

# La webcam, Est-ce une vraie menace pour les utilisateurs d'ordinateurs

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

**LE NET EXPERT**  
AUDITS & EXPERTISES

**EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES**  
**LENETEXPERT**.fr

**RGPD CYBER**

**SPY DETECTION**  
Services de détection de logiciels espions

**LE NET EXPERT**  
MISES EN CONFORMITE

**LE NET EXPERT**  
FORMATIONS

**LE NET EXPERT**  
ARNAQUES & PIRATAGES

**La webcam, est-ce une vraie menace pour les utilisateurs d'ordinateurs**

Après Mark Zuckerberg et sa webcam masquée par du scotch, voilà que c'est le directeur du FBI, James Comey, qui admet avoir adopté le même réflexe.

#### Une webcam cachée pour s'éviter bien des ennemis

A l'heure où les hackers multiplient les attaques contre les machines des entreprises et des particuliers, beaucoup se sont moqués de Mark Zuckerberg et de son bout de scotch sur la webcam et sur la prise jack, certains allant même jusqu'à le traiter de « parano ». Pourtant, il semblerait qu'il s'agisse d'un réflexe à prendre et ce pour tout le monde. En effet, un pirate talentueux peut assez simplement prendre le contrôle d'une webcam à distance et pousser ainsi l'utilisateur à télécharger un malware sur sa machine. Aussi, lors d'une interview, James Comey, le directeur du FBI, a défendu l'idée de masquer la webcam. Il a même précisé que ce devait être un réflexe de base en matière de sécurité. En prenant le contrôle de votre caméra, un pirate peut effectivement visionner vos saisies sur clavier et récupérer ainsi identifiants, mots de passe et coordonnées bancaires pour ne citer qu'eux... lire la suite]

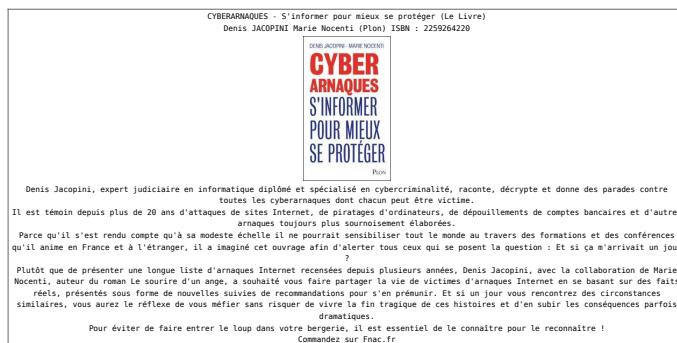
#### Conseils de Denis JACOPINI :

Les personnes averties croient utiliser la méthode miracle pour protéger leur vie privée en masquant leur Webcam.

Certes, je recommande toutefois de masquer votre Webcam car, même si, en l'absence de logiciel de sécurité adapté, le pirate peut la mettre en marche sans que vous rendiez compte de rien. Le pirate peut en effet voir votre tête en train de taper au clavier ou de jouer (ce qui en soit n'aura rien d'intéressant) mais selon l'orientation, voir le reste lorsque vous éloignez de l'ordinateur.

A l'instar des baby phones piratés, mettre en route le microphone de votre ordinateur est tout aussi facile que de mettre en route votre Webcam et même mieux d'ailleurs, car à ma connaissance, il n'existe pas de logiciel de sécurité qui empêche l'accès au microphone. Certes tout le monde n'est pas Mark Zuckerberg, mais tout professionnel devrait en plus de couper son téléphone pendant les réunions, penser aussi à boucher le microphone de son appareil ou mieux, enfincher une fiche Jack vide.

