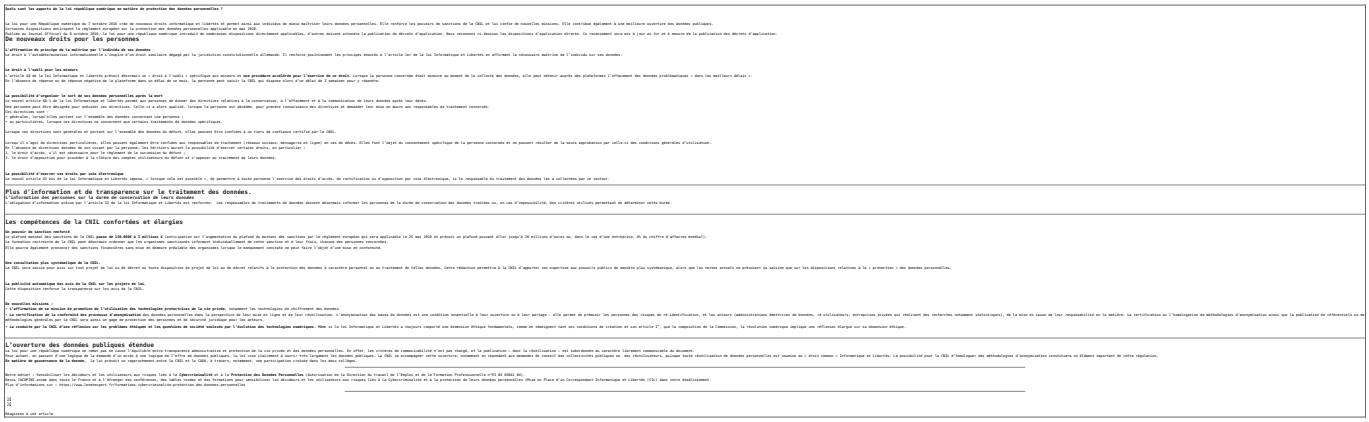
La loi pour une République numérique protège encore plus nos données personnelles

	La loi pour une République numérique protège encore plus nos données personnelles



Original de l’article mis en page : Ce que change la loi pour une République numérique pour la protection des données personnelles | CNIL

Comment être en conformité au Règlement sur les Données Personnelles dans les temps ?

Comment être en conformité au Règlement sur les Données Personnelles dans les temps ?

Conformité au GDPR : comment être dans les temps ?

Nous le savons tous, la transformation numérique a bouleversé et continue de bouleverser notre quotidien, nos modèles économiques et modifie nos échelles de temps. On ne parle plus que d'instantanéité, de prédiction et d'anticipation. Les technologies permettent de disposer de millions de « données consommateur », de les exploiter dans l'instant, et ainsi inciter à tel achat ou tel comportement. Ces données, nous les fournissons d'ailleurs volontairement ou involontairement à travers l'utilisation quotidienne de nos smartphones, tablettes, ordinateurs et de plus en plus d'objets connectés de toutes sortes.
Mais que se passe-t-il si ces données, nos données, sont dérobées et exploitées ? Les conséquences peuvent être dévastatrices…tant pour le consommateur que pour l'entité qui les détient.
Le GDPR, nouveau règlement européen, a notamment pour ambition de faire prendre conscience aux entreprises de la valeur des données personnelles et de les responsabiliser quant à leur utilisation et donc à leur protection…

Seulement deux ans pour se mettre en conformité
Même si la protection des données n'est qu'un volet d'un texte qui en comporte beaucoup d'autres (droit à l'oubli, portabilité des données, gestion des consentements…), en mai 2018, toute entreprise devra être en mesure de prouver à n'importe quel moment, que les données personnelles qu'elle détient (IBAN, numéros de téléphone, identifiants divers, etc.) sont protégées et surtout inexploitables en cas de vol. Le texte préconise à cet effet la « pseudonymisation » des données (c'est-à-dire les « anonymiser » de manière réversible) afin de garantir l'impossibilité de leur utilisation en cas de vol.

