

# Les obligations des Associations vis à vis de la CNIL | Denis JACOPINI



**Les obligations des Associations vis à vis de la CNIL** Dans le cadre de leur activité, les associations sont amenées à constituer des fichiers de leurs adhérents, de leurs donateurs ou de donateurs potentiels. Quelles sont les règles à respecter ?

Dans le cadre de leur activité, les associations sont amenées à constituer des fichiers de leurs adhérents, de leurs donateurs ou de donateurs potentiels. Quelles sont les règles à respecter ?

Nous allons tenter d'y répondre au travers de réponses par Oui ou par Non à des questions correspondant à des cas concrets : **Une association peut-elle céder, louer ou vendre le fichier de ses adhérents à des fins commerciales ?**

OUI. La loi « informatique et libertés » n'interdit pas cette pratique. Il y a toutefois des précautions à prendre : Il faut d'abord informer les adhérents de cette possible revente de leurs coordonnées à des fins commerciales et leur permettre de s'y opposer. Cette opposition peut se faire par exemple au moyen d'une case à cocher figurant sur le bulletin d'adhésion.

**Une association peut-elle diffuser sur son site web l'annuaire de ses adhérents ?**

OUI. Dans ce cas, comme pour la réponse précédente, les adhérents doivent en être informés au préalable. Ils ont tout à fait le droit de s'opposer à une telle diffusion compte-tenu des risques particuliers de capture des informations diffusées sur le web.

La CNIL propose des mentions type à faire figurer sur les bulletins d'adhésion pour bien informer les adhérents de leurs droits.

**Mention d'information à inscrire sur le bulletin d'adhésion**

Les informations recueillies sont nécessaires pour votre adhésion. Elles font l'objet d'un traitement informatique et sont destinées au secrétariat de l'association. En application des articles 39 et suivants de la loi du 6 janvier 1978 modifiée, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent.

Si vous souhaitez exercer ce droit et obtenir communication des informations vous concernant, veuillez vous adresser à .....  
[indiquez-ici le service en charge de traiter les demandes]

**Il arrive que des mairies demandent aux associations de leur transmettre le fichier de ses adhérents en vue d'obtenir des subventions ? Est-ce légal ?**

NON. Un maire ne peut pas demander, même au titre de la subvention qu'il accorde à une association, la liste nominative des adhérents. Une telle pratique est contraire au principe constitutionnel de la liberté d'association.

En revanche, les mairies peuvent demander, au titre du contrôle des subventions qu'elles versent aux associations, la copie certifiée du budget et des comptes de l'exercice écoulé, ainsi que la communication de tous les documents faisant apparaître les résultats de l'activité de l'association.

### **Un membre d'association peut-il exiger la communication de la liste de tous les autres adhérents ?**

OUI, si les statuts de l'association prévoient cette possibilité. Une association est en effet libre de préciser dans ses statuts que l'adhésion implique d'accepter que ses coordonnées puissent être communiquées à tout adhérent qui en fait la demande, à la condition que cette communication ait un lien direct avec l'activité de l'association.

Dans ce cas, un membre ne peut s'opposer à cette diffusion.

### **Lors du renouvellement du bureau d'une association, un candidat peut-il obtenir la liste des adhérents ?**

OUI. Si les statuts de l'association le prévoient, tout candidat peut demander que la liste des adhérents lui soit transmise, à partir du moment où il s'engage à ne pas l'utiliser à d'autres fins que l'élection et à la détruire à la fin des opérations électorales.

### **Les membres du bureau d'une association, dont les statuts ont été déposés en préfecture, peuvent ils s'opposer à la**

## **diffusion de leurs identités et coordonnées ?**

NON. La loi du 1er juillet 1901 relative au contrat d'association prévoit qu'une association ne peut obtenir la capacité juridique qu'en rendant publics, par une insertion au Journal officiel, son titre, son objet, l'adresse de son siège et les noms, professions, domiciles et nationalités de ceux qui sont chargés de son administration. Cette diffusion peut aussi se faire sur en ligne via la version Internet du journal Officiel.