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



06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger", Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 Invités : 7 Millions de victimes de la Cybercriminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risquer ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

<https://www.youtube.com/watch?v=vlDw3kI7ra2s>  
12/04/2018 Denis JACOPINI est invité sur Europe 1 à l'occasion de la sortie du livre "CYBERARNAQUES S'informer pour mieux se protéger"  
Comment se protéger des arnaques Internet  
Commandez sur amazon.fr



Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coédité avec Marie Nocenti, romancière.  
Pour ma part, je suis Expert de Justice en Informatique spécialisé en Cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.  
J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).  
Commandez sur Fnac.fr

Original de l'article mis en page : La webcam, une vraie menace pour les utilisateurs d'ordinateurs

# Comment retirer des publications gênante sur les réseaux sociaux ? Les conseils de la CNIL

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer



LE NET EXPERT  
AUDITS & EXPERTISES



EXPERTISES DE SYSTEMES DE  
VOTES ELECTRONIQUES  
LE NET EXPERT  
.fr



RGPD CYBER  
LE NET EXPERT  
MISES EN CONFORMITE



SPY DETECTION  
Services de détection  
de logiciels espions



LE NET EXPERT  
FORMATIONS



LE NET EXPERT  
ARNAQUES & PIRATAGES



Comment retirer  
des publications  
génante sur les  
réseaux sociaux  
? Les conseils  
de la CNIL

**Sur les réseaux sociaux, vous pouvez être confronté à la diffusion d'informations personnelles publiée par d'autres internautes. Voici quelques liens utiles pour demander rapidement l'effacement de ces contenus**

Une donnée personnelle est « toute information se rapportant à une personne physique identifiée ou identifiable ». Sur une publication, vous pouvez être identifié :

- **directement** (exemple : nom, prénom, etc.)
- ou **indirectement** (exemple : par un identifiant (n° client), un numéro (de téléphone), une donnée biométrique, plusieurs éléments spécifiques propres à votre identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi votre voix ou votre image).

Votre identification peut être réalisée :

- **à partir d'une seule de vos données** (exemple : numéro de sécurité sociale, etc.)
- **à partir du croisement d'un ensemble de données** (exemple : une femme vivant à telle adresse, née tel jour, abonnée à tel magazine et militant dans telle association)

Avant de demander la suppression du contenu, assurez-vous que le compte ou l'information n'appartient pas à un homonyme.

En cas de doute raisonnable, le réseau social peut être en mesure de vous demander tout document permettant de prouver que ce contenu vous concerne. En revanche, **il ne peut pas vous demander des pièces justificatives qui seraient abusives, non pertinentes et disproportionnées par rapport à votre demande.**

## **1. Signaler la publication à effacer**

En fonction du réseau social, vous devez vous rendre sur la page appropriée qu'il a mis à votre disposition à cet effet.

Twitter : Signaler la divulgation d'informations privées

Instagram : Signaler une photo ou vidéo pour violation de vos droits de confidentialité sur Instagram

Facebook : Utiliser le lien » Signaler »

situé à côté de la publication, de la photo ou du commentaire

Snapchat : Signaler la publication ou Utiliser ce formulaire en ligne ou Utiliser le formulaire de droit à l'image

LinkedIn : Signaler le harcèlement d'un utilisateur ou un problème de sécurité

Youtube : Réclamer une atteinte à la vie privée

Dailymotion : Sous chaque vidéo figure un bouton » Signaler cette vidéo »

en cliquant dessus, vous aurez à remplir un formulaire.

## **2. Si le réseau social ne fait pas partie de cette liste**

- Rendez-vous vous en bas de la page d'accueil du réseau social ;
- Identifiez une page « politique de confidentialité » ou « données personnelles » ou « vie privée » ;
- Dans cette page, recherchez les coordonnées du service ou le formulaire qui répondra à votre demande ;
- Envoyez si besoin un modèle à personnaliser qui comprend les références aux textes de loi et vous permet d'indiquer un motif.

**Quelle réponse attendre du réseau social ?**

Le réseau social doit procéder à l'effacement dans les meilleurs délais et au plus tard dans un délai d'un mois, qui peut être porté à trois mois. Dans ce dernier cas, l'organisme doit vous informer des raisons de cette prolongation dans le délai d'un mois.

En parallèle de cette démarche d'effacement – et si ce contenu est référencé dans les moteur de recherche – exercez votre droit au déréférencement de manière à ce que ce contenu ne soit plus associé à votre nom et prénom dans les résultats d'un moteur de recherche.

En cas de réponse insatisfaisante – ou d'absence de réponse sous un mois – de la part du réseau social ou du moteur de recherche, vous pouvez saisir la CNIL.

