

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 inexploitable 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 la 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>



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- 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

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

Interrogation des entreprises sur le Règlement européen sur la protection des données



Les entreprises veulent obtenir de la CNIL et du G29 des clarifications sur la responsabilité du délégué à la protection des données (DPO).

La Commission nationale de l'informatique et des libertés (CNIL) a rendu publique lundi la synthèse de contributions proposées lors d'une consultation sur le Règlement européen sur la protection des données (RGPD ou GDPR, en anglais). Rappelons que ce Règlement, qui entrera en vigueur en mai 2018, introduit de nouveaux droits des personnes et des obligations nouvelles pour les entreprises. Le texte renforce également les sanctions administratives à l'encontre des responsables de traitement et des sous-traitants qui ne respecteraient pas les dispositions du texte. Les entreprises et les administrations actives dans l'Union européenne sont toutes concernées, et pas seulement celles qui ont adopté le Cloud. Les professionnels ont été consultés cet été par la CNIL.

225 contributeurs, entreprises et fédérations professionnelles, ont posté plus de 540 contributions, soumises à 994 votes. Quatre premiers thèmes inscrits au plan d'action du G29, le groupe des CNIL européennes, ont été abordés. La mission de délégué à la protection des données inquiète le plus.

CIL, de futurs DPO ?

Un délégué à la protection des données (DPO) est-il responsable pénalement ? Peut-il être licencié pour faute ? Pourra-t-il exercer une autre fonction ? Les interrogations des entreprises sont nombreuses. Elles attendent des clarifications sur la responsabilité, le rôle, les moyens et les missions de ce DPO, qui n'est pas sans rappeler le CIL (correspondant informatique et libertés).

Pour répondre à ces attentes, la CNIL se dit prête à réaliser « des actions de communication auprès des organismes ayant actuellement un CIL, et auprès des fédérations professionnelles concernées par la désignation obligatoire d'un DPO (courriers spécifiques, fiches pratiques) ». Par ailleurs, les ateliers CIL seront enrichis (format, volume et contenus), a fait savoir le régulateur français.

Selon les prévisions de l'IAPP (International Association of Privacy Professionals), 75 000 postes de DPO seront à pourvoir dans le monde, dont au moins 28 000 en Europe et aux États-Unis. Le but : répondre présent dès le lancement du Règlement européen sur la protection des données.

Portabilité mal perçue

Le droit à la portabilité permet à une personne de récupérer des données à caractère personnel, sous une forme aisément réutilisable, et, si elle le souhaite, de les transférer à un tiers. Les entreprises y voient l'occasion de « redonner confiance au client dans l'exploitation qu'elles font de ses données ». Mais elles s'interrogent aussi beaucoup sur le coût et le périmètre réel de ce nouveau droit, qu'elles souhaitent « limiter au strict minimum », selon la CNIL.

Le groupe technologie du G29, de son côté, planche sur un avis visant à clarifier ce périmètre, « en fonction duquel les actions à mettre en oeuvre pourront être définies ». À préciser, par conséquent.

Certification et labellisation

Le Règlement européen encourage aussi la mise en place de mécanismes de certification et de labels de protection des données. La délivrance de ces labels pourra être réalisée par le régulateur ou des organismes de certification accrédités. Les entreprises y sont plutôt favorables, à la condition que le cadre européen garantisse « un niveau élevé et homogène des normes utilisées ». Et les PME ne veulent pas de processus coûteux et complexes de certification ou labellisation. Les attentes des CIL, organismes et fédérations professionnelles sont fortes dans ce domaine. La CNIL, en plus d'actions déjà menées à leur attention, leur proposera de nouveaux supports et outils didactiques...[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 la 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>



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- 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

Original de l'article mis en page : Règlement européen sur la protection des données : les entreprises s'interrogent

Des téléphones Android espions ?

Des téléphones Android espions ?

Vous être l'heureux propriétaire d'un smartphone tournant sous Android acheté pas trop cher ? Vos SMS, vos contacts, la liste de vos appels téléphoniques ou encore vos données de déplacement sont peut-être en train d'être analysés à Pékin....[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.