Néanmoins, des mesures techniques empêchent d'accéder directement à la page de l'association concernée lorsqu'on interroge les différents moteurs de recherche sur la base de l'identité des membres de son bureau.

## **Les fichiers de membres et donateurs d'une association doivent-ils être déclarés à la CNIL ?**

NON, ces fichiers sont dispensés de déclaration à la CNIL.

Attention, être dispensé de déclaration n'exonère pas pour autant des obligations que la loi informatique et libertés impose aux responsables de fichiers. Cela signifie qu'il faut informer les personnes qu'un fichier est constitué et qu'elles ont un droit d'accès aux informations qui les concernent. Enfin bien sûr, le responsable du fichier doit prendre toutes les mesures utiles afin d'assurer la sécurité des informations personnelles collectées.

Source : Denis JACOPINI et [www.cnil.fr](http://www.cnil.fr)

**Cet article vous a plu ? Laissez-nous un commentaire  
(notre source d'encouragements et de progrès)**

---

# **Comment sécuriser vos données et systèmes d'information ? | Denis JACOPINI**

5

**Comment sécuriser vos données et systèmes d'information ?**

**La cyberattaque, dont a été victime la chaîne TV5 Monde, puis ultérieurement le journal Belge Le Soir et d'autres médias, appelle à s'interroger quant à la sécurité des systèmes d'information.**

La #sécurité des données informatiques représente un enjeu quotidien particulièrement important pour les sites d'e-commerce, les médias, les hébergeurs et les éditeurs de sites internet. Les banques et les compagnies d'assurances sont également concernées, en raison des multiples données qu'elles sont amenées à traiter dans le cadre de leurs activités. La cyberattaque, dont a été victime la chaîne « TV5 Monde », puis ultérieurement le journal Belge « Le Soir » et d'autres médias, en témoigne et appelle à s'interroger quant à la sécurité des systèmes d'information, face au volume colossal des échanges de données sur les réseaux[1]. Outre les mesures préventives d'ordre technique à mettre en place, il est des mesures juridiques qu'il est hautement recommandé d'instaurer. Qu'à l'origine de l'attaque on identifie une faille interne à l'entreprise, ou externe (sous-traitant, hébergeur, etc.), il existe différents moyens juridiques à mettre en œuvre pour l'éviter. Les acteurs peuvent en effet être nombreux (éditeur, intégrateur, consultant, sous-traitant, prestataire, etc.) et la chaîne des responsables potentiels apparaît complexe. Face au risque croissant de cyberattaque et aux enjeux du Big Data, il est indispensable de sécuriser l'ensemble des moyens techniques, humains et juridiques qui permettent de garantir la sécurité d'un système informatique.

### **1) La mise en place d'une stratégie en interne**

a) En premier lieu, il est conseillé de procéder à un audit (juridique et technique) de sécurité du système d'information. L'objectif de cet audit sera de répertorier les points forts, et surtout les axes d'amélioration du système d'information dans son ensemble. Dans un monde en « hyper connexion » analyser une partie du système d'information n'a pas de sens car les risques peuvent venir d'un réseau ou d'une filiale non revus. Le but est de vérifier la sécurité du système afin d'identifier les mesures de réaction à une attaque, de tester un nouvel équipement, et surtout de mettre en place un planning de mise en conformité.