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

## **Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :**

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Source : *Publication gênante sur les réseaux sociaux : signalez pour supprimer ! | CNIL*

---

# **Des solutions pour la sensibilisation et formation des salariés face à la Cybercriminalité | Denis JACOPINI**



**Des solutions pour la sensibilisation et formation des salariés face à la Cybercriminalité**

## **La sensibilisation et l'éducation des utilisateurs jouent un grand rôle dans la réduction des risques.**

Il importe donc pour les entreprises d'encourager leurs collaborateurs à se comporter de manière cohérente, en respectant des processus et procédures communiqués clairement, dont la conception et la surveillance sont centralisées et qui couvrent la totalité des équipements en usage. Cela n'évitera peut-être pas toute tentative d'attaque mais renforcera certainement la sécurité de l'entreprise.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

formateur n°93 84 03041 84

---

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet... ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

---

Cet article vous plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : Denis JACOPINI et

<http://www.globalsecuritymag.fr/Les-entreprises-revoient-leur,20150826,55304.html>

# Nos ordinateurs ont-ils la mémoire courte ? Vidéo



Nos  
ordinateurs  
ont-ils la  
mémoire  
courte ?  
Video

**Que trouveront les archéologues du futur, d'ici quelques siècles ou quelques milliers d'années ? Des pierres taillées du paléolithique, des hiéroglyphes, des rouleaux de parchemins probablement, des livres peut-être.**

Quelles images, quels sons, quels écrits de notre société restera-t-il dans 2000 ans ? Auront-ils résisté aux épreuves du temps et aux mutations technologiques comme l'ont fait la première photo, le premier film, le premier enregistrement sonore. Mais que deviendront les milliards d'informations engrangées dans les disques durs qui se démagnétisent, et sur les CD ou DVD, qui redoutent la lumière du soleil ?[lire la suite]

## LE NET EXPERT

:

- **MISE EN CONFORMITÉ RGPD / CNIL**
- AUDIT RGPD ET CARTOGRAPHIE de vos traitements
- MISE EN CONFORMITÉ RGPD de vos traitements
- SUIVI de l'évolution de vos traitements
- FORMATIONS / SENSIBILISATION :
  - CYBERCRIMINALITÉ
- PROTECTION DES DONNÉES PERSONNELLES
  - AU RGPD
  - À LA FONCTION DE DPO
- RECHERCHE DE PREUVES (outils Gendarmerie/Police)
  - ORDINATEURS (Photos / E-mails / Fichiers)
  - TÉLÉPHONES (réécupération de Photos / SMS)
  - SYSTÈMES NUMÉRIQUES
- EXPERTISES & AUDITS (certifié ISO 27005)
  - TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
    - SÉCURITÉ INFORMATIQUE
  - SYSTÈMES DE VOTES ÉLECTRONIQUES

### Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité, Recherche de preuves et en Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

Source : *Nos ordinateurs ont-ils la mémoire courte ?*

---

# Mise en conformité RGPD : Accompagnement personnalisé par des Experts

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

**LE NET EXPERT**  
AUDITS & EXPERTISES

**EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES**  
**LENETEXPERT**  
**.fr**

**RGPD CYBER**

**LE NET EXPERT**  
MISES EN CONFORMITÉ

**SPY DETECTION**  
Services de détection de logiciels espions

**LE NET EXPERT**  
FORMATIONS

**LE NET EXPERT**  
ARNAQUES & PIRATAGES

**Mise en conformité RGPD : Accompagnement personnalisé par des Experts**

**Vous souhaitez manifester un intérêt pour le RGPD (peut-être un peu par obligation) et nous souhaiter faire partie d'un projet. Nous avons réservé des places pour votre conférence.**

Intervenant sur des séances RGPD depuis 2012, après avoir identifié différentes types d'attentes, nous avons dessiné nos offres pour qu'elles correspondent au mieux à vos besoins.