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

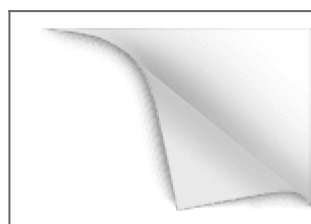
- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Intel Security promeut l'union face au cybercrime



Intel Security promeut l'union face au cybercrime

Intel Security a présenté de nombreux nouveaux produits dans toutes ses gammes. « Il y a trois fois plus d'innovations à cette conférence que dans les trois précédentes éditions réunies », constate Fabien Rech, directeur général France....[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.



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- 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

BlackNurse : un déni de

service à bas volume ciblant les firewalls



C'est une attaque au parfum franchement vintage mais à l'efficacité redoutable....[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.



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- 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

Contrôles biométriques en entreprise : vos obligations changent !



**Contrôles
biométriques
en entreprise
: vos
obligations
changent !**

Le cadre légal régit la mise en place de dispositifs biométriques en entreprise évolue. En effet, la Cnil a adopté le 30 juin 2016, suite aux exigences fixées par le règlement européen sur la protection des données personnelles (2), 2 autorisations uniques, publiées au Journal officiel le 27 septembre 2016.

Ces autorisations uniques fixent un nouveau cadre légal afin d'encadrer le recours aux dispositifs biométriques et protéger au mieux les libertés individuelles des personnes concernées par de tels systèmes d'identification. Ainsi, les entreprises ayant recours à la mise en place de dispositifs biométriques ne seront plus soumises à une autorisation préalable de la Cnil. Elles devront simplement réaliser une demande d'autorisation unique et se conformer aux obligations prévues par l'autorisation.

La Cnil distingue désormais 2 types de dispositifs :

1/ L'autorisation unique 052 (3) pour les dispositifs garantissant la maîtrise par la personne concernée sur son gabarit biométrique. Ce peut être soit :
– un système recourant au stockage des données biométriques sur un support individuel détenu par les personnes concernées ;
– si la détention d'un support dédié au seul stockage du gabarit n'est pas adaptée à l'architecture et au contexte d'exploitation du dispositif, le responsable du traitement peut, de manière alternative, assurer le verrouillage des données biométriques stockées en base, par un secret détenu uniquement par la personne concernée ;
Dans ces deux hypothèses, l'utilisation du gabarit biométrique est conditionnée à une action de la personne concernée en tant que détentrice du gabarit ou du secret permettant de le déverrouiller.

2/ L'autorisation unique 053 (4) pour les dispositifs reposant sur une conservation des gabarits en base par le responsable du traitement.

Un « gabarit » biométrique désigne les mesures qui sont mémorisées lors de l'enregistrement des caractéristiques morphologiques, biologiques ou comportementales de la personne concernée.

Ainsi, à chaque demande d'autorisation unique visant à mettre en place un dispositif biométrique dans leur entreprise, les dirigeants doivent se conformer à certaines exigences :

- justifier de la nécessité et de la pertinence d'avoir recours à un dispositif biométrique. Le recours à ce dernier ne doit pas avoir pour effet de se substituer à des dispositifs non biométriques ;
- privilégier les dispositifs biométriques qui garantissent aux personnes concernées la maîtrise de leur gabarit ;
- justifier et garantir la protection et la conservation des gabarits en base ;
- prendre toute mesure permettant de limiter les risques d'atteinte à la vie privée.

Si vous avez mis en place un dispositif biométrique sous couvert de l'ancien cadre légal, vous devez vérifier s'il répond à ces nouvelles exigences :

- si c'est le cas : un engagement de conformité à l'une de ces nouvelles autorisations peut être réalisé ;
- si ce n'est pas le cas : vous avez 2 ans pour vous mettre en conformité.

Zans pour être en conformité

Si vous ne vous êtes pas mis en conformité d'ici la fin de ce délai, sachez néanmoins que la Cnil pourra à tout moment contrôler que le dispositif de biométrie mis en place dans votre entreprise répond aux obligations imposées par les nouvelles autorisations uniques.