Pseudonymiser les données : le challenge d'y arriver seul
Outre la complexité et le coût du développement d'une technologie permettant d'anonymiser les données, la conformité au GDPR a des impacts techniques, organisationnels et juridiques importants, ne serait-ce « que » pour la gestion des consentements et le droit à l'oubli. Il faut répertorier les données, mesurer leur degré de sensibilité, mettre en œuvre des techniques permettant le niveau de protection correspondant à la finalité de leur traitement, etc. Tout ceci va bien sûr engendrer des charges importantes pour les DSI. Partir de zéro avec un délai de deux ans pour réussir est un challenge que seules les entreprises avec une DSI disponible vont pouvoir relever. Une DSI disponible ? Elle est déjà bien occupée à développer de nouveaux services, de nouvelles applications. C'est pourquoi, se reposer sur des outils et des services qui sont capables depuis des années de protéger des données sensibles de paiement en réalisant des centaines de millions d'opérations de tokenisation / dé-tokenisation par mois semble être une solution à privilégier…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l’article mis en page : Conformité au GDPR : comment être dans les temps ? – Global Security Mag Online

---

Le décret du fichier biométrique TES attaqué en justice

	Le décret du fichier biométrique TES attaqué en justice

Le collectif des Exégètes Amateurs annonce son intention d'attaquer devant le Conseil d'État le décret donnant naissance au controversé fichier TES.

L'offensive judiciaire est lancée. Mardi, le collectif des Exégètes Amateurs a annoncé sa décision d'engager un recours au Conseil d'État – la plus haute des instances administratives en France – contre le décret du fichier TES (Titres Électroniques Sécurisés), qui a été publié discrètement au Journal officiel le 30 octobre 2016, en plein week-end de la Toussaint.
Découvert à ce moment-là, le fichier TES inquiète. Il s'agit d'une base de données qui réunira les données personnelles et biométriques de la quasi totalité des Français. En effet, il est destiné aux passeports et aux cartes d'identité. Néanmoins, il inquiète par l'ampleur et la nature des informations qu'il est amené à recevoir. Surtout, il pourrait servir tôt ou tard à d'autres fins que celles actuellement prévues.

La stratégie exacte des Exégètes Amateurs – qui rassemble La Quadrature du Net, la fédération de FAI associatifs FFDN et l'opérateur French Data Network (FDN) – contre le décret n'a pas été précisée. La coordinatrice des campagnes de La Quadrature du Net, Adrienne Charmet, a simplement indiqué sur Twitter que les détails seront communiqués ultérieurement.
Parmi les angles d'attaque éventuels, l'avocat des nouvelles technologies Rubin Sfadj suggère sur son blog une incompatibilité du décret avec l'article 34 de la Constitution. Celui-ci expose que c'est au législateur que revient le pouvoir de fixer les règles applicables en matière de libertés publiques et de procédure pénale. Dit autrement, c'est au parlement de décider par à l'exécutif.
Les Exégètes Amateurs – une expression de l'ex-député socialiste Jean-Jacques Urvoas, désignant, de manière dédaigneuse, ceux qui s'opposent par des arguments de droit à la loi sur le renseignement dont il était le rapporteur – regroupent des juristes et bénévoles qui ont pris l'habitude de multiplier les recours en justice contre des textes législatifs et réglementaires qu'ils jugent dangereux…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Le décret du fichier biométrique TES attaqué en justice – Politique – Numerama

Denis JACOPINI intervient au Conseil de l’Europe lors de la conférence Octopus 2016

	Denis JACOPINI intervient au Conseil de l’Europe lors de la conférence Octopus 2016

A l'occasion de sa conférence annuelle consacrée à la lutte de la Cybercriminalité à travers le monde du 16 au 18 Novembre prochain au Conseil de l'Europe, Denis JACOPINI intervient au Workshop n°7

Au programme :