Les interventions liées aux opérations de maintenance corrective et évolutive doivent être régulièrement planifiées, notamment par l'application de correctifs de sécurité.

b) Ensuite, il est recommandé de rédiger une Charte de sécurité informatique, visant à sensibiliser chacun à la confidentialité et à l'intégrité des données d'un système d'information. Une telle Charte représente une étape indispensable dans le processus de sécurisation des données. Elle doit viser les postes fixes, les mobiles, les tablettes, etc... et traiter, notamment, de la gestion des mots de passe, mais aussi de l'accès au réseau de l'entreprise depuis l'extérieur.

c) Soulignons qu'il convient d'instaurer une politique de gestion des mots de passe. L'utilisation d'un mot de passe dit « fort » est un élément fondamental dans la sécurisation d'un système d'information. Or, bien souvent, les mots de passe sont trop communs ou configurés par défaut. Il est donc essentiel de mettre en œuvre une politique de gestion des mots de passe afin de protéger tant l'utilisateur final, que le système d'information lui-même.

La surveillance des logs de connexion et de l'accès via des hotspot et/ou VPN est à encadrer également avec minutie.

d) Enfin, il est opportun de prévoir des clauses spécifiques dans les contrats de travail de l'ensemble des salariés au-delà des seuls administrateurs système, Directeurs des Systèmes d'Information (DSI).

### **2) Le développement d'une stratégie en externe**

a) Avant tout accord, il convient de mettre en place une politique efficace de confidentialité en signant des accords de non divulgation (« Non-Disclosure Agreement ») avec l'ensemble de la chaîne des sous-traitants.

b) En parallèle de cela, il est nécessaire :

- de rédiger de solides contrats avec les différents prestataires techniques dont le non-respect sera sanctionné par des clauses pénales ;
- de vérifier régulièrement les contrats conclus avec les hébergeurs.

La rédaction des contrats informatiques nécessite en effet une expertise toute particulière. On pense notamment aux contrats de maîtrise d'œuvre, d'intégration, de sous-traitance, de licence d'utilisation, etc.

Pour ce qui concerne les obligations et garanties des parties, le contrat doit refléter la réalité des responsabilités. Le risque juridique est donc associé à la personne qui est effectivement responsable des traitements et des usages qui sont faits des données et des résultats.

L'application du régime du contrat de fourniture de prestations de services, complété par des obligations accessoires de surveillance et de respect de la confidentialité des données stockées, assure une protection optimale au bénéficiaire du service. Tout en servant les intérêts des utilisateurs, ce régime est également opportun à l'égard des prestataires car il correspond à leur nature juridique et à leur responsabilité sur le Web.

c) Il demeure indispensable de veiller au respect des recommandations de la CNIL. Il est nécessaire de procéder à toute déclaration requise en fonction de la nature des données et des modalités du traitement (déclaration simplifiée, déclaration normale, ou autorisation préalable) ; les formalités préalables étant allégées en cas de désignation d'un Correspondant Informatique et Libertés ou « CIL ».

Au sein de sa structure, ou en externe pour les petites structures, le responsable du traitement désigne une personne qui sera chargée de (i) tenir à jour un registre des traitements mis en œuvre au sein de l'organisme et (ii) veiller au respect des dispositions de la loi « informatique et libertés » au sein de l'organisme. Le CIL ainsi désigné peut être notamment être un salarié de la société, ou le conseil de cette société.

d) Le contrat doit également permettre la possibilité aux acteurs de la DSU d'auditer leur prestataire (droit d'audit). Cela permet de contrôler que les mesures contractuelles, par exemple sur la sécurisation de données, sur l'hébergement des données au sein de l'espace Européen, sont respectées.

e) Enfin, il est toujours possible de solliciter l'intervention de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) qui veille quotidiennement au renforcement de la Cyber sécurité en accompagnant les entreprises par des actions de conseil, de politique industrielle et de réglementation.

### **3) En phase contentieuse**

En cas de conflit, il est nécessaire de faire dresser des constats informatiques aux fins de préserver la matérialité de l'infraction et surtout de retracer l'origine de l'attaque ou de l'intrusion.

Par conséquent, la sécurité des données implique la mise en place d'une stratégie juridique renforcée, que ce soit tant au niveau des systèmes d'information que des réseaux de communications électroniques (mails et réseaux sociaux).

