

Les PME , dépassées par l'arrivée du RGPD ?



Le Règlement Général sur la Protection des Données (GDPR) dont sa application est déjà prévue pour le 25 mai 2018, laisse aux entreprises un peu plus d'une année pour se conformer. Cependant, elles semblent toutefois avoir du mal à lancer les projets adaptés pour assurer leur conformité à ce nouveau Règlement.

Au moins c'est la conclusion principale du dernier rapport mené par IDC selon lequel **Sur les 700 entreprises interrogées, 77% des décideurs informatiques ne sont pas conscients de l'impact du RGPD sur l'activité de leur entreprise ou n'ont même pas connaissance de ce règlement.** Parmi celles qui connaissent le RGPD, 20% affirment y être déjà conformes, 59% travaillent à l'être et 21% avouent ne pas du tout être préparés.

« La protection des données à caractère personnel des clients et partenaires est primordiale pour les entreprises. Elles doivent prendre conscience de la valeur que représentent ces informations et mettre en place des mesures adaptées pour répondre aux obligations du RGPD. », explique Mark CHILD, Research Manager chez IDC. Dans ce sens, **les petites et moyennes entreprises reconnaissent que leur logiciel anti-malware est insuffisant dans l'environnement de menace actuel**, et la moitié des répondants ont avoué que ce point était le plus important à améliorer...[lire la suite]

A Lire aussi :

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016

Le RGPD, règlement européen de protection des données. Comment devenir DPO ?

Comprendre le Règlement Européen sur les données personnelles en 6 dessins

Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Notre métier : Vous accompagner dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits 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.



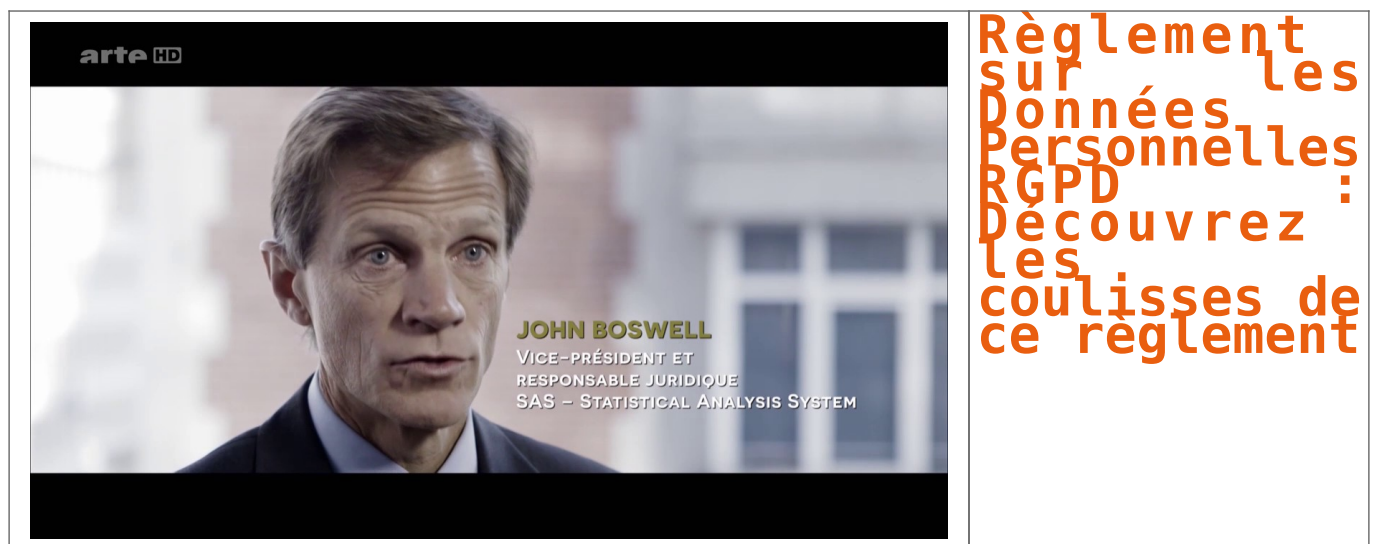
[Contactez-nous](#)



Réagissez à cet article

Source : *Les PME , dépassées par l'arrivée du RGPD ? – Globb Security FR*

Règlement sur les Données Personnelles RGPD : Découvrez les coulisses de ce règlement



Depuis les couloirs du Parlement Européen, chronique de la difficile élaboration d'une nouvelle loi pour la protection des données personnelles, enjeu central opposant les citoyens aux intérêts privés.