• La Convention de Budapest: 15e anniversaire
• Criminalité et compétence dans le cyberespace : la voie à suivre
Ateliers
• Coopération entre les fournisseurs de service et les services répressifs en matière de cybercriminalité et de preuve électronique
• L'accès de la justice pénale aux preuves dans le Cloud: les résultats du groupe sur les preuves dans le Cloud (Cloud Evidence Group)
• Renforcement des capacités en cybercriminalité: les enseignements tirés
• L'état de la législation en matière de cybercriminalité en Afrique, en Asie/Pacifique et en Amérique latine/aux Caraïbes
• Le terrorisme et les technologies de l'information : la perspective de la justice pénale
• Coopération internationale: amélioration du rôle des points de contact 24/7
• A la recherche des synergies: politiques et initiatives en cybercriminalité des organisations internationales et du secteur privé

Participation

La conférence sera l'occasion, pour les experts en cybercriminalité des secteurs public et privé ainsi que les organisations internationales et non gouvernementales du monde entier, d'échanger.

La conférence Octopus fait partie du projet **Cybercrime@Octopus** financé par les contributions volontaires de l'Estonie, du Japon, de Monaco, de la Roumanie, du Royaume-Uni, des Etats-Unis d'Amérique et de Microsoft ainsi que du budget du Conseil de l'Europe.
Agenda Octopus 2016

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : Octopus 2016

L’adresse IP est une donnée personnelle, encadrée par la CNIL

	L’adresse IP est une donnée personnelle, encadrée par la CNIL

Dans le cadre d'un pourvoi lié à l'affaire de piratage d'un cabinet immobilier, la Cour de Cassation a estimé que l'adresse IP est une donnée à caractère personnel et sa collecte est soumise à une déclaration auprès de la CNIL.

Voici une jurisprudence qui devrait mettre fin à un débat : l'adresse IP est-elle une donnée personnelle ? La Cour de Cassation vient de répondre par l'affirmative dans un arrêt du 3 novembre. La plus haute juridiction judiciaire avait été saisie en pourvoi dans une affaire de piratage d'un cabinet immobilier, Logisneuf.

Petit rappel des faits, lors d'un contrôle de sécurité sur ses serveurs, le service informatique du cabinet immobilier constate des centaines de connexions illicites provenant toutes d'adresses IP n'appartenant pas à son réseau. Par recoupement, les adresses provenaient d'un cabinet immobilier nantais, Peterson. Logisneuf a donc saisi le tribunal de commerce pour qu'une ordonnance réclame aux opérateurs de révéler le nom des utilisateurs des adresses IP suspectes. Cette opération a permis d'identifier plusieurs personnes chez Peterson et une plainte a été déposée auprès du procureur de la République contre ces personnes. Or les deux sociétés ont continué à se disputer sur la question de la conservation sous forme de fichier des adresses IP et l'obligation de le déclarer à la CNIL. Un arrêt de la Cour d'Appel de Rennes avait statué que « *l'adresse IP ne constituait pas une donnée même indirectement nominative* » et que le fait de « *conserver les adresses IP des ordinateurs… ne constitue pas un traitement des données à caractère personnel* ».

Une adresse IP est une donnée à caractère personnel

La Cour de Cassation était donc invité à se positionner sur ce sujet. Dans sa décision, les juges de la Première chambre civile se sont appuyés en premier lieu sur la loi du 6 janvier 1978 modifiée en 2004 et notamment son article 2 qui définit une donnée personnelle comme « *toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres* ». Pour la juridiction, l'adresse IP entre dans cette catégorie. Elle suit ainsi la position de la CNIL qui s'est prononcée sur le sujet depuis 2007, ainsi que l'ensemble des CNIL européennes. Le régulateur s'inquiétait des évolutions jurisprudentielles qui ne considéraient plus l'adresse IP comme une donnée personnelle. La Cour de Cassation a finalement tranché en faveur de la qualification de donnée à caractère personnel de l'adresse IP…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : L'adresse IP est une donnée personnelle, encadrée par la CNIL

Les données biométriques de tous les Français dans un fichier commun. Utile ou risqué ?