**1. Vous recherchez l'absolu?**

Si vous recherchez l'absolu, nous vous proposons d'apprendre l'essentiel de la réglementation européenne relative à la Protection des Données à Caractère Personnel et le nécessaire pour comprendre et débattre une mise en conformité. Une fois la formation achevée, vous êtes autonome mais pourrez toujours compter sur notre soutien sous forme de formation personnalisée, soit sous forme d'accompagnement personnalisé ;

L'issue de cette formation, nous vous recevrez une attestation prouvant que vous êtes en place d'une démarche de mise en conformité de votre établissement avec le RGPD (Règlement Général sur la Protection des Données). Pour information, nous sommes référencés auprès de la CNIL.

**2. Vous recherchez pour l'essentiel?**

Si vous recherchez pour l'essentiel ce qui est nécessaire pour exiger la mise en conformité, nous vous proposons une formation de deux heures avec un certificat de participation au format papier (RGPD (Règlement Général sur la Protection des Données)).

**3. Vous souhaitez confier la totalité de votre mise en conformité?**

Si vous souhaitez confier la totalité de votre mise en conformité de votre établissement avec le RGPD (Règlement Général sur la Protection des Données) et les différentes réglementations relatives à la protection des données à caractère personnel.

En l'absence de toute autre demande, nous pourrons compter sur votre expertise à la fois technique et pédagogique pour que votre établissement soit accompagné de manière extrêmement efficace.

**Nous vous garantissons une confidentialité extrême sur les informations communiquées. Les personnes habilitées à les consulter sont soumises au secret professionnel.**

Votre Prénom : **MATHIEU** (obligatoire)

Votre Date de naissance : **01/01/1980** (obligatoire)

Votre numéro de téléphone : **06 88 88 88 88** (ne sera pas utilisée pour le téléchargement)

Payez-vous tout débours pour cette activité ? **Oui** (obligatoire)

**Informations complémentaires :**

Tous peuvent nous écrire directement un message dans la zone « INFORMATIONS COMPLÉMENTAIRES QUE VONS JUGEZ UTILES ». Néanmoins, si vous souhaitez que nous vous établissions un chiffrage précis, nous aurons besoin dans un premier temps des informations ci-dessous.

**POUR VOTRE MISE EN CONFORMITÉ RGPD :**

1. La démonstration de vos obligations : Souhaitez-vous démontrer le RGPD et l'essentiel pour comprendre et débattre la démarche ? (recommandé) <input checked="" type="checkbox"/>	Non <input type="checkbox"/>
2. Concernant l'audit : Souhaitez-vous démontrer la mise en conformité de votre établissement avec le RGPD dans le contexte de départ ? <input checked="" type="checkbox"/>	Non <input type="checkbox"/>
Notre considération qu'au moins une période dont vous laissez est indispensable. La date de la dernière peut être fixée à distance.	
3. Concernant la mise en conformité : Elle consiste à mettre en place des améliorations ? <input checked="" type="checkbox"/>	Non <input type="checkbox"/>
Selectionnez votre choix	
4. Concernant le suivi de la mise en conformité : Cette phase consiste à assurer la mise en conformité avec le temps et une mise à jour précise du registre des traitements. <input checked="" type="checkbox"/>	Non <input type="checkbox"/>
Selectionnez votre choix	
5. Votre demande concerne-t-elle un groupement de professionnels ? (coopération, fédération, à nous préciser dans les commentaires...) ou est-elle formulée à titre individuel ? <input checked="" type="checkbox"/>	Individuel <input type="checkbox"/>
INFORMATIONS COMPLÉMENTAIRES QUE VOUS JUGEZ UTILES :	
<b>RGPD</b> "RGPD" title="Mentionnez également formulaires"	
Ensuite, cliquez sur le bouton "Ajouter" et sur "Envoyer" pour valider la saisie.	

