plus grande ampleur que celle qui a touché Target en 2013, et pourtant déjà affecté plus de **110 millions de données clients (numéros de cartes, codes PIN et informations personnelles)**.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.zdnet.fr/actualites/home-depot-victime-d-une-cyberattaque-et-d-un-vol-massif-de-donnees-39805665.htm

5 conseils pour protéger ses photos et données perso dans le cloud

5 conseils pour protéger ses photos et données perso dans le cloud

Chiffrement, mot de passe et bon sens commun sont les meilleures armes pour protéger ses données dans le cloud. Même si le risque zéro n'existe pas.

Avec le piratage des photos nues de stars féminines, le problème de la sécurité des services cloud se rappelle à notre bon souvenir. Externaliser le stockage de ses données auprès d'un service en ligne peut être très pratique, mais cela présente aussi des risques, et même de plus en plus. Lors des dernières conférences de sécurité BlackHat et Defcon à Las Vegas, les experts en sécurité sont d'ailleurs unanimes à ce sujet : à force d'interconnecter de plus en plus de services en ligne et d'objets, on augmente la surface d'attaque, et donc le risque de se faire pirater. « Un bon hacker suffisamment motivé peut pirater presque n'importe quoi aujourd'hui », estime même Dan Geer, un expert américain reconnu en sécurité informatique.
Mais alors, le combat est-il perdu d'avance ? Par forcément, car il existe un certain nombre de règles de bons sens qui permettent quand même de limiter le risque.

1) Evitez le cloud pour stocker des données confidentielles. Stocker ses photos sur iCloud ou Google Drive, c'est très pratique, notamment pour les synchroniser et les partager avec vos amis. Mais, de grâce, n'y mettez pas les clichés de vos derniers ébats sexuels. Vous pourriez le regretter.

2) Utilisez un bon mot de passe. Certains experts pensent que le service d'Apple a été victime d'un attaque par force brute, c'est-à-dire le test une par une de toutes les combinaisons possibles (voir ci-dessous). Avec un mot de passe tel que « 0123456 », votre compte explose en quelques secondes. Choisissez, de préférence, une suite aléatoire de chiffres et de lettres. Evidemment, il est impossible de s'en souvenir, c'est pourquoi il faut utiliser un gestionnaire de mots de passe tel que 1pass ou LastPass.

3) Chiffrez vos données. Si vous avez des données confidentielles et que vous voulez quand même utiliser le cloud, il y a une solution : le chiffrement préalable. Les données sont d'abord cryptées par un logiciel tel que TrueCrypt, puis envoyées vers le service de stockage en ligne. Même en cas de vol, les données sont (théoriquement) inutilisables. Certains services en ligne, comme SpiderOak, intègrent d'emblée cette procédure de chiffrement, la rendant plus simple d'usage (technologie Zero-Knowledge). Le revers de la médaille est que le chiffrement n'autorise pas certaines fonctionnalités très pratiques comme le partage ou la modification en ligne. Il faut faire un choix…

4) Analysez la sécurité de votre fournisseur. Tous les fournisseurs cloud ne sont pas au même niveau technologique. Certes, tous utilisent au minimum le chiffrement HTTPS, mais qu'en est-il du chiffrement des communications entre les datacenters (comme l'ont implémenté Google et Yahoo désormais) ? Le fournisseur propose-t-il l'authentification à deux étapes (comme Twitter, Google + ou Apple) ? Utilise-t-il la technologie Perfect Forward Secrecy pour blinder encore plus ses communications chiffrées (comme Microsoft ou Twitter) ? Cette analyse n'est pas aisée à faire, mais elle s'impose dès lors que les données sont sensibles.