	Les données biométriques de tous les Français dans un fichier commun. Utile ou risqué ?

Un fichier unique, baptisé « Titres électroniques sécurisés » (TES). Ce fichier a un rôle-clé : rassembler dans une même base de données les données personnelles et biométriques des Français pour la gestion des cartes nationales d'identité et des passeports. Mais il suscite de vives inquiétudes.

À la toute fin du mois d'octobre, le gouvernement a fait publier un décret qui donne le coup d'envoi à la création d'un fichier qui rassemblera les données personnelles et biométriques de la quasi totalité des Français. Destiné aux passeports et aux cartes nationales d'identité, il inquiète par son ampleur et la nature des informations qu'il est amené à recevoir. Nous vous expliquons de quoi il en retourne en quelques questions.

À QUOI ÇA SERT ?

Le fichier en question, dénommé « Titres Électroniques Sécurisés » (TES), a vocation à être une base de données centrale rassemblant des informations personnelles et biométriques relatives aux détenteurs d'un passeport et / ou d'une carte nationale d'identité. Il remplace deux fichiers précédents, l'un pour le passeport l'autre pour la carte nationale d'identité.

QUELLES SONT LES ALTERNATIVES ?

Était-il possible de faire autrement ? Pour la commission nationale de l'informatique et des libertés (CNIL), sans aucun doute. Dans sa délibération, elle évoque un « *composant électronique sécurisé dans la carte nationale d'identité* » qui « *serait de nature à faciliter la lutte contre la fraude documentaire, tout en présentant moins de risques de détournement et d'atteintes au droit au respect de la vie privée* »
Elle ajoute que cette solution, qui n'a pas été censurée par le Conseil constitutionnel quand un précédent texte du même acabit a été présenté sous une autre majorité, « *permettrait de conserver les données biométriques sur un support individuel exclusivement détenu par la personne concernée, qui conserverait donc la maîtrise de ses données, réduisant les risques d'une utilisation à son insu* ».

SUIS-JE DÉJÀ FICHÉ ?

En pratique, oui. Il existe déjà deux fichiers, l'un pour le passeport, l'autre pour la carte nationale d'identité. La nouvelle base de données n'est que le prolongement de ce qui existait déjà. À moins de n'avoir jamais possédé ces titres (ils ne sont pas obligatoires), vous figurez déjà certainement dans ces fichiers. Seuls les enfants en bas âge peuvent y échapper, si aucune demande de titre d'identité n'a été faite.

EST-CE ACTÉ ?

Le système TES existe déjà pour le passeport et, pour les demandes de passeport, le dispositif n'est pas modifié par le décret ; TES est donc actif. Quant aux demandes de cartes, la CNIL nous précise que le nouveau dispositif entrera progressivement en vigueur, selon les arrêtés mentionnés dans le décret ; les empreintes seront prises à partir des dates de ces arrêtés ; le tout doit être finalisé avant le 31 décembre 2018.

POURQUOI C'EST DANGEREUX ?

« *Ce que la technique a fait, la technique peut le défaire* » prévient le sénateur PS Gaëtan Gorce, commissaire de la CNIL, dans une interview à Libération. Aujourd'hui, l'exécutif a pris des dispositions pour éviter certaines dérives (croisement ou remontée de données) et assurer un bon niveau de sécurité, ce que la CNIL reconnaît dans sa délibération. Mais demain ?
Comme nous l'indiquions dans notre sujet, maintenant que la base existe il pourrait bien y avoir un jour la tentation de l'utiliser pour faire de la reconnaissance automatisée des visages avec des caméras de surveillance. Un futur gouvernement, moins scrupuleux sur les questions de libertés publiques, pourrait vouloir l'employer autrement. Après tout, ne sommes-nous pas en guerre contre le terrorisme ?

QU'EN PENSE LA CNIL ?

