

# Astuce : Un logiciel anti-espions gratuit pour Windows

## | Denis JACOPINI

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



LE NET EXPERT  
AUDITS & EXPERTISES

RGPD CYBER

SPY DETECTION  
Services de détection de logiciels espions

LE NET EXPERT  
MISES EN CONFORMITE

LE NET EXPERT  
FORMATIONS

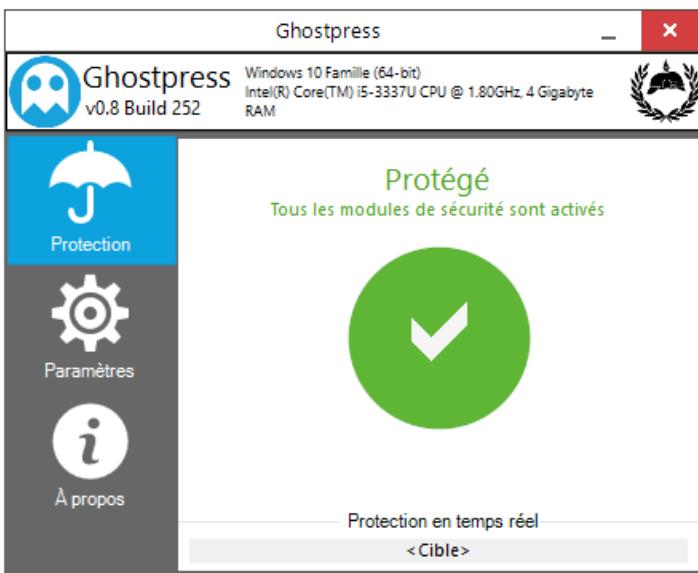
LE NET EXPERT  
ARNAAQUES & PIRATAGES

Denis JACOPINI

Astuce : Un logiciel anti-espions gratuit pour Windows

vous informe

**Ghostpress un logiciel anti-keylogger portable gratuit qui est en mesure de protéger votre ordinateur contre les logiciels espions.**



Dans cet article, je vous présente **Ghostpress**, un logiciel anti-keylogger portable totalement gratuit qui est en mesure de protéger votre ordinateur des logiciels espions.

## **Mais qu'est-ce qu'un keylogger ?**

*En informatique, un keylogger (enregistreur de frappe) est un logiciel espion qui espionne l'utilisateur d'un ordinateur. Le but d'un tel outil est de s'introduire entre la frappe au clavier et l'apparition du caractère à l'écran. Cela permet à un pirate informatique de récupérer toutes les informations que vous avez tapez avec votre clavier comme un login et un mot de passe, une adresse, des informations bancaires etc. [Source]*

## **Ghostpress**

*Ghostpress est un outil très simple d'utilisation et peu gourmand en ressource système. Il vous suffit simplement de le télécharger, puis de le lancer pour que tous les modules de sécurité soient activés. Ainsi, chaque actions que vous exécuterez sur l'ordinateur seront cachés des regards indiscrets.*

*Vous pouvez également désactiver temporairement le programme en cliquant sur le gros bouton vert et exécuter le programme automatiquement au démarrage de Windows en cochant une petite case dans les paramètres de l'outil.*

[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"]

Article original de @justgeekOriginal  
<http://www.justgeek.fr/ghostpress-logiciel-anti-keylogger-windows-47093>

---

# Formation en cybercriminalité : Virus, arnaques et piratages informatiques, Solutions pour nos entreprises



Denis JACOPINI



vous informe

Formation en  
cybercriminalité  
: Virus et  
arnaques  
piratages  
informatiques,  
Solutions pour  
nos entreprises

---

## Présentation

Le contexte de l'Internet et l'ampleur du phénomène de la cybercriminalité, nous poussent à modifier nos comportements au quotidien.

Avons-nous raison d'avoir peur ? De quoi doit-on avoir peur ? Comment se protéger ?

Les réponses évidentes sont techniques, mais il n'en est pas moins vrai que des règles de bonnes pratiques et des

attitudes responsables seront les clés permettant d'enrayer le phénomène....

## Objectif

Découvrez les règles de bonnes pratiques et des attitudes responsables qui sont les clés permettant d'enrayer ce phénomène.

## Durée

1 journée

ou conférence de 2 heures.

## Public concerné

Chefs d'entreprise, présidents d'associations, élus, décideurs, employés, agents, ....

## Moyens pédagogiques

Vidéo projecteur et sonorisation souhaitée selon la taille de la salle.

## Animateur

Denis JACOPINI

Expert Judiciaire en Informatique diplômé en Cybercriminalité, Droit, Sécurité de l'information, informatique Légale et en Droit de l'Expertise Judiciaire. Spécialisé en Protection des données personnelles et certifié ISO 27005, il a été pendant une vingtaine d'année à la tête d'une société spécialisée en sécurité Informatique.

