

Que sait de nous Google grâce à nos comportements sur Internet ?



Que sait de nous
Google grâce à
nos comportements
sur Internet ?

Mondialement connu, la firme américaine Google est utilisée par de nombreux internautes, pour son moteur de recherche, mais aussi pour ses nombreux services gratuits (Gmail, Drive, Youtube, Google Maps...). Seul petit hic ? Le revers de la médaille. Puisque Google exploite vos données sans que vous n'en ayez toujours conscience.

Tout le monde connaît Google pour son moteur de recherche ultra-performant. C'est d'ailleurs le moteur préféré des Français. Fin 2016, selon Netbooster, plus de 94 % d'entre eux l'ont utilisé pour effectuer leurs recherches en ligne. Pour apprécier la démesure de ce chiffre, il suffit de voir la part restante à ses principaux concurrents : moins de 4 % pour Bing (Microsoft) et à peine plus de 2 % pour Yahoo.

Plus de 200 services gratuits

À travers sa maison mère « **Alphabet** », Google est l'une des premières capitalisations mondiales avec une valeur de 588 milliards de dollars, juste derrière Apple. La firme de Mountain View n'est pas la seule à analyser les données qui lui parviennent. Tous les géants du secteur (Apple, Amazon, Facebook...) le font en s'appuyant sur les traces que nous laissons chaque jour sur Internet. Ils engrangent des milliards de dollars grâce à ces informations personnelles.

Inutile donc d'être un financier avisé pour comprendre que la seule activité de moteur de recherche ne suffit pas à générer de telles entrées d'argent. Google est une pieuvre géante, dont les tentacules s'étendent dans des domaines aussi nombreux que variés. Le système d'exploitation Android, le navigateur Internet Chrome, les vidéos YouTube, la plateforme de téléchargement Google Play, la cartographie Google Maps, la suite bureautique Google Documents, le site de partage de photos Picasa... Ce sont plus de 200 services proposés gratuitement par l'entreprise. Pour la plupart d'entre eux, la seule contrepartie demandée est l'ouverture d'un compte Gmail, le service de messagerie en ligne maison. L'adresse email et le mot de passe associé deviennent alors vos sésames pour vous identifier et entrer dans la sphère Google, depuis n'importe quel terminal à travers le monde.

— en échange de vos données personnelles

Toute cette gratuité a cependant une face cachée : l'exploitation commerciale de nos données personnelles. En effet, elles représentent une manne financière des plus importante. En acceptant les « **conditions générales d'utilisation** », que nous ne lisons quasiment jamais, nous donnons le droit à Google de tracer et d'utiliser tout ce que nous faisons sur Internet : les sites visités, les achats effectués, les lieux dans lesquels nous nous rendons, les films regardés, les livres lus, la musique écoutée... L'ensemble de ces données est alors analysé par les puissants ordinateurs de la firme, dans le but de créer une sorte de carte d'identité très précise de chaque utilisateur. Ces profils, compilant de très nombreuses données, se revendent à prix d'or aux marques désireuses de cibler au mieux leur publicité. C'est ce que l'on appelle le « **Big Data** ».

Pour profiter gratuitement des services de Google, comme ceux de nombreux autres acteurs des nouvelles technologies, nous devons donc rogner sur notre vie privée, en abandonnant la confidentialité de nos données personnelles. Il existe une formule qui résume parfaitement cette pratique : « **si c'est gratuit, c'est que le produit c'est vous !** »[\[lire la suite\]](#)

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°53 84 030451 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis JACOPINO est Expert Judiciaire en Informatique spécialisée en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audit Sécurité (ISO 27001) ;
- Expertises techniques et judiciaires (Avis techniques, recherche de preuves numériques, données clés, e-mails, contenus, documents de clients...) ;
- Expertises de systèmes de vote électronique ;
- Formation et conférences de cybersécurité ;
- Formation à la protection des données (RGPD) ;
- Formation de CIL (Correspondant Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Le Net Expert
INFORMATIQUE
Cybersécurité & Conformité

[Contact@lenetexpert.fr](mailto:contact@lenetexpert.fr)

Réagissez à cet article

Source : *Données personnelles. Voici ce que Google sait de vous*

Que fait Auchan avec notre ticket de caisse ?



Que fait Auchan avec notre ticket de caisse ?

Anticipation de pénurie, état des stocks, performance des zones commerciales... rien n'échappe aux caisses connectées du groupe nordiste.