[1] En 1 minute, voici notamment ce qui s'échange sur la toile :

- 204 millions d'emails expédiés ;
- 1.875.000 likes sur Facebook ;
- 278 000 Tweets expédiés ;
- 694 445 recherches sur Google ;
- 70 noms de domaine enregistrés ;
- 13 000 applications téléchargées.

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.

Besoins d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en cybercriminalité et en déclarations à la CNIL, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la formation de vos salariés afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.

Contactez-nous

Après cette lecture, quel est votre avis ?  
Cliquez et laissez-nous un commentaire...

Source : <http://www.journaldunet.com/solutions/expert/60588/cyberattaque--comment-securiser-vos-donnees-et-systemes-d-information.shtml>

---

# **Windows 8 : Identifier les applications malveillantes à partir des services par défaut | Denis JACOPINI**

Windows 8 : Identifier les applications malveillantes à partir des services par défaut



---

# Règlement européen sur la protection des données : Renforcement des droits des personnes



Règlement européen sur la protection des données : Renforcement des droits des personnes

## **Le règlement européen renforce les droits des personnes et facilite l'exercice de ceux-ci.**

### **Consentement renforcé et transparence**

Le règlement impose la mise à disposition d'une information claire, intelligible et aisément accessible aux personnes concernées par les traitements de données.

L'expression du consentement est définie : les utilisateurs doivent être informés de l'usage de leurs données et doivent en principe donner leur accord pour le traitement de leurs données, ou pouvoir s'y opposer. La charge de la preuve du consentement incombe au responsable de traitement. La matérialisation de ce consentement doit être non ambiguë.

### **De nouveaux droits**

**Le droit à la portabilité des données** : ce nouveau droit permet à une personne de récupérer les données qu'elle a fournies sous une forme aisément réutilisable, et, le cas échéant, de les transférer ensuite à un tiers. Il s'agit ici de redonner aux personnes la maîtrise de leurs données, et de compenser en partie l'asymétrie entre le responsable de traitement et la personne concernée.

**Des conditions particulières pour le traitement des données des enfants** : Pour la première fois, la législation européenne comporte des dispositions spécifiques pour les mineurs de moins de 16 ans. L'information sur les traitements de données les concernant doit être rédigée en des termes clairs et simples, que l'enfant peut aisément comprendre. Le consentement doit être recueilli auprès du titulaire de l'autorité parentale. Les États membres peuvent abaisser cet âge par la loi, sans toutefois qu'il puisse être inférieur à 13 ans. Devenu adulte, le consentement donné sur un traitement doit pouvoir être retiré et les données effacées.

**Introduction du principe des actions collectives** : Tout comme pour la législation relative à la protection des consommateurs, les associations actives dans le domaine de la protection des droits et libertés des personnes en matière de protection des données auront la possibilité d'introduire des recours collectifs en matière de protection des données personnelles.

**Un droit à réparation des dommages matériel ou moral** : Toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi.

source : CNIL



Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 0304184).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs aux **risques en informatique**, découvrir et comprendre les **arnachues et les piratages informatiques** pour mieux s'en protéger et se mettre en conformité avec la **CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées 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, conteneurs, 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 : ce qui change pour les professionnels | CNIL

# Un œil sur vous, citoyens

# sous surveillance - Documentaire 2015 | Denis JACOPINI

 Un oeil sur vous, citoyens sous surveillance Documentaire  
2015 2h24

**Des milliards de citoyens connectés livrent en permanence – et sans toujours s'en rendre compte – des informations sur leur vie quotidienne à des sociétés privées qui les stockent dans de gigantesques serveurs. Ces informations sont rendues accessibles aux États et vendues aux entreprises. Dans ce monde sous étroite surveillance, jusqu'où irons-nous en sacrifiant nos vies intimes et nos droits à la liberté individuelle ?**

---

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

---

Expert Informatique assermenté et formateur spécialisé en #sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** 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