La CNIL, garante du respect des libertés et de l'équilibre des traitements automatisés de données, fait part de « *plusieurs réserves* » dans sa délibération. Le contournement du législateur est regretté, au regard de « *l'ampleur inégalée de ce traitement et du caractère particulièrement sensible des données qu'il réunira* ». La commission demande une « *évaluation complémentaire du dispositif* ».

QUELS SONT LES RECOURS ?

Le gouvernement ayant fait le choix de passer par un décret, il n'a pas été possible de discuter de la création de ce fichier au cours de son parcours parlementaire s'il avait été présenté sous la forme d'un projet de loi. Interrogé à ce sujet par Libération, le sénateur PS Gaëtan Gorce, commissaire de la CNIL, explique qu'il doit être possible d'attaquer le décret par un recours devant le Conseil d'État
[Article de Numerama]

Réagissez à cet article

Original de l'article mis en page : Le fichage biométrique des Français en 7 questions – Politique – Numerama

---

60 millions de Français

fichés dans une base de données commune des titres d'identité

60 millions de Français fichés dans une base de données commune des titres d'identité

Un décret publié pendant le pont de la Toussaint officialise la création d'un gigantesque fichier national.
Soixante millions de Français glissés, à l'occasion d'un week-end de pont de la Toussaint, dans une même base de données : un décret paru au Journal officiel dimanche 30 octobre, et repéré par le site NextInpact, officialise la création d'un « traitement de données à caractère personnel commun aux passeports et aux cartes nationales d'identité ». En clair, les données personnelles et biométriques de tous les détenteurs d'une carte d'identité ou d'un passeport seront désormais compilées dans un fichier unique, baptisé « Titres électroniques sécurisés » (TES). Cette base de données remplacera à terme le précédent TES (dédié aux passeports) et le Fichier national de gestion (dédié aux cartes d'identité), combinés dans ce nouveau fichier.

La base de données rassemblera ainsi des informations comme la photo numérisée du visage, les empreintes digitales, la couleur des yeux, les adresses physiques et numériques… Au total, la quasi-totalité des Français y figurera, puisqu'il suffit de détenir ou d'avoir détenu une carte d'identité ou un passeport pour en faire partie – les données sont conservées quinze (pour les passeports) à vingt ans (pour les cartes d'identité)…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : 60 millions de Français

fichés dans une base de données commune des titres d’identité

Quelles sont les messageries qui protègent le mieux vos données personnelles ?

	Quelles sont les messageries qui protègent le mieux vos données personnelles ?

Apple, Google, Snapchat, Blackberry, ou encore le Chinois Tencent, tous ces géants du web proposent à leurs utilisateurs des messageries instantanées. Aujourd'hui, ce sont plusieurs milliards de personnes qui les utilisent quotidiennement. Au sein de ceux-là, des minorités opprimées, des militants pour les droits de l'Homme, des dissidents politiques, des lanceurs d'alertes… Mais comment ces messageries protègent-elles nos données ?

Amnesty International a rendu un rapport accablant sur la question, dans lequel elle effectue un classement des messageries privées.

Classement Amnesty International

Les onze grandes entreprises évaluées affichent toutes des engagements écrits en termes de protection de la vie privée. Et pourtant, aucune n'est irréprochable, toutes ne respectent pas les normes internationales en vigueur et peu proposent un niveau élémentaire de protection. Facebook, Apple ou Google sont en haut du classement, quand Microsoft, Snapchat, ou Tencent font figure de mauvais élèves. L'ONG a mis au point un barème.