Nos tickets de caisse sont des mines d'informations! Si on imagine d'emblée qu'une connaissance précise de notre consommation individuelle, destinée à proposer des offres ciblées, constitue un graal pour les Carrefour, Leclerc et consorts, ce n'est pas forcément l'intérêt premier qu'y voient les professionnels de la grande distribution.

Ainsi, pour le groupe Auchan, c'est d'abord à un juste réapprovisionnement des rayons que servent les informations enregistrées par les 7.000 caisses connectées de ses hypermarchés. Remontées en temps réel vers la base de données installée par l'Américain Teradata en région lyonnaise, les données de nos facturettes nourrissent ensuite une appli développée en interne par les services informatiques du groupe détenu par la famille Mulliez. Dès lors, les salariés peuvent connaître en temps réel l'état de leur rayon par produit, au sein de chaque magasin. Ainsi, le responsable du rayon boissons non-alcoolisées peut, grâce à une icône, savoir si son rayon manque partiellement d'une référence ou, selon le jargon maison, s'il est « fantôme », c'est-à-dire vide.

« Pour certains rayons, tels que les sandwiches entre 12h et 14h, c'est anticipable. L'intérêt est donc pour nous de détecter d'autres comportements du consommateur qu'on ne peut prévoir... Un rayon peut être dévalisé en un rien de temps par une personne ou un groupe de personnes, de façon imprévisible ou bien en fonction d'une promotion. En ce sens, l'application peut fournir une information utile au chef de gondole », estime Eric Dewilde, directeur architecture et données au sein du groupe Auchan. Parce que rien ne vaut l'œil humain, les salariés utilisateurs de l'appli sont amenés à faire un retour d'expérience pour dire si le réassort est en cours ou s'il s'agit d'une fausse alerte. « Nous sommes en phase de rodage. En outre, on n'envoie pas de « push » pour signifier que le rayon se vide. Le principe est de délivrer une information, pas un ordre », précise-t-on au sein d'Auchan...[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Source : *Ce qu'Auchan fait vraiment de nos tickets de caisse*
– *Challenges.fr*

Comment se protéger du smishing ?



Comment se
protéger
du smishing
?

Pour rappel Smishing est la contraction de SMS et de Phishing. On l'appelle également Hameçonnage par SMS.

Lorsque vous utilisez votre téléphone, appliquez des précautions de base, par exemple :

- Ne cliquez pas sur les liens que vous recevez sur le téléphone sauf si vous connaissez la personne qui vous les envoie.
- Même dans ce cas, si vous recevez d'un ami un SMS contenant un lien, avant de cliquer sur ce lien, assurez-vous que cet ami vous l'a bien envoyé.
- Les suites complètes de sécurité Internet ne sont pas réservées aux ordinateurs portables et aux PC. Elles trouvent également toute leur utilité sur votre téléphone mobile.
- Un VPN est également une possibilité à envisager pour vos appareils mobiles. Le VPN sécurisera et cryptera toutes les communications intervenant entre votre mobile et Internet.
- N'installez jamais d'applications à partir de SMS. Vous ne devez installer sur votre appareil que des applications en provenance directe de l'app store officiel. Ces programmes ont été testés de manière rigoureuse avant d'être autorisés sur le marché.
- Pratiquez le principe de précaution. En cas de doute sur la sécurité d'un SMS, ne l'ouvrez pas.

La quasi totalité des SMS que vous recevez est sans problèmes. Mais il suffit d'un mauvais SMS pour totalement compromettre votre sécurité. Un peu de bon sens vous évitera de vous faire dérober votre identité.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel. Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRIEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Source : *Qu'est-ce que le smishing ?*

Qu'est ce que le Smishing ?

Denis JACOPINI



Qu'est ce que le
Smishing ?

Smishing est la contraction de SMS et de Phishing. On l'appelle également Hameçonnage par SMS.

Tout comme le phishing, un message à caractère urgent est envoyé à un utilisateur pour qu'il entreprenne une action. Lors d'un Smishing, c'est un message texte qui est envoyé à un utilisateur sur son téléphone. Le texte du message demande généralement à l'utilisateur d'appeler un numéro de téléphone ou de se rendre sur un site Internet pour effectuer une action précise. La plupart du temps, lorsque vous composez ce numéro de téléphone, vous êtes automatiquement redirigé vers un serveur vocal interactif. Il est demandé à l'utilisateur de fournir des informations personnelles (mot de passe) ou bancaires (numéro de carte bancaire).