---

Cet article vous plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

# **Victime d'une arnaque vous demandant de régler par coupons recharges PCS ? Pas de panique !**

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

 <b>LE NET EXPERT</b> AUDITS & EXPERTISES	 <b>EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES</b> <b>LENETEXPERT</b> .fr	 <b>RGPD CYBER</b> <b>LENETEXPERT</b> MISES EN CONFORMITE	 <b>SPY DETECTION</b> Services de détection de logiciels espions	 <b>LE NET EXPERT</b> FORMATIONS	 <b>LE NET EXPERT</b> ARNAQUES & PIRATAGES
<b>Denis JACOPINI</b> 	<b>vous informe</b>	<b>Victime arnaque demandant régler coupons recharges PCS Pas de panique !</b>	<b>d'une vous de par</b>		

**Les escroqueries à la Carte prépayée et aux coupons recharges PCS Mastercard (ou Transcash ou Tonéo) se développent de plus en plus et ont tendance à remplacer certaines arnaques plus anciennes, mais désormais mieux détectées par les internautes**

Par mail ou via Facebook, ils envoient tout d'abord soit un appel au secours venant d'une personne proche ou toute autre raison aboutissant à un chantage.

Ils demandent ensuite de recharger leur carte de crédit par ce nouveau moyen très moderne qu'est la carte prépayée PCS Mastercard. Souvent les personnes ne connaissent même pas le principe de recharge de carte de crédit mais lorsque l'interlocuteur nous explique qu'il suffit simplement de descendre au bureau de tabac en bas de chez nous, d'acheter 1, 2, 3 ou 4 tickets de recharge (coupons recharges), puis de lui envoyer les codes pour répondre à la demande, beaucoup commencent à flaire le piège.

Ce moyen de paiement vient en remplacement des mandats cash ou des versement par Western Union qui ont aujourd'hui une telle mauvaise réputation que leur nom seul éveille des soupçons pour la plupart d'entre nous.. Il permet de rendre impossible de remonter jusqu'au destinataire par la voie judiciaire habituelle.

Ainsi, que ça soit quelqu'un qui se fait passer pour un ami qui vous signale avoir perdu ses papiers ou son téléphone en vous suppliant de l'aide par ce moyen de paiement ou une personne qui exerce sur vous un chantage :

- N'hésitez pas à porter plainte en commissariat de Police ou en Brigade de Gendarmerie (en fonction de votre résidence) ;
- Vous pouvez utiliser un site internet de pré-plainte sur Internet (<https://www.pre-plainte-en-ligne.gouv.fr>)
- Ne répondez plus à ses messages ;
- Signalez ses agissements sur [www.internet-signalement.gouv.fr](http://www.internet-signalement.gouv.fr) ;

Si vous avez du temps à perdre, vous pouvez aussi vous amuser à les mener en bateau, **les capacités de nuisance de ces arnaqueurs du dimanche étant très limitées** à seulement pouvoir vous envoyer des e-mails ou vous téléphoner si vous avez commis l'imprudence de leur communiquer votre numéro. Vous pouvez rétorquer en leur faisant croire que vous allez les payer ou que vous avez aussi besoin d'un coupon de recharge PCS pour vous déplacer pour aller en acheter un !

#### **Attention :**

Si vous êtes en contact avec une personne se présentant comme victime s'étant faite arnaquer par un escroc et que cette dernière vous communique ensuite les coordonnées d'un contact chez Interpol présenté comme son sauveur, fuyez ! Il s'agit aussi d'une arnaque.

Interpol ne rentre jamais en contact directement avec les victimes !

Ceux qui vous soutiennent le contraire ou qui vous contactent directement en se faisant passer pour Interpol ont malheureusement aussi pour objectif de vous soutirer de l'argent.

Plus d'infos sur : <https://www.lenetexpert.fr/contacter-interpol-en-cas-darnaque-est-une-arnaque/>

#### **Remarque :**

Il est possible qu'au moment où vous êtes sur le point de déposer plainte, la personne en face de vous cherche à vous dissuader. C'est normal, face au faibles changes de retrouver l'auteur de l'acte délictueux, ils considèrent comme une perte de temps le fait de devoir traiter votre demande sous forme de plainte et vous inviteront à déposer une main courante.