**Son métier : Aider les professionnels à se protéger des pirates informatiques, et à se mettre en conformité avec la CNIL et le règlement Européen sur la Protection des Données Personnelles.**

Il intervient dans la France entière et à l'étranger pour former ou sensibiliser les décideurs, informaticiens et utilisateurs sur les techniques utilisées par les Pirates informatiques pour piéger leurs victimes et sur les obligations en matière de protection des données à caractère personnel.

Différentes interventions pour :

- Le **Conseil de l'Europe** ;
- Un **Centre d'Enseignement et de Recherche en Informatique** ;
- Le **Centre d'Etudes des Techniques Financières** et d'Ingénierie d'Aix en Provence ;
- Des **écoles d'avocats** ;
- Des **Compagnies d'Experts Judiciaires** ;
- De nombreux clubs ou associations de chefs d'entreprises dans la **France entière et à l'étranger** ;
- Le **Centre National de la Fonction Publique Territoriale** (CNFPT) pour des élus, des S.G. et des agents publics.

(Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle – Numéro formateur : 93 84 03041 84)

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

# Une entreprise peut-elle être condamnée pour défaut de sécurisation de l'accès à ses outils informatiques ?

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 CONFORMITE

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

**LE NET EXPERT**  
FORMATIONS

**LE NET EXPERT**  
ARNAQUES & PIRATAGES

Une entreprise peut-être condamnée pour défaut de sécurisation de l'accès à ses outils informatiques ?

Nous attirons votre attention sur le fait que cette information est modifiée par la mise en place du RGPD (Règlement Général sur la Protection des données). Plus d'informations [ici](#) : <https://www.lenetexpert.fr/comment-se-mettre-en-conformite-avec-le-rgpd> Nous l'avons toutefois laissée accessible non pas

par nostalgie mais à titre d'information.

---

---

## **Une entreprise peut être condamnée pour défaut de sécurisation de l'accès à ses outils informatiques ?**

Une entreprise peut être sanctionnée par la CNIL, par exemple, si l'organisme juge que les mots de passe sont peu sécurisants : les noms des employés, inchangés depuis quelques années. Avec les nouvelles réglementations européennes entrées en vigueur en 2018, les amendes peuvent s'élever à 20 millions d'euros voire 4% du chiffre d'affaires mondial...

**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



DataDock  
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"]

---

Source : Connaissez-vous vos droits sur les données personnelles au travail (VRAI-FAUX) ? – La Voix du Nord

# La durée du travail de tous les salariés peut être contrôlée par un système de géolocalisation ?

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



**La durée du travail de tous les salariés peut être contrôlée par un système de géolocalisation ?**

La durée du travail de tous les salariés peut être contrôlée par un système de géolocalisation ?

Il n'est pas possible pour l'employeur d'utiliser les résultats de la géolocalisation si ce n'est pas déclaré à la CNIL (Commission nationale de l'informatique et des libertés) et sans que le sache le salarié, encore moins si l'entreprise possède déjà un moyen de contrôler la durée de travail. Si un salarié a une liberté de son temps de travail, c'est surtout le résultat qui compte.

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

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

Quels sont les droits et devoirs des salariés en matière de sécurité informatique

La durée du travail de tous les salariés peut être contrôlée par un système de géolocalisation ?

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

Une entreprise peut-elle être condamnée pour défaut de sécurisation de l'accès à ses outils informatiques ?

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)

---

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

Besoin d'une **formation pour apprendre à vous mettre en conformité avec le RGPD** ?

**Contactez-nous**



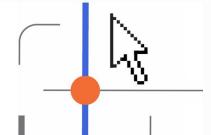
Notre Expert, Denis JACOPINI est Expert de justice en informatique spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Denis JACOPINI a bientôt une expérience d'une dizaine d'années dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel. De formation d'abord technique, Correspondant CNIL (CIL : Correspondant Informatique et Libertés) puis récemment Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il m'est ainsi facile pour moi d'expliquer le côté pragmatique de la démarche de mise en conformité avec le RGPD.

*« Mon objectif, vous transmettre mon savoir, vous dévoiler ma technique et mes outils car c'est bien ce qu'attendent les personnes qui font appel à nos services. ».*

Source : Connaissez-vous vos droits sur les données personnelles au travail (VRAI-FAUX) ? – La Voix du Nord

# Quels sont les droits et devoirs des salariés en matière de sécurité informatique | Denis JACOPINI

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> <i>.fr</i>	 <b>RGPD CYBER</b> <b>LENET EXPERT</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
<input checked="" type="checkbox"/>	<b>Quels sont les droits et devoirs des salariés en matière de sécurité informatique</b>				

**Il n'est pas rare que des salariés soient surpris en train, au sein de leur entreprise, d'utiliser des outils de type Keylogger – permettant l'enregistrement des touches utilisées sur le clavier – et des logiciels visant à capter et à forcer les mots de passe de sessions de systèmes d'exploitation.**

Or, dans la majorité des cas, aucune sanction n'est prise par les employeurs, y compris lorsque les auteurs des faits sont animés d'intentions malveillantes et non simplement ludiques.