Chaque fois que nous faisons nos courses sur Internet, interrogeons un moteur de recherche, activons la géolocalisation sur notre smartphone ou même utilisons notre carte de transport ou de crédit, nous laissons des traces : des masses d'informations personnelles sont collectées sur nos habitudes de consommation, nos goûts, nos déplacements ou nos opinions. Des informations hautement exploitables – et monnayables. Nombreux sont les observateurs à l'affirmer : les données seront le pétrole du XXI^e siècle. Utilisée de manière judicieuse, cette manne offre la promesse de transformer nos vies en profondeur. Mais à quel prix ? Ces données personnelles échappent de plus en plus aux citoyens, au profit des entreprises. Comment nous protéger contre l'utilisation incontrôlée de nos données, garantir notre droit à l'autodétermination et sanctionner les contrevenants ? Selon les lobbies privés, une loi trop draconienne risquerait de faire fuir les entreprises du territoire européen. Mais faut-il pour autant sacrifier la vie privée des citoyens ?

Loi à réformer

Depuis plusieurs années, l'Union européenne travaille à réformer la loi sur la protection des données personnelles. Le jeune député vert européen Jan Philipp Albrecht a notamment pris ce combat à bras-le-corps, en se faisant le rapporteur du Parlement européen sur la réglementation de la protection des données. Ce documentaire suit le parcours complexe de la législation européenne en la matière, en interrogeant des acteurs aux intérêts souvent divergents : politiques, juristes, membres de la société civile ou du monde des affaires.

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

Sur la Protection des données personnelles, les programmes d'Emmanuel Macron et Marine Le Pen sont plutôt faibles



Emmanuel Macron et Marine Le Pen présentent tous les deux des programmes numériques assez parcellaires. On fait le point.

Sur la question de la vie privée des internautes, **Marine Le Pen** propose de « créer une charte à valeur constitutionnelle de protection des données personnelles », sans jamais préciser ce qu'une telle charte pourrait induire pour les citoyens. La candidate frontiste souhaite également mettre en place l'obligation « de stocker les données personnelles des Français sur des serveurs hébergés en France », sans toutefois livrer plus de détails sur les modalités techniques de telles mesures. Seule véritable proposition concrète dans ce dossier : la création de la carte unique biométrique, qu'elle aimerait étendre à la carte vitale afin de lutter contre la fraude, et l'obligation pour les entreprises de stocker en France les données personnelles des citoyens français.

Emmanuel Macron, lui, reste tout autant vague. Il souhaite « développer les instruments d'une transparence sur l'usage des données privées par les acteurs du numérique », mais ne dit pas lesquels. On retrouve le même flou lorsqu'il propose de « bâtir des murailles » et « patrouiller dans le cyberspace » pour faire de la cybersécurité, « une priorité de la sécurité nationale ». L'ancien ministre de l'Économie et des finances va même jusqu'à proposer « une banque de données numériques réutilisables » : « Dans le respect de la vie privée et du secret des affaires, les administrations qui délivrent des licences (par exemple pour les hôtels) devront mettre à disposition leurs données. Face aux géants étrangers, des nouvelles start-up pourront ainsi s'adresser par exemple à tous les hôteliers pour leur offrir une alternative aux services existants ». Et l'ancien banquier d'affaires français de suggérer également « un service public numérique de la justice », avec portail unique d'accès : « Les citoyens et leurs avocats y trouveront toutes les informations pratiques et la jurisprudence applicable à leur cas. Ils pourront se pourvoir en justice depuis leur ordinateur, transmettre une requête, des pièces, ou suivre leur dossier depuis leur smartphone ». Il aimerait également renégocier le « Privacy Shield » d'ici 2018 et créer une « agence européenne pour la confiance numérique » qui serait « chargée de réguler les grandes plateformes numériques »...[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 DRTTEF 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 : Sur le numérique, les programmes d'Emmanuel Macron et Marine Le Pen sont plutôt faibles

Un pirate informatique réclame une rançon pour ne pas dévoiler la prochaine saison de la série Orange Is the New Black



Un pirate informatique réclame une rançon pour ne pas dévoiler la prochaine saison de la série Orange Is the New Black

Un pirate informatique affirme s'être procuré illégalement la prochaine saison de la série de Netflix Orange Is the New Black. Il réclame à la plateforme le paiement d'une rançon pour ne pas dévoiler le contenu des nouveaux épisodes de la fiction à succès.