Références :

- (1) Article 25 de la Loi n°78-17 du 6 janvier 1978 modifiée, modifié par la Loi n°2016-1321 du 7 octobre 2016 pour une République numérique
- (2) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE)
- (3) Délibération n°2016-186 du 30 juin 2016 portant autorisation unique de mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail et garantissant la maîtrise par la personne concernée sur son gabarit biométrique (AU-052)
- (4) Délibération n°2016-187 du 30 juin 2016 portant autorisation unique de mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail, reposant sur une conservation des gabarits en base par le responsable du traitement (AU-053)–[Article source et complet]

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 la 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>



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphoniques, disques durs, e-mails, contenus, débrouchements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- 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

Original de l'article mis en page : Contrôles biométriques en entreprise : vos obligations changent !

Comment pirater des codes PIN en sniffant le WiFi des smartphones ?



Comment
pirater des
codes PIN
en sniffant
le WiFi des
smartphones
?

Des chercheurs peuvent récupérer des données sensibles en se basant sur les perturbations du signal WiFi lors des frappes sur l'écran.

Quand un utilisateur déplace ses doigts sur l'écran tactile de son téléphone, il perturbe le signal WiFi émis par son terminal. Ces interruptions peuvent être interceptées par un pirate, analysées et en appliquant de la rétro-ingénierie deviner quelle sont les frappes saisies sur le téléphone ou dans les champs de saisie de mot de passe.

Ce type d'attaque est nommé WindTalker (messenger du vent), par des chercheurs chinois et elle n'est possible que si le pirate contrôle le point d'accès WiFi (un hotspot par exemple dans un rayon de 1,5 mètre) afin de collecter les perturbations du signal WiFi. Un contrôle impératif pour analyser le trafic et savoir quand l'utilisateur accède à des pages nécessitant une authentification.

Le CSI en ligne de mire

Si l'attaque semble issue du domaine de la science-fiction, cette menace se sert du CSI (Channel State Information), un composant du protocole WiFi chargé de fournir les informations générales sur l'état du signal WiFi. Quand l'utilisateur tape du texte sur l'écran, sa main modifie les propriétés de CSI du signal WiFi sortant et la modification peut être captée par un point d'accès malveillant.

Dans une démonstration exposée lors de la ACM Conference on Computer and Communications Security à Vienne, les chercheurs ont montré qu'en réalisant une analyse et un traitement basique du signal, un pirate peut avoir accès aux signaux CSI perturbés et deviner avec une précision moyenne de 68,3% les caractères qu'un utilisateur a tapé. La précision de WindTalker est différente selon les modèles de smartphones et elle peut être améliorée avec le niveau de données collectées...[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 la 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>



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- 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

Original de l'article mis en page : WindTalker : pirater des

Les bases de données désormais aussi touchées par les Ransomwares



Cerber n'en finit pas d'évoluer en se tournant maintenant vers les bases de données des entreprises. Un marché particulièrement lucratif.

Un des ransomwares les plus célèbres, Cerber, a commencé à s'en prendre aux bases de données, précise McAfee. Les cybercriminels derrière ce malware ont élaboré un module ciblant notamment les entreprises. Auparavant, Cerber se focalisait sur le grand public avec un beau palmarès : environ 160 campagnes en juillet dernier visant 150 000 personnes pour une rançon totale de 195 000 dollars en un mois. Etant dans un modèle de partage de revenus, le développeur de Cerber a empoché 78 000 dollars en un mois. Un retour sur investissement qui aiguise les appétits...[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 la 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>



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- 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

Original de l'article mis en page : Le ransomware Cerber chasse les bases de données des entreprises

Piratage de Yahoo : des employés savaient dès 2014



Dès 2014, des employés de Yahoo savaient que leur entreprise avait été victime d'un piratage sophistiqué mené par un hacker téléguidé par un Etat étranger...[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.



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- 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

Piratage de Yahoo : des employés savaient dès 2014



Dès 2014, des employés de Yahoo savaient que leur entreprise avait été victime d'un piratage sophistiqué mené par un hacker téléguidé par un Etat étranger...[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.



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- 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