Dans un raisonnement inspiré du droit du travail, l'employeur – arguant par exemple de ne pas disposer de charte de sécurité informatique spécifiant les comportements à respecter, ainsi que les sanctions applicables – estime qu'à défaut d'avoir porté par écrit à la connaissance de l'employé la réglementation en vigueur au sein de l'entreprise, celui-ci ne peut être légalement sanctionné.

Il est important de rappeler que le seul fait de collecter des données à caractère personnel par un moyen frauduleux est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende (article 226-18 du Code pénal) et ce, quelles que soient les intentions du salarié. De même, le fait de s'introduire frauduleusement dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans de prison et de 30 000 euros d'amende (article 321-1 du même code). La loi est d'application directe et ne nécessite pas d'être citée dans une charte informatique pour en assurer le respect par les salariés. Les employeurs peuvent donc prendre immédiatement les sanctions afférentes à une telle faute.

En outre, la responsabilité de l'employeur peut se voir engagée par ce type d'agissements, sur la base de plusieurs fondements :

- la personne cible/victime des menées de son/ses collègues pourra, en cas de dommage, agir contre l'employeur, responsable de ses salariés. Il reviendra alors à la société de prouver que le mis en cause a agi « hors des fonctions auxquelles il était employé, sans autorisation et à des fins étrangères à ses attributions », ce qui est rarement admis en pratique.
- de par la jurisprudence « Sarenza c/ Jonathan » du 21 février 2013, le juge a précisé que la société devait supporter, à hauteur de 30%, son propre dommage, engendré par les lacunes dans la gestion des identifiants d'accès aux bases de données. Le juge a donc instauré l'obligation, pour l'employeur, de mettre en place des mesures de protection informatique efficaces, afin de prévenir l'installation de tout logiciel espion.
- Enfin, la plupart des logiciels utilisés à ces fins proviennent de téléchargements, susceptibles de contenir des virus. Les réseaux internes des entreprises sont régulièrement infectés par ce biais, ce qui facilite les intrusions informatiques et, partant, l'accès, l'utilisation, l'extraction, voire la destruction de données stratégiques pour l'entreprise.

#### **Préconisations de la DGSI**

La DGSI recommande à toute entreprise :

- En priorité, d'établir une charte de sécurité informatique qui permettra de sensibiliser les salariés aux enjeux numériques, tout en les responsabilisant.
- D'organiser régulièrement des conférences de sensibilisation à destination de l'ensemble des collaborateurs, qui insisteront sur leurs droits et obligations à l'ère du tout-numérique et dispenseront des mises à jour sur les évolutions technologiques en cours.
- De mettre en place des mesures de protection efficaces afin de prévenir l'utilisation potentielle de logiciels et matériels espions. L'existence de tels dispositifs de sécurité informatique permettra à l'employeur de dégager sa responsabilité juridique et d'optimiser le bon fonctionnement de son entreprise en augmentant le niveau de protection.

Vous avez besoin de recueillir des preuves, expertiser un système informatique, vérifier des contenus, Denis JACOPINI peut vous conseiller, vous accompagner et réaliser toutes les phases techniques nécessaires à la constitution d'un dossier juridique solide.

Contactez Denis JACOPINI

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

**Quelques articles sélectionnés par nos Experts :**

Quels sont les droits et devoirs des salariés en matière de sécurité informatique

La durée du travail de tous les salariés peut être contrôlée par un système de géolocalisation ?

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

Une entreprise peut-elle être condamnée pour défaut de sécurisation de l'accès à ses outils informatiques ?

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)

---

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

**Besoin d'une formation pour apprendre à vous mettre en conformité avec le RGPD ?**

**Contactez-nous**

---



Notre Expert, Denis JACOPINI est Expert de justice en informatique spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Denis JACOPINI a 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 (CIL : Correspondant Informatique et Libertés) puis récemment Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il m'est ainsi facile pour moi d'expliquer le côté pragmatique de la démarche de mise en conformité avec le RGPD.

*« Mon objectif, vous transmettre mon savoir, vous dévoiler ma technique et mes outils car c'est bien ce qu'attendent les personnes qui font appel à nos services. ».*

Source :  
<http://www.ccirezo-normandie.fr/document/104108-flash-ingerence-economique-n-15-rappel-des-droits-et-devoirs-des-salaries-en-entrepr>

# Ne pas avertir son employeur de propos injurieux sur Facebook peut vite devenir une faute grave | Denis JACOPINI

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

 <b>LE NET EXPERT</b> AUDITS & EXPERTISES	 <b>LENETEXPERT</b> .fr	 <b>RGPD CYBER</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
<input checked="" type="checkbox"/> <b>Ne pas avertir son employeur de propos injurieux sur Facebook peut vite devenir une #faute grave</b>					

**La cour d'appel de Lyon a confirmé le mois dernier le licenciement d'une salariée accusée d'avoir tenu sur Facebook des propos dégradants et injurieux à l'égard de ses collègues de travail. L'employeur n'a pourtant pas réussi à prouver que la personne mise en cause était bien l'auteur des messages délivrés sur un groupe spécialement créé à cet effet. Explications.**

Travaillant en tant que sellière maroquinière depuis