Souvent, cette forme de phishing implique un message de texte dans un SMS ou dans un numéro de téléphone. Le numéro de téléphone comporte un message automatisé à partir duquel vos informations commencent à être réellement recueillies. Ce qui rend particulièrement effrayant le smishing, c'est que l'on a plutôt tendance à faire confiance à un SMS qu'à un e-mail. La plupart des gens sont conscients des risques encourus pour la sécurité lorsqu'on clique sur des liens contenus dans des e-mails. Mais c'est moins le cas lorsqu'il s'agit de SMS.

Ne cliquez jamais sur les liens contenus dans ces messages et ne rappelez jamais ces numéros.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

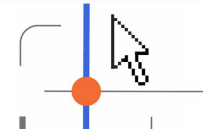


[Contactez-nous](#)



Réagissez à cet article

Les présidentielles ne seront pas affectées par une cyberattaque

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
 LE NET EXPERT AUDITS & EXPERTISES	 LE NET EXPERT EXPERTISES DE SYSTÈMES DE VOTES ÉLECTRONIQUES	 LE NET EXPERT MISES EN CONFORMITÉ	 SPY DETECTION Services de détection de logiciels espions	 LE NET EXPERT FORMATIONS	 LE NET EXPERT ARNAQUES & PIRATAGES
			Les résultats des présidentielles ne seront pas affectés par une cyberattaque		

Le directeur de l'agence nationale de la sécurité des systèmes d'information a tenu à se montrer rassurant sur la solidité du système informatique qui sera utilisé lors de l'élection présidentielle pour collecter et remonter le vote des Français, alors que des craintes de piratage subsistent.



À quelques jours du premier tour de l'élection présidentielle française, faut-il craindre des résultats faussés par une attaque informatique venue de l'étranger pour favoriser tel ou tel candidat, ou au contraire nuire à l'un d'entre eux ? Cette perspective tout à fait inquiétante pour le bon fonctionnement de la démocratie est prise très sérieusement à Paris, surtout depuis les incidents qui ont émaillé la campagne électorale américaine.



Guillaume Poupard

Mais pour Guillaume Poupard, directeur général de l'agence nationale de la sécurité des systèmes d'information (Anssi), il n'y a pas de raison de s'alarmer outre mesure. Si des menaces planent effectivement sur le scrutin, des mesures ont été prises tout au long de ces derniers mois pour éviter un scénario à l'américaine. Ou en tout cas en réduire la portée et la probabilité.

« Le réseau propre du ministère de l'intérieur va être robuste pour être capable de travailler », a-t-il confié jeudi 20 avril au micro de France Inter. « On a fait un travail de qualité, je pense, de manière à résister à ces nouvelles menaces » qui pourraient fausser la sincérité du vote. Tous les maillons de la chaîne informatique servant au processus ont ainsi été renforcés lorsque cela s'est avéré nécessaire.

« Tous les réseaux informatiques qui vont notamment collecter les résultats, qui vont les additionner, pour au final donner dimanche soir les premières tendances puis les résultats définitifs, ces réseaux ont été durcis là où il le fallait », a insisté M. Poupard. Et d'ajouter « [qu'on s'est] assuré que les autres réseaux informatiques qui vont être impliqués dans l'élection seront bien opérationnels le jour de l'élection »...[lire la suite]

[block id="24761" title="Pied de page HAUT"]

A Lire aussi :

- Nouveautés dans l'organisation des votes électroniques pour les élections professionnelles
- 3 points à retenir pour vos élections par Vote électronique
- Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique
- Modalités de recours au vote électronique pour les Entreprises
- L'Expert Informatique obligatoire pour valider les systèmes de vote électronique
- Dispositif de vote électronique : que faire ?
- La CNIL sanctionne un employeur pour défaut de sécurité du vote électronique pendant une élection professionnelle
- Notre sélection d'articles sur le vote électronique

Vous souhaitez organiser des élections par voie électronique ? Cliquez ici pour une demande de chiffrage d'Expertise



Vos expertises seront réalisées par Denis JACOPINI :

- Expert en Informatique **assermenté et indépendant** ;
- spécialisé dans la sécurité** (diplômé en cybercriminalité et certifié en Analyse de risques sur les Systèmes d'Information « ISO 27005 Risk Manager ») ;
- ayant suivi la **formation délivrée par la CNIL sur le vote électronique** ;
- qui n'a **aucun accord ni intérêt financier** avec les sociétés qui créent des solutions de vote électronique ;
- et possède une expérience dans l'analyse de nombreux systèmes de vote de prestataires différents.