L'auteur du chantage, qui se fait appeler The Dark Overlord, aurait déjà mis en ligne plusieurs épisodes sur un service de partage de fichiers illégal. The Associated Press n'a pas été en mesure de confirmer l'authenticité des fichiers en question. On ne connaît pas non plus le montant réclamé.

Les nouveaux épisodes de la cinquième saison de la série qui se déroule dans une prison pour femmes doivent être diffusés sur Netflix le 9 juin. La bande-annonce a été dévoilée le 8 février dernier.

Un éventuel piratage de l'une des séries à l'origine de la popularité de Netflix pourrait avoir des conséquences sur le nombre d'abonnés de la plateforme. La valeur financière de l'entreprise pourrait alors se trouver en danger...[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 : *Un pirate informatique réclame une rançon à Netflix | ICI.Radio-Canada.ca*

Allocab condamné par la Cnil

The logo for Allocab, featuring the word "allocab" in a sans-serif font. "allo" is in black and "cab" is in orange. Below it, the tagline "move around your city" is written in a smaller, black, sans-serif font.

allocab
move around your city

Allocab
condamné
par la
Cnil

La police de protection des données personnelles en ligne vient de condamner la société Allocab à verser une amende de 15 000 euros. L'entreprise de VTC aurait mal protégé et conservé certaines données bancaires de ses utilisateurs sans tenir compte des avertissements de la Cnil, dont le verdict est tombé ce 25 avril.

Les données des utilisateurs frauduleusement conservées

La société de VTC (Voiture avec chauffeur) Allocab propose des chauffeurs privés aux utilisateurs de son application. En réponse aux demandes des clients, la Cnil (Commission nationale de l'informatique et des libertés) a effectué un contrôle des activités de la firme dans le cadre de la loi « Informatique et Libertés ». L'enquête a révélé qu'Allocab commettait plusieurs manquements à ce texte : elle rapporte notamment que « des données relatives à des comptes inactifs et des cryptogrammes de cartes bancaires étaient encore présents dans le système d'information et la sécurité des données n'était pas suffisamment assurée » et que les mots de passe à un seul caractère étaient par ailleurs admis, ce qui ne garantit aucune sécurité aux données des utilisateurs. Il ne s'agit pourtant pas du premier faux pas de cette entreprise, déjà sanctionnée en 2015.

Des avertissements ignorés

Le 10 novembre 2015, Allocab se voyait mise en demeure par la Cnil suite à la plainte d'un utilisateur. L'institution ordonnait à l'entreprise de détruire les données des anciens clients et de « prendre toute mesure nécessaire pour garantir la sécurité et la confidentialité des données des utilisateurs du site », notamment en limitant la durée de conservation des cryptogrammes de cartes bancaires et de toutes les données des utilisateurs. Suite à cette première condamnation s'est déroulée une longue correspondance dans laquelle Allocab prétextait des dysfonctionnements techniques et certifiait mettre en place des mesures nécessaires. Ces affirmations ont incité la Cnil à mener un deuxième contrôle. Au cours de cette seconde investigation fin 2016, elle découvre que plusieurs de ses injonctions ne sont pas respectées : de nombreux comptes inactifs existent encore sur la plateforme, tout comme les données et cryptogrammes des cartes bancaires de nombreux utilisateurs.

15 000 euros d'amende

Les fameux dysfonctionnements invoqués par Allocab n'ont pas convaincu la commission, dont un comité restreint l'a condamné le 13 avril dernier au versement d'une amende de 15 000 euros...[lire la suite]

A Lire aussi :

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016

Le RGPD, règlement européen de protection des données. Comment devenir DPO ?