Daniel JACOPPIZI est notre expert qui vous accompagnera dans votre mise en conformité avec le RGPD



Je me présente : **Daniel JACOPPIZI**, je suis持有者 d'un certificat en informatique assurant la **sécurisation en RGPD (Protection des Données à Caractère Personnel) et en Confidentialité**. Consultant depuis 1986 et formateur depuis 1988, j'ai une expérience depuis 2012 dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel. De formation d'abord Technique, Correspondant CNIL (CD : Correspondant Informatique et Liberté) puis

**Mon objectif est de mettre à disposition toute ma expérience pour mettre en conformité votre établissement avec le RGPD.**

# Cybersécurité : Aller plus loin dans la formation des salariés



# Cybersécurité : Aller plus loin dans la formation des salariés

**Alors que les entreprises sont de plus en plus sensibilisées aux risques de failles, de mise hors service de leurs systèmes (attaques DDOS) et de destruction de leurs données (via des ransomwares), elles ne pensent pas forcément que leurs outils de communication unifiée sont également concernés par les règles de protection.**

• **Le chiffrement** : toutes les données, qu'elles soient stockées ou en transmission, doivent être protégées, les premières avec au minimum un chiffrement AES 128 bits et les secondes en ajoutant au moins le protocole TLS. Point important : il faut bien évidemment que les messages de tous les interlocuteurs, externes compris, soient cryptés.

• **Le pare-feu** : attention à ne pas tomber dans le piège d'une solution qui exposent des applications, des serveurs ou des équipements hors du pare-feu. De plus, il faut s'assurer que les solutions gèrent correctement le parcours des données au travers des serveurs d'authentification déjà en place.

• **Les mises à jour** : puisque les mises à jour de firmwares et autres logicielles corrigent essentiellement des vulnérabilités ou apportent des dispositifs de sécurité plus robustes, il est primordial qu'elles se fassent de manière automatique pour s'assurer que le SI est protégé le plus tôt possible. Une des approches consiste à passer par une solution en Cloud, automatiquement mise à jour par le fournisseur lui-même **mais à manier avec précaution car si vous avez déjà opté pour le Cloud, avez-vous la certitude que seuls les utilisateurs autorisés accèdent à cet espace de stockage externalisé ? Qui peut bien se connecter pendant que vous dormez ?**

• **La sécurité physique** : où se situent les données que stocke la solution de communication ? Il est essentiel d'avoir la garantie que le datacenter du fournisseur soit protégé 24/7 et qu'il soit régulièrement audité et protégé contre les intrusions physiques.

• **Changer les paramètres par défaut** : Changer tous les identifiants et mots de passe de ceux proposés par défaut pour quelque chose de plus complexe est une règle d'or en matière de cybersécurité.

« Parmi les nombreuses cyberattaques survenues en 2016, la plus célèbre fut celle lancée par le botnet Mirai qui ciblait les webcams. Or, si cette attaque a autant réussi, c'est parce que les mots de passe administrateurs par défaut de ces équipements étaient toujours actifs », dit-il.

• **Sécuriser le réseau... jusqu'aux utilisateurs** : Un segment non sécurisé du réseau est une porte d'entrée par laquelle peuvent passer les cyber-attaques pour atteindre tout le SI d'une entreprise. Les méthodes pour sécuriser le réseau comprennent l'application de restrictions d'accès, le blocage au niveau du pare-feu de certaines pièces attachées et le test régulier des failles de sécurité connues. Mais Gustavo Villardi prévient qu'il ne s'agit là que de résoudre une partie du problème. « Selon une étude récente menée par Verizon sur les failles de sécurité, l'erreur humaine continue d'être la cause principale des cyber-attaques. Les collaborateurs sont le maillon faible et les entreprises se doivent de former leur personnel pour qu'ils restent protégés en ligne et depuis quelque appareil que ce soit », témoigne-t-il.

• **L'usage à domicile** : les collaborateurs en télétravail ne bénéficient pas de l'encadrement de la DSI pour sécuriser leur accès domestique. Il est donc nécessaire de leur indiquer comment sécuriser une box pour activer le chiffrement du Wifi et passer par un VPN.

• **Les mots de passe** : des bonnes pratiques doivent être appliquées pour que les mots de passe de chaque salarié soient impossibles à deviner ; cela comprend aussi bien de la complexité dans l'enchaînement des caractères que la fréquence de remplacement des mots de passe.