Insistez pour déposer plainte car sans cette acte citoyen qu'on ne peut vous refuser (en faisant bien attention de le faire en mentionnant la bonne qualification juridique), vous ne laisserez pas passer la moindre chance (même si elle est minime) de faire arrêter l'escroc.

#### **Pour information**

- Les délits d'usurpation d'identité, pouvant être associé au phishing selon l'article 226-4-1 du code pénal sont punis d'un an d'emprisonnement et de 15 000 € d'amende.
- Selon l'article Article 312-1 du code pénal, le délit d'extorsion ou de tentative d'extorsion (demande d'argent en échange de ne pas supprimer des données ou de ne pas divulguer des secrets volés) est punie de sept ans d'emprisonnement et de 100 000 euros d'amende.
- Les délits d'escroquerie ou tentative d'escroquerie, selon les articles 313-1, 313-2 et 313-3 du code pénal, sont punis de cinq ans d'emprisonnement et de 375 000 euros d'amende.

[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 : *Comment fonctionne une escroquerie à la Carte prépayée et aux coupons recharges PCS Mastercard, Transcash ou Tonéo? | Ms2i On Air*

---

**Quoi et comment supprimer vos données si vous rendez votre ordinateur professionnel à votre employeur ?**



Quoi et comment supprimer vos données si vous rendez votre ordinateur professionnel à votre employeur ?

---

Est-il possible d'effacer toutes nos données présentes sur un ordinateur de fonction lorsque l'on quitte son travail et que l'on ne souhaite pas laisser de trace sur celui-ci ? Si oui, quels moyens préconisez-vous pour être sûr que ce type de données soit bien effacé (effacer l'historique de ses comptes mails et personnelles, formatage complet, logiciel d'aide à la suppression etc..) ?

La première étape consiste à identifier les données à supprimer et celles à sauvegarder avant de procéder au nettoyage.

- Sur la plupart des ordinateurs professionnels, parfois sans le savoir, en plus de nos documents de travail nous stockons :
  - Des programmes ajoutés ;
  - Nos e-mails ;
  - Nos traces de navigation ;
  - Nos fichiers téléchargés ;
  - Divers identifiants et mots de passe ;
  - Les fichiers temporaires

Afin d'éviter l'accès à ces informations par le futur locataire / propriétaire / donataire de votre ordinateur, il sera important de procéder à leur suppression minutieuse.

#### Concernant les programmes ajoutés

Facile sur Mac en mettant le dossier d'un programme à la corbeille, n'utilisez surtout pas la corbeille pour supprimer des programmes sous Windows. La plupart des programmes apparaissent dans la liste des programmes installés. Pour procéder à leur suppression, nous vous conseillons de procéder :

- soit par le raccourci de désinstallation que le programme a créé ;
- s'il n'y a pas de raccourci prévu à cet effet, passez par la fonction « Ajout et Suppression de Programmes » ou « Programmes et fonctionnalités » (ou fonction équivalente en fonction de votre système d'exploitation de sa version) ;

• Enfin, vous pouvez utiliser des programmes adaptés pour cette opération tels que RevouInstall (gratuit).

#### Concernant les e-mails

Selon le programme que vous utiliserez, la suppression du/des compte(s) de messagerie dans le programme en question suffit pour supprimer le ou les fichiers contenant les e-mails. Sinon, par précaution, vous pouvez directement les localiser et les supprimer :

- fichiers « .pst » et « .ost » de votre compte et archives pour le logiciel « Outlook » ;
- fichiers dans « %AppData%\Microsoft\Windows Live Mail » pour le logiciel « Windows Live Mail » ;
- les fichiers contenus dans « %APPDATA%\Thunderbird\Profiles » pour le programme Mozilla Thunderbird
- le dossier contenu dans « ..Local Settings\Application Data\IMIdentities » pour le programme IncrediMail.