Comprendre le Règlement Européen sur les données personnelles en 6 dessins

Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Notre métier : Vous accompagner dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits 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>



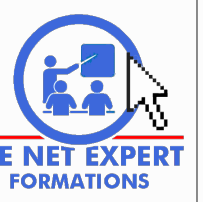
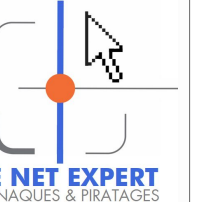
Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- 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.



Réagissez à cet article

Est-ce que le vote électronique des élections Françaises est fiable ?

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
 LE NET EXPERT AUDITS & EXPERTISES	 LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES	 LE NET EXPERT RGPD CYBER MISES EN CONFORMITE	 LE NET EXPERT SPY DETECTION Services de détection de logiciels espions	 LE NET EXPERT FORMATIONS	 LE NET EXPERT ARNAQUES & PIRATAGES
 Denis JACOPINI vous informe		Est-ce que le vote électronique des élections Françaises est fiable ?			

Le vote électronique : nouvelle preuve de manipulation des élites qui peuvent en deux temps trois mouvements truquer les votes comme bon leur semble ...

Pendant les élections Françaises, les scellés appliqués sur la machine à voter et l'expertise des systèmes de votes électroniques réalisées par les experts indépendants respectant les **recommandations de la CNIL dans délibération n° 2010-371 du 21 octobre 2010 relative à la sécurité des systèmes de vote électronique** garantit le respect de l'intégrité et de la confidentialité des scrutins.

[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 Délibération 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.

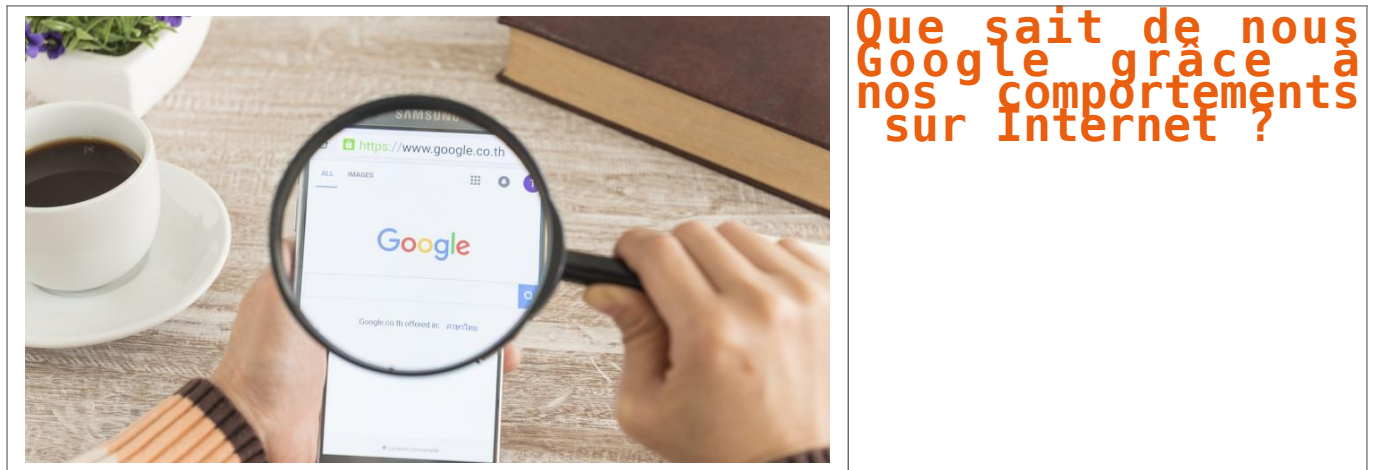
Son expérience dans l'expertise de systèmes de votes électroniques, son indépendance et sa qualification en sécurité Informatique (ISO 27005 et cybercriminalité) vous apporte l'assurance d'une qualité dans ses rapports d'expertises, d'une rigueur dans ses audits et d'une impartialité et neutralité dans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

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



Worldiement 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°13 84 03041 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-mail, 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

Contactez nous

Réagissez à cet article

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

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

Est-ce que Linky aspire nos données personnelles ?



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* –