Denis JACOPINI ainsi respecte l'ensemble des conditions recommandées dans la Délégation de la CNIL n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.

Son expérience dans l'expertise de systèmes de votes électroniques, son indépendance et sa qualification en sécurité informatique (ISO 27005 et cybercriminalité) vous apporte l'assurance d'une qualité dans ses rapports d'expertises, d'une rigueur dans ses audits et d'une impartialité et neutralité dans ses positions vis à vis des solutions de votes électroniques.

Correspondant Informatique et Libertés jusqu'en mai 2018 et depuis Délégué à La Protection des Données, nous pouvons également vous accompagner dans vos démarches de mise en conformité avec le RGPD (Règlement Général sur la Protection des Données).

Contactez-nous

Source : *Présidentielle : l'Anssi assure que les résultats ne seront pas affectés par une cyberattaque – Politique – Numerama*

Est-ce légal de vendre des

ordinateurs avec des logiciels préinstallés ?

 Denis JACOPINI vous informe LCI	Est-ce légal de vendre des ordinateurs avec des logiciels préinstallés ?
---	---

Vente d'ordinateurs avec logiciels préinstallés : absence de pratique commerciale déloyale

Par un arrêt du **29 mars 2017**, la Cour de cassation a confirmé l'arrêt de la Cour d'appel de Versailles qui avait condamné, pour pratique commerciale trompeuse, une société qui commercialisait des ordinateurs avec logiciels préinstallés sans indiquer aux consommateurs les conditions d'utilisation de ces logiciels ainsi que leurs caractéristiques principales. En revanche, la Cour a confirmé que « *la vente d'un ordinateur équipé de logiciels préinstallés sans possibilité pour le consommateur de se procurer le même modèle d'ordinateur non équipé de logiciels préinstallés ne constitu[ait] pas, en tant que telle, une pratique commerciale déloyale* ». A cette occasion, elle a rappelé qu'une pratique commerciale n'était trompeuse que si elle omettait une information substantielle, or, selon la Cour, le prix de chacun des logiciels et la possibilité d'acquérir un ordinateur non équipé de logiciels ne constituent pas de telles informations.

Pour lire l'arrêt sur Légifrance

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur
: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Source : *Toute l'Actualité juridique des DSI*

Les données de santé des Français désormais en libre accès



Les
données
de santé
des
Français
désormais
en libre
accès

Dans un communiqué du 10 avril 2017, le gouvernement a indiqué qu'il ouvrirait l'accès aux données issues du Système national des données de santé (SNDS) aux organismes exerçant une mission de service public pour toute étude, recherche et évaluation présentant un intérêt public. Ces organismes peuvent désormais consulter et exploiter les données du SNDS suivant certaines conditions détaillées dans le décret du 26 décembre 2016.

Ainsi, comme le précise le gouvernement :

- L'État, l'Assurance maladie, l'Agence nationale de sécurité du médicament et des produits de santé (ANSM), la Haute Autorité de santé (HAS) ou encore Santé publique France peuvent accéder aux données du SNDS de manière permanente pour leur permettre d'assumer leurs missions
- Les équipes de recherche des centres hospitaliers universitaires (CHU), de l'Institut national de la santé et de la recherche médicale (INSERM) et des centres de lutte contre le cancer peuvent désormais consulter l'échantillon correspondant à 1/100ème de la population.
- Les autres organismes publics ou privés, à but lucratif ou non lucratif, auront eux aussi prochainement accès aux données issues de cette base pour toute étude, recherche et évaluation présentant un intérêt public. Ils seront, eux-aussi, soumis aux conditions précisées dans le décret du 26 décembre 2016

La loi interdit l'usage de ces informations pour deux finalités :

- La promotion commerciale des produits d'assurance santé
- La modulation des contrats d'assurance santé (évolution des primes, exclusions,...)

Toutefois, cette annonce suscite des craintes et la réprobation, notamment chez certains acteurs de la santé.

Ainsi, la Fédération des Médecins de France – syndicat qui regroupe près de 3000 adhérents – s'oppose à cette mesure. « Si la loi autorise des accès à cette vaste base de données au nom de la recherche et annonce la future possibilité à des entreprises lucratives de pouvoir y accéder également, la FMF rappelle que les données du SNDS ne seront pas anonymisées mais seulement pseudonymisées avec une possibilité d'identification. » explique le syndicat dans un communiqué.