#### Concernant nos traces de navigation

En fonction de votre navigateur Internet et de sa version, utilisez, dans les « Options » ou les « Paramètres » la fonction supprimant l'Historique de Navigation » ou les « Données de Navigation ».

#### Concernant les fichiers téléchargés

En fonction de votre système d'exploitation l'emplacement de stockage par défaut des fichiers téléchargés change. Pensez toutefois à parcourir les différents endroits de votre disque dur, dans les lecteurs réseau ou les lecteurs externes à la recherche de fichiers et documents téléchargés que vous auriez pu stocker.

#### Concernant divers identifiants et mots de passe

Du fait que le mot de passe de votre système d'exploitation stocké quelque part (certes crypté), si vous êtes le seul à le connaître et souhaitez en conserver la confidentialité, pensez à le changer et à en mettre un basic de type « utilisateur ».

Du fait que les mots de passe que vous avez mémorisé au fil de vos consultations de sites Internet sont également stockés dans votre ordinateur, nous vous recommandons d'utiliser les fonctions dans ces mêmes navigateurs destinées à supprimer les mots de passe et les informations qui pré remplissent les champs.

#### Concernant les fichiers temporaires

En utilisant la fonction adaptée dans vos navigateurs Internet, pensez à supprimer les fichiers temporaires liés à la navigation Internet (images, cookies, historiques de navigation, autres fichiers).

En utilisant la fonction adaptée dans votre systèmes d'exploitation, supprimez les fichiers temporaires que les programmes et Windows génèrent automatiquement pour leur usage.

#### Pour finir

Parce qu'un fichier supprimé n'est pas tout à fait supprimé (il est simplement marqué supprimé mais il est toujours présent) et dans bien des cas toujours récupérable, vous pourrez utiliser une application permettant de supprimer définitivement ces fichiers supprimés mais pourtant récupérables telle que « Eraser », « Clean Disk Security », « Prevent Restore ».

Denis Jacopini anime des conférences et des formations et est régulièrement invité à des tables rondes en France et à l'étranger pour sensibiliser les décideurs et les utilisateurs aux CyberRisques (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons conférences et formations pour sensibiliser décideurs et utilisateurs aux risques en informatique, découvrir et comprendre les arnaques et les piratages informatiques pour mieux s'en protéger et se mettre en conformité avec la CNIL en matière de Protection des Données Personnelles. Nos actions peuvent être personnalisées et organisées dans votre établissement.

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



Denis Jacopini est Expert Informatique assurément spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (falsification d'identité, fraude à la sécurité sociale, contrefaçon, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de CIL (Correspondants Informatique et Liberté);
- Accompagnement à la mise en conformité CNIL de votre Etablissement.



Contactez-nous

Réagissez à cet article

Original de l'article mis en page : 5 applications pour effacer des données de façon sécurisée – ZDNet

# Quelles formalités une pharmacie doit déclarer à la CNIL ? | Denis JACOPINI



**vous informe...**

## Quelles formalités une pharmacie doit déclarer à la CNIL ?

Les fichiers relatifs à la gestion d'une pharmacie doivent être déclarés à la CNIL : Par une déclaration simplifiée de conformité à la norme n°52 si le fichier correspond aux caractéristiques énoncées dans ce texte ;  
Par une déclaration normale si le fichier sort du cadre de cette norme.

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=193E337DAA685A15B25C9E90E19E80BF?name=Activit%C3%A9+d%27une+pharmacie+%3A+quelles+formalit%C3%A9s+%C3%A0+la+CNIL+%3F&id=545>

# Votre boite e-mail a été piratée. Quelle attitude adopter ? | Denis JACOPINI



**Votre boite e-mail a été piratée. Quelle attitude adopter ?**

## **Il vous semble ou vous avez la certitude que votre boite e-mail a été piratée ?Quelle attitude adopter ?**

### **Un choix s'offre à vous :**

Vous protéger et faire cesser le piratage, ou bien rechercher l'auteur et porter plainte.