Les critères du classement

Amnesty International attribue une note de 0 à 100 aux entreprises, selon leur résultat sur cinq critères provenant des normes internationales en la matière. Trois sont primordiaux pour assurer la sécurité des données personnelles.
Les entreprises sont jugées sur leur capacité à **reconnaître les menaces contre la vie privée et la liberté d'expression**. En clair, que mettent-elles en place pour protéger les droits de leurs utilisateurs ?
Elles doivent ensuite **appliquer par défaut le chiffrement de bout en bout**. Une question au cœur des préoccupations d'Amnesty International. L'ONG estime que seul le chiffrement de bout en bout est apte à protéger la vie privée. Ici, seul l'émetteur et le receveur détiennent la clef de chiffrement. Les acteurs intermédiaires du processus (fournisseur d'accès, entreprise de messagerie) n'ont donc pas accès au contenu de la conversation.
Les messageries doivent enfin **rendre publiques les informations sur les demandes de données d'utilisateurs par des gouvernements et refuser de contourner les clefs de chiffrements.**

Facebook, Apple, Telegram et Google en tête

La messagerie de Facebook est la mieux classée, avec un score de 73 points. Le bébé de Mark Zuckerberg totalise environ un milliard de fidèles quotidiens. C'est lui qui offre le plus de garanties à ses utilisateurs. Mais ses deux messageries ne sont pas équivalentes. Si WhatsApp propose un chiffrement de bout en bout par défaut (l'utilisateur n'a pas à choisir, c'est automatique), cette option récente de Facebook Messenger doit être activée.
Apple cumule 67 points. La marque à la pomme offre un chiffrement de bout en bout sur ses deux messageries (iMessenger et Facetime). Mais Amnesty International relève qu'elle « *devrait adopter un protocole de chiffrement plus ouvert qui permette une vérification indépendante complète* ».
Telegram est deuxième ex aequo, avec 67 points aussi. Ce nom vous dit quelque chose ? C'est normal, cette messagerie a beaucoup defrayé la chronique car elle est l'application de messagerie instantanée la plus prisée des milieux djihadistes. Elle perd des points car son système de chiffrement n'est pas automatique et doit être activé.
Vient ensuite Google avec un score de 53. Le moteur de recherche est critiqué par Amnesty International car ses trois messageries instantanées ne proposent pas toutes des systèmes de chiffrement.
Les quatre entreprises qui caracolent en tête se sont toutes publiquement prononcées contre les moyens de contournement des clés de chiffrement par les États. Et toutes, à l'exception de Telegram, préviennent leurs utilisateurs des demandes faites par les gouvernements.

Skype, Snapchat et Tencent, les mauvais élèves

Snapchat, c'est cette messagerie qui permet de s'envoyer une photo ou un texte sur un temps très court. Skype, propriété de Microsoft, c'est celle qui vous permet de faire des appels vidéo. Les deux applications sont mauvaises élèves aux quatrième et troisième plus mauvaises places.
Aucun chiffrement de bout à bout n'est proposé par les deux géants, qui présentent tous deux un système « *très vulnérable* », selon Amnesty. Les deux sont utilisées par des millions de jeunes quotidiennement, un public très menacé et très exposé à la cybercriminalité.
BlackBerry occupe l'avant-dernière place. La messagerie privée canadienne n'offre pas un système de chiffrement de bout en bout, elle le vend. Ainsi, si on ne paie pas, on n'est pas protégé sur BlackBerry. Qui plus est, d'après le site américain Vice, BlackBerry aurait donné sa clef de chiffrement à la police canadienne qui a alors pu intercepter des messages.
À la dernière place, on retrouve Tencent, le mastodonte chinois. L'entreprise accuse un score de 0 point. Aucun des critères n'est rempli et les données personnelles de plus d'un un milliard et demi de personnes ne sont absolument pas protégées, conséquence de la censure que subit l'Internet chinois. En 2013, un développeur de Tencent confiait au journal *Le Monde* , « *Les autorités ont le privilège d'accéder aux historiques, donc elles savent tout sur vous dès lors que vous utilisez nos services*. » Le ton est donné…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