La FMF alerte :

– du risque élevé de perte de confidentialité de leurs données personnelles, soit en raison du piratage, soit en raison du nombre élevé de personnes potentiellement concernées par l'accès aux données du SNDS. La CNIL elle-même a estimé que « le niveau de sécurité envisagé ne sera pas atteint au lancement du traitement SNDS en mars 2017 »[1]. Bien que la loi prévoie un agrément très sévère pour les hébergeurs de données de santé, les mini serveurs de données, de radiologie ou de biologie, permettant un accès rapide aux résultats, ne sont pas tous agréés, et leur accès est très modérément protégé...[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus

d'informations

sur

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)



Réagissez à cet article

Source : *Les données de santé des Français désormais en accès libre* –

Protection des données : ce qui va changer pour les entreprises en 2018



En mai 2018, un règlement européen va entraîner d'importants changements dans la pratique des entreprises en matière de gestion des données personnelles. En quoi consistent ces changements et comment s'y préparer ?

Protection des données : ce que prévoit le règlement européen de 2016

Contrairement à une directive, le règlement européen, adopté en 2016, est directement applicable dans l'ensemble de l'Union européenne sans nécessiter de transposition dans les différents Etats membres et ce à partir du 25 mai 2018. Il concerne toutes les entreprises utilisant des données personnelles.

Ainsi, à cette date, les responsables de traitement devront s'être mis en conformité avec le règlement sous peine de sanctions.

Principal changement :

Ce règlement marque le passage d'une logique de « formalités préalables » (déclarations, autorisations) à une logique de « conformité » dont les acteurs seront responsables sous le contrôle du régulateur (la CNIL en France). Ainsi, les responsables de traitements de données n'auront plus à effectuer de déclarations à la CNIL dès lors que les traitements ne constituent pas un risque pour la vie privée des personnes.

Par contre, ils devront d'entrée mettre en œuvre toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données personnelles. Concrètement, ils devront veiller à limiter la quantité de données traitée dès le départ (principe dit de « minimisation »). Ils devront également être capables de démontrer cette conformité à tout moment.

✖	✖ ✖	✖
✖	Pour les traitements à risque, il faudra toutefois conduire une étude d'impact complète faisant apparaître les caractéristiques du traitement, les risques et les mesures adoptées. Cela concerne notamment les données sensibles qui révèlent l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, les données concernant la santé ou l'orientation sexuelle, mais aussi les données génétiques ou biométriques. En cas de risque élevé, il faudra consulter la CNIL avant de mettre en œuvre ce traitement, cette dernière pouvant décider de s'y opposer.	✖
✖		✖

Ce règlement renforce par ailleurs les droits des personnes. En effet, chaque personne concernée par les traitements de données va avoir le droit à la mise à disposition d'une information claire, intelligible et aisément accessible et va devoir donner son accord pour le traitement des données. La preuve de ce consentement incombant au responsable de traitement.

Protection des données : mise en place des délégués à la protection des données

Le règlement européen instaure des délégués à la protection des données (DPD). Ce seront les successeurs des correspondants informatique et libertés (CIL) dont plus de 17 700 organismes sont d'ores et déjà dotés en France et dont la mise en place permet de se dispenser de certaines déclarations.

A la différence du CIL, dont la désignation est actuellement optionnelle, la désignation du DPD est obligatoire dans le secteur public et pour les responsables de traitement et les sous-traitants dont les activités principales les amènent :

- à réaliser un suivi régulier et systématique des personnes à grande échelle ;
- à traiter (toujours à grande échelle) des données dites « sensibles » ou relatives à des condamnations pénales et infractions.

Pour les autres, leur désignation est facultative...[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » et « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation de la DRTF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Contactez-nous



Réagissez à cet article

Source : *Protection des données : ce qui va changer pour les entreprises – Editions Tissot*

Le Bitcoin n'est pas la seule monnaie virtuelle



Le
Bitcoin
n'est pas
la seule
monnaie
virtuelle

La plus connue des crypto-monnaies, le Bitcoin, est valorisée en bourse à 19,4 milliards de dollars. Ces monnaies électroniques n'ont plus rien de virtuelles. Classement.