• **L'accès** : les collaborateurs devraient toujours éteindre un équipement lorsqu'ils ne s'en servent pas, afin d'éviter que quelqu'un ne se connecte sur les services restés ouverts

• **Le mode privé** : l'utilisation d'un système de visioconférence uniquement avec les paramètres du mode privé évite que quelque des personnes extérieures puissent se greffer sur une conférence.

[lire l'intégralité de l'article source]

#### LE NET EXPERT

:

- FORMATIONS / SENSIBILISATION (utilisateurs / chefs d'entreprises / DSI) :
  - CYBERCRIMINALITÉ
  - PROTECTION DES DONNÉES PERSONNELLES
    - AU RGPD
    - À LA FONCTION DE DPO
    - MISE EN CONFORMITÉ RGPD / CNIL
    - ÉTAT DES LIEUX RGPD de vos traitements)
    - MISE EN CONFORMITÉ RGPD de vos traitements
    - SUIVI de l'évolution de vos traitements
  - RECHERCHE DE PREUVES (outils Gendarmerie/Police)
    - ORDINATEURS (Photos / E-mails / Fichiers)
    - TÉLÉPHONES (récupération de Photos / SMS)
    - SYSTÈMES NUMÉRIQUES
  - EXPERTISES & AUDITS (certifié ISO 27005)
  - TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
    - SÉCURITÉ INFORMATIQUE
  - SYSTÈMES DE VOTES ÉLECTRONIQUES

#### Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité »

« Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- **Mises en conformité RGPD** ;
- Accompagnement à la mise en place de DPO ;
- **Formations** (sensibilisations) à la **cybercriminalité** (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Experts techniques et judiciaires ;
- **Recherche de preuves** téléphones, disques durs, e-mails, contentieux, décomptes de clientèle... ;
- **Expertises de systèmes de vote électronique** ;

Source : Cybersécurité : les trois mesures à prendre pour protéger la communication unifiée – Global Security Mag Online

---

# Formations RGPD Protection des données personnelles et en Cybercriminalité

Parce que la Cybercriminalité et la Protection des données personnelles sont liés, nous couvrons ces sujets concomitamment.



## NOS SERVICES :

- Formations **RGPD** (Règlement Général sur la Protection des Données) ;
- Formations en **Cybercriminalité** ;
- **Sensibilisations** à la cybercriminalité ;
- **État des lieux RGPD** ;

- **Mise en conformité RGPD** ;
- **Analyses de risques** (PIA / DPIA) ;
- **Audits sécurité** ;

## **VOTRE PROFIL :**

- **CLUB D'ENTREPRISES, ORDRES, FÉDÉRATIONS, CORPORATION** : Quelles sont vos responsabilités, quels sont vos risques, quelles devraient être vos priorités ? Que ça soit en matière de Protection des Données Personnelles (RGPD) ou de cybercriminalité, faisons ensemble un état des lieux. Agir sur vos équipements ? Sensibiliser votre personnel ? Libre à vous ensuite d'agir en fonctions de nos recommandations sur les points qui vous sembleront prioritaires.
- **ÉTABLISSEMENTS / CENTRES DE FORMATION / ORGANISATEURS D'ÉVÉNEMENTS** : Que ça soit en protection des données personnelles ou en Cybercriminalité, permettez à vos stagiaires de découvrir les notions essentielles ;
- **CHEFS D'ENTREPRISE / ÉQUIPE INFORMATIQUE** : Nous vous formons dans vos locaux et réalisons en collaboration avec votre équipe informatique une analyse détaillée de vos installations à la recherche de failles et d'axes d'amélioration conformément aux règles de l'art ou de la réglementation en vigueur (RGPD).

## **LES SUJETS DE FORMATION :**



Consultez notre catalogue

## **COMMENT PROTÉGER VOTRE ORGANISME DE LA CYBERCRIMINALITÉ**

Durée : 2 jours ou 4 jours (2 jours tout public + 2 jours approfondissement pour techniciens/informaticiens)