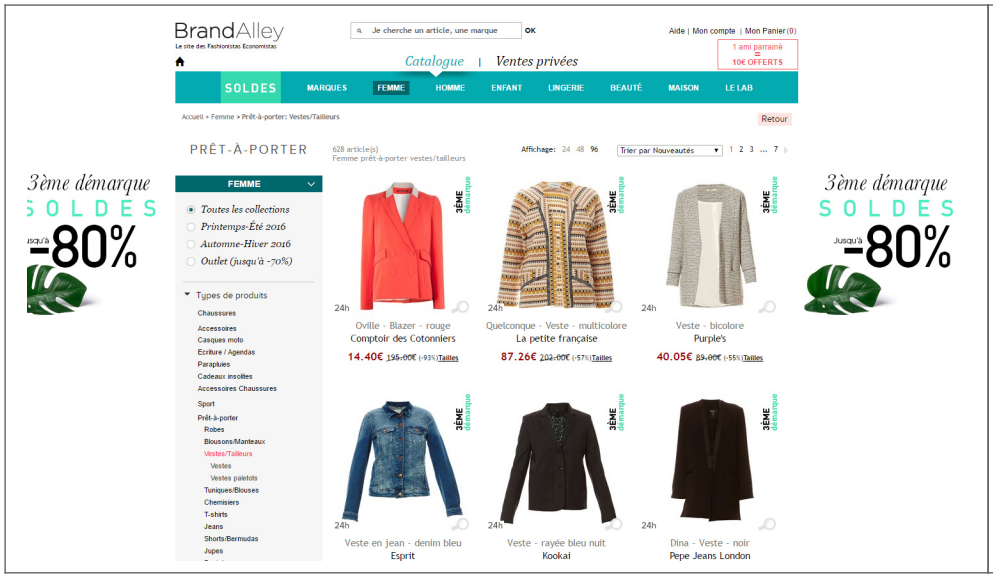
---

Réagissez à cet article

Original de l'article mis en page : Quelles sont les messageries qui protègent le mieux vos données personnelles ? – La Voix du Nord

---

La Cnil s'énerve contre Brandvalley mais la sanction est faible



La Cnil s'énerve contre Brandvalley mais la sanction est faible

La Cnil a dressé un constat sévère de l'irrespect de la loi Informatique et Libertés par le site de ventes privées BrandValley, spécialisé dans les grandes marques. Mais le site qui génère environ 300 millions d'euros de chiffre d'affaires n'a été condamné qu'à 30 000 euros d'amende.…[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** en Cybercriminalité et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **Dangers liés à la Cybercriminalité (Arnaques, Piratages…) pour mieux s'en**

protéger (Autorisation de la Direction du travail de l’Emploi et de la Formation Professionnelle n°93 84 03041 84).
Plus d’informations sur sur cette page.

Réagissez à cet article

Décryptage du réglement européen sur les données personnelles

	Décryptage du réglement européen sur les données personnelles

---

L’Association Française des Correspondants à la protection des Données Personnelles (AFCDP) a réalisé une version française commentée du règlement européen sur les données personnelles. Elle est disponible gratuitement en ligne

A compter du 25 mai 2018, le nouveau Règlement Européen 2019/679 sur la protection des données personnelles s’appliquera dans toutes les entreprises de l’Union Européenne. Ce texte modifie considérablement la législation en vigueur et fait peser des obligations nouvelles sur les responsables de traitements. L’AFCDP (Association française des correspondants à la protection des données personnelles) a réalisé une version française commentée de ce texte.
Le résultat de ce travail est librement accessible sur le site de l’association. Outre une rapide introduction et un index très complet, bien pratique pour retrouver des thèmes précis, l’essentiel du document est constitué par le texte même du Règlement. Les commentaires apparaissent dans une colonne sur le tiers de la page, en regard de la portion commentée. Si parfois, surtout au début, les commentaires se limitent à quelques mots, à d’autres moments ces commentaires explicitent en profondeur et contextualisent un article du Règlement.
Ne nous cachons pas que la simple mise en page du document en français est des plus agréables pour travailler. Les DSI et les directions juridiques ont en effet fort à faire d’ici 2018 et télécharger dès à présent ce document est donc des plus utiles.
Article original de Bertrand Lemaire

Réagissez à cet article