### **Vous protéger et faire cesser le piratage**

Il vous semble ou vous avez la certitude que votre boite e-mail a été piratée. Quels sont les éléments qui vous font penser ça ?

– Quelqu'un est au courant de choses dont il ne devrait pas être au courant qui n'apparaît que dans les e-mails ?

– Vous constatez que des e-mails que vous n'avez pas lu sont tout de même « lus » ?

– Vous avez constaté dans l'historique des connexions une connexion qui ne semble pas être la vôtre ?

1°/ Pour vous protéger contre ça et faire cesser tout piratage, la première chose à faire est de lancer des outils de détection de virus, d'espions, keyloggers et autres logiciels malveillants.

Vous fournir une liste serait très compliqué car ceci engagerait quelque part ma responsabilité de vous conseiller un outil plutôt qu'un autre, alors qu'il en existe un grand nombre et aucun n'est fiable à 100%. Je ne peux vous conseiller que de rechercher sur Internet des « Antivirus Online », des Anti-Malwares, des Anti-espions... Toutefois, pour nos propres besoins nous avons une liste de liens accessible sur [www.antivirus.lenetexpert.fr](http://www.antivirus.lenetexpert.fr).

2°/ Une fois votre ordinateur nettoyé, vous pouvez procéder aux changements de mots de passe des différents services que vous utilisez régulièrement (e-mail, banque, blog, réseaux sociaux...).

Une fois ces deux étapes réalisées, vous ne devriez plus être « espionné ».

### **Rechercher l'auteur et porter plainte**

Si vous suspectez une personne en particulier et que vous souhaitez l'attraper la main dans le sac, sachez que votre action doit prendre la voie de la justice.

Soit vous avez les éléments techniques pouvant l'action de l'auteur clairement identifié, et vous pouvez faire constater par huissier, soit, vous n'avez comme élément qu'une adresse IP, au quel cas, il sera nécessaire de se rapprocher d'un avocat conseil qui rédigera une requête auprès du Tribunal Adhoc afin d'obtenir une ordonnance nous permettant, en tant qu'expert, de réaliser les démarches auprès des fournisseurs de services concernés par le piratage.

Une autre solution plus économique car gratuite mais à l'issue incertaine est de signaler les actes de piratages dont vous êtes victime aux services de Gendarmerie ou de Police en commissariat, en brigade ou sur le site Internet [www.internet-signalement.gouv.fr](http://www.internet-signalement.gouv.fr). Cependant, s'il n'y a pas de très grosses sommes en jeu, d'actes délictueux auprès de mineurs ou en rapport avec des entreprises terroristes, vous comprendrez aisément que votre demande ne sera pas considérée comme prioritaire. Sachat que les opérateurs conservent les traces qui vous permettront d'agir en justice quelques mois, quelques semaines ou quelques jours, votre demande par cette voie risque fortement d'être classée sans suite.

---

Denis Jacopini anime des **conférences et des formations** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs aux **risques en informatique, découvrir et comprendre les arnaques et les piratages informatiques pour mieux s'en protéger et se mettre en conformité avec la CNIL en matière de Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.

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

---

Cet article vous plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : Denis JACOPINI

---

# Étape par étape : comment bien effacer et conserver vos données informatiques stockées sur votre ordinateur professionnel si vous changez de travail à la rentrée (et pourquoi c'est très important) ?



Étape par étape : comment bien effacer et conserver vos données informatiques stockées sur votre ordinateur professionnel si vous changez de travail à la rentrée (et pourquoi c'est très important) ?

---



Original de l'article mis en page : Étape par étape : comment bien effacer et conserver vos données informatiques stockées sur votre ordinateur professionnel si vous changez de travail à la rentrée (et pourquoi c'est très important) | Atlantico.fr