Coinmarketcap.com a réalisé le classement des crypto-monnaies en fonction de leur valorisation boursière. Sans surprise, le Bitcoin arrive en tête avec une capitalisation boursière de 19,4 milliards de dollars en avril. Viennent ensuite l'Ethereum, une chaîne de bloc lancée en 2015 qui utilise l'Ether comme moyen de paiement, valorisée à 3,9 milliards de dollars. Puis, le Ripple à 1,2 milliard de dollars. Pour se différencier du Bitcoin, nombre d'autres monnaies cryptographiques mettent en avant un anonymat total, là où il n'est que partiel chez Bitcoin.

1. Bitcoin

Lancement : 2009

Capitalisation boursière au 10 avril 2017 : 19,4 milliards de dollars

Fonctionnement du Bitcoin : transfert d'argent entre personnes sur internet.

2. Ethereum

Lancement : 2015

Capitalisation boursière en avril 2017 : 3,9 milliards de dollars

Fonctionnement : l'Ethereum est le protocole d'échange décentralisé, l'Ether est son unité de compte et moyen de paiement.

3. Ripple

Lancement : 2012

Capitalisation boursière en avril 2017 : 1,2 milliard de dollars

Fonctionnement de Ripple : à la fois système de règlement brut réel, marché des changes et réseau d'envois de fonds.

4. Litecoin

Lancement : 2011

Capitalisation boursière en avril 2017 : 449, 8 millions de dollars

Fonctionnement : comme Bitcoin, elle fonctionne sous licence libre, le code du Litecoin est une modification du code Bitcoin.

5. Dash

Lancement : 2014

Capitalisation boursière en avril 2017 : 443,6 millions de dollars

Fonctionnement : mot valise de digital et cash. Ex Darkoin, elle veut s'affranchir des limitations du Bitcoin et promet l'anonymat.

6. Monero

Lancement : 2014

Capitalisation boursière en avril 2017 : 304,5 millions de dollars

Fonctionnement : se dit totalement anonyme, contrairement aux autres crypto-monnaies qui sont des clones de Bitcoin, Monero repose sur un fonctionnement cryptographique différent, et utilise des signatures en cercle. Un utilisateur ne peut connaître le contenu ni l'historique des transactions.

7. Ethereum Classic

Capitalisation boursière en avril 2017 : 234 millions de dollars

Fonctionnement : à la différence de l'Ethereum, l'Ethereum classic est "unstoppable".

8. NEM

Lancement : 2015

Capitalisation boursière en avril 2017 : 186,6 millions de dollars

Fonctionnement : Nem pour New Economic Movement. Sa monnaie est le Xem. Nem réécrit le code de zéro.

9. Augur

Capitalisation boursière en avril 2017 : 104 millions de dollars

10. MadeSafeCoin

Capitalisation boursière en avril 2017 : 88, 5 millions de dollars

[Plus d'infos sur l'article de Forbes]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité », « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRETF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Réagissez à cet article

Source : *Bitcoin, Ethereum, Ripple, classement des cryptomonnaies dans le monde*

Est-ce que Linky aspire nos données personnelles ?



Linky, un compteur qui ne vous veut pas que du bien ! Ce boîtier qui doit être installé dans tous les foyers relèvera en direct et à distance vos habitudes de consommation d'électricité.

Par ailleurs, des incidents ont lieu lors de la pose de ces compteurs, notamment lorsque des personnes s'y opposent : à Plouha et dans sa région récemment, plusieurs incidents ont été constatés, avec notamment une dame de 73 ans bousculée par un installateur alors qu'elle s'opposait à l'installation.

Avec le prétexte d'établir une facture plus précise, EDF prévoit de remplacer 90% des anciens compteurs en 4 ans. Un changement qui suscite de vives polémiques. En effet, de nombreuses communes s'opposent à l'installation de ce compteur dit intelligent. Si l'efficacité et le risque de surcoût sont remis en question, la menace d'intrusion dans la vie privée est également pointée du doigt.

En effet, par son système de collecte de données à distance, le compteur Linky est un véritable concentré d'informations personnelles. Il est techniquement capable de recueillir les index journaliers et la courbe de charge, c'est-à-dire un relevé précis de la consommation électrique de l'utilisateur. Ces données permettent de déduire des informations sur les habitudes de vie des consommateurs.

Des millions de Français seront concernés et des millions de données personnelles seront stockées par ERDF, qui souhaite entrer dans la danse du commerce d'informations, le Big Data. Pas étonnant, car cette mine d'or peut rapporter très gros. En effet, elle fait l'objet d'un véritable business, estimé à plusieurs milliers de milliards d'euros...[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Source : *Linky, vendeur de données personnelles* –