## **VIRUS, DEMANDES DE RANÇONS, VOL DE DONNÉES... PROTÉGEZ-VOUS !**

Durée : 1 jour

## **LES ARNAQUES INTERNET À CONNAÎTRE POUR NE PLUS SE FAIRE AVOIR**

Durée : 1 jour

## **COMMENT BIEN UTILISER LE CLOUD**

Durée : 1 jour

## **COMMENT PROTÉGER VOTRE IDENTITÉ ET VOTRE VIE PRIVÉE SUR INTERNET**

Durée : 1 jour

## **DÉCOUVREZ 50 LOGICIELS GRATUITS À CONNAÎTRE ABSOLUMENT**

Durée : 1 jour

## **RGPD CE QU'IL FAUT SAVOIR POUR NE PAS LE PAYER CHER**

Durée : 1 jour

## **RGPD : ANALYSONS CE QUE VOUS AVEZ COMMENCÉ**

Durée : 1 jour (il est recommandé d'avoir déjà mis en pratique une mise en conformité au moins 15 jours avant)

## COMMENT BIEN UTILISER LES DONNÉES DANS LE CLOUD

Durée : 1 jour

## À LA DÉCOUVERTE DU DARKNET (LE WEB CLANDESTIN)

Durée : 1 jour

## DÉTECTER ET GÉRER LES CYBER-ATTAQUES

Durée : 2 jours

## APPRENEZ À RÉALISER DES AUDITS SÉCURITÉ SUR VOTRE SYSTÈME INFORMATIQUE

Durée : 2 jours

## APPRENEZ À RÉALISER DES TESTS D'INTRUSION SUR VOTRE SYSTÈME INFORMATIQUE

Durée : 2 jours

### Remarque :

*Un sujet peut être traité en quelques heures mais aussi en quelques jours.*

*Malgré un minimum de théorie à connaître, nous pouvons réaliser un mélange de ces thèmes afin de vous proposer un contenu personnalisé en fonction des thèmes et durées globales souhaités.*

# **EN FORMAT CONFÉRENCE :**

## **QUE NOUS RÉSERVE LA CYBERCRIMINALITÉ DANS LES 12 PROCHAINS MOIS ?**

Conférence personnalisable en général sur 1h30 + 30min Questions / réponses) (Demandez le programme détaillé)

## **RGPD – CE QU'IL FAUT SAVOIR POUR NE PAS LE PAYER**

Conférence personnalisable en général sur 1h30 + 30min Questions / réponses) (Demandez le programme détaillé)

## **FONCTIONNEMENT :**

- Vous organisez des formations dans votre établissement ou dans des locaux adaptés : Nous pouvons animer de 1 à 6 jours de formation sur les sujets ci-dessus ;
- Vous organisez un forum ou un salon, nous pouvons préparer une conférence de 20 minutes à 1h30 ou participer à des tables rondes ;
- En faculté ou établissement scolaire, nos interventions seront de 3 à 35 heures.
- Pour une journée de formation, nos interventions sont prévues généralement prévues du mardi au jeudi (Lundi, Vendredi et Samedi sous conditions).
- Nos formations d'une journée sont prévues pour une durée de 7 heures par jour maximum.

**Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.**



DÉSIGNATION  
N° DPO-15945



Data**dock**  
Organisme **validé**  
**et référencé**

---

**Besoin d'un expert pour vous mettre en conformité avec le RGPD ?**

**Contactez-nous**

---

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une expérience d'une dizaine d'années dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisément d'accompagner les organismes dans leur démarche de mise en conformité avec le RGPD.

« Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL. ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :



**Nous animons des Formations sur le RGPD**  
en individuel ou en groupe



**Nous vous accompagnons dans la mise en conformité RGPD de votre établissement**

### **Quelques articles sélectionnés par nos Experts :**

Comment se mettre en conformité avec le RGPD

Accompagnement à la mise en conformité avec le RGPD de votre établissement

Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles

Comment devenir DPO Délégué à la Protection des Données

Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL

Mise en conformité RGPD : Mode d'emploi

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

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

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

---

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

---

---

# **Dispositif biométrique d'accès à la cantine : quelles formalités à la CNIL ? | Denis JACOPINI**

 <p><b>Le Net Expert</b> <b>INFORMATIQUE</b> Protection des données personnelles Sécurité informatique - Cybercriminalité</p>  <p>vous informe...</p>	<p><b>Dispositif biométrique d'accès à la cantine : quelles formalités à la CNIL ?</b></p>
---	--

**Les dispositifs biométriques utilisant le contour de la main des élèves pour gérer l'accès à la cantine scolaire sont couverts par une autorisation unique adoptée par la CNIL.**

Les établissements qui souhaitent installer ce type de dispositifs doivent faire une déclaration simplifiée, en sélectionnant dans l'onglet « Finalité » l'autorisation unique AU-009.