5) Ne partagez pas tout avec n'importe qui. Le niveau de sécurité de vos données est égal au plus bas niveau de sécurité mis en place par vos amis avec qui vous les partagez. C'est le principe du maillon faible. Donc, sélectionnez bien les amis avec qui vous partagez vos photos confidentielles. Evitez, par exemple, d'inclure votre ex-petit ami(e) dans la liste…
Gilbert Kallenborn01netle 02/09/14 à 15h09

Pour information, Denis JACOPINI et son équipe proposent des solutions pour protéger vos données :
– protection contre la perte de données
– protection contre la fuite de données
– cryptage de clés usb, d'ordinateurs, d'espace Cloud ou de données
– renforcement des autorisations (sécurité avancée par SMS, biométrie…)
Audit – Conseils – Sensibilisation/Formation des utilisateurs à la sécurité informatique
Contactez-nous

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.01net.com/editorial/625810/vol-de-photos-de-nus-5-conseils-pour-proteger-ses-donnees-dans-le-cloud/#?xtor=EPR-1-NL-01net-Actus-20140902

La dangereuse faille informatique Heartbleed constitue toujours une menace

La dangereuse faille informatique Heartbleed constitue toujours une menace

Près de cinq mois après la révélation de la vulnérabilité Heartbleed, IBM dresse un premier bilan, avec le rapport trimestriel de sa division X-Force, en s'appuyant sur les informations retirées des infrastructures des clients de ses services de sécurité managés. Et celui-ci s'avère contrasté.

La bonne nouvelle, c'est que l'intérêt malveillant pour la vulnérabilité semble s'être sensiblement tassé : si IBM a enregistré jusqu'à plus de 300 000 attaques par jour exploitant Heartbleed le 15 avril dernier, le chiffre est rapidement retombé, à quelques centaines d'incidents par jour fin avril. L'effet de grandes entreprises qui ont été capables de mettre rapidement en œuvre des contre-mesures. De quoi pousser les attaquants à déplacer leurs efforts sur d'autres vulnérabilités. Pour autant, l'activité malveillante liée à Heartbleed se maintient, explique IBM, estimant qu'environ « 50 % des serveurs potentiellement vulnérables ont été laissés sans correctif ». De quoi faire, pour le groupe, de la vulnérabilité « une menace continue et critique ».
Mais pour IBM, le plus important est peut-être à chercher du côté de la gestion de la réaction : « disposer d'un plan de réaction aux incidents – et d'une base de données à jour des actifs – s'est avéré absolument critique pour réduire l'exposition au risque. » En outre, selon le groupe, si les pare-feux ont pu rapidement offrir une protection pour les systèmes concernés, les dispositifs de détection et de prévention des intrusions ont pu « fournir une protection encore plus importante en bloquant les attaques au niveau des paquets ». D'autant plus que les attaquants semblent avoir privilégié la carte de l'exploitation distribuée de la vulnérabilité Heartbleed, rendant plus difficile la protection par des pare-feux.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.lemagit.fr/actualites/2240227500/Heartbleed-constitue-toujours-une-menace?asrc=EM_MDN_33243175&utm_medium=EM&utm_source=MDN&utm_campaign=20140827_L%27essentiel%20IT%20:%20Premi%e8re%20politique%20globale%20de%20s%e9curit%e9%20en%20France%20-%20VMWare%20se%20convertit%20aux%20appli_

L'utilisation juridique des documents numériques – Article de presse dans L'Echo du mardi du 12 08 2014


Consultants

Consultants

Nos experts ont la parole

Utilisation juridique des documents numériques

L’utilisation juridique des documents numériques

Article de presse dans L’Echo du mardi du 12/08/2014

L’utilisation juridique des documents numériques

«Dans le doute, après avoir numérisé un document officiel, vous avez probablement préféré conserver l’original dans son format matériel (bien souvent papier).

A l’heure de la dématérialisation à outrance (remplacement dans une entreprise ou une organisation de ses supports d’informations matériels, souvent en papier, par des fichiers informatiques et des ordinateurs, jusqu’à la création de « bureau sans papier » ou « zéro papier » quand la substitution est complète), il est temps de se poser des questions sur la valeur juridique des documents informatiques en cas de contestation ou de litige. Le traitement de documents dématérialisés présente un certain nombre d’avantages significatifs.»

Télécharger l’article complet

Cet article vous à plu ? Laissez-nous un commentaire (notre source d’encouragements et de progrès)