Le responsable du dispositif s'engage ainsi à se conformer aux caractéristiques décrites dans ce texte.

Les autres dispositifs biométriques (réseaux veineux, empreintes digitales, reconnaissance faciale, etc.) doivent faire l'objet d'une demande d'autorisation préalable auprès de la CNIL.

---

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

---

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet... ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

---

Cet article vous plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source :

<http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=D5FEF7DD5664BF01E19E95AF8AF7782F>

---

# RGPD : Qu'est-ce qu'une donnée à caractère personnel ?

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

LE NET EXPERT AUDITS & EXPERTISES

EXPERTISES DE SYSTÈMES DE VOTES ÉLECTRONIQUES  
LENETEXPERT.fr

RGPD CYBER

LE NET EXPERT MISES EN CONFORMITÉ

SPY DETECTION Services de détection de logiciels espions

LE NET EXPERT FORMATIONS

LE NET EXPERT ARNAQUES & PIRATAGES

Denis JACOPINI vous informe

RGPD : Qu'est-ce qu'une donnée à caractère personnel ?

L'entrée en vigueur, en mai dernier, du Règlement UE 2016/679 (RGPD [1]), a donné un souffle nouveau à la protection des données des consommateurs et usagers d'internet en France et en Europe. Mais si on entend beaucoup parler de données personnelles, il n'est pas toujours facile de savoir précisément ce qu'il faut entendre par cette notion.

Le règlement (article 4) les définit comme étant toute *information se rapportant à une personne physique identifiée ou identifiable*.

Le règlement précise également ce qu'est une personne physique identifiable : *une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale*.

En pratique, il faut comprendre de cette définition que, toute donnée se rapportant à votre personne et permettant, même indirectement de vous identifier est une donnée personnelle.

Ainsi, votre nom, prénom, âge, date et lieu de naissance, une photo de vous, un pseudonyme, un numéro de téléphone ou de sécurité sociale, une adresse IP, etc. constituent des données à caractère personnel.

...[lire la suite]

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

**Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :**

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Source : *Qu'est-ce qu'une donnée à caractère personnel ?* – Force Ouvrière

---

**Mon employeur peut-il enregistrer ou écouter mes conversations téléphoniques à mon insu ? | Denis JACOPINI**



**Mon employeur peut-il enregistrer ou écouter mes conversations téléphoniques à mon insu ?**

<p>Un employeur n'a le droit ni d'enregistrer ni d'écouter les conversations téléphoniques de ses employés s'ils n'en sont pas informés.S'il le fait, il commet un délit et risque des sanctions pénales.</p>
<p>Nous organisons régulièrement des <b>actions de sensibilisation ou de formation</b> au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement. Besoins d'informations complémentaires ? Contactez-nous Denis JACOPINI Tel : 06 19 71 79 12 formateur n°93 84 03041 84</p>
<p>Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en <b>cybercriminalité</b> et en <b>déclarations à la CNIL</b>, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la <b>formation de vos salariés</b> afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise. Contactez-nous</p>
<p>Cet article vous plaît ? Partagez ! Un avis ? Laissez-nous un commentaire !</p>
<p>SOURCE : <a href="http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=4FBDF806985B62BC62EB30EBC567BF6F?name=Mon+employeur+peut-il+enregistrer+ou+%C3%A9couter+mes+conversations+t%C3%A9l%C3%A9phoniques+%C3%A0+mon+insu+%3F&amp;id=106">http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=4FBDF806985B62BC62EB30EBC567BF6F?name=Mon+employeur+peut-il+enregistrer+ou+%C3%A9couter+mes+conversations+t%C3%A9l%C3%A9phoniques+%C3%A0+mon+insu+%3F&amp;id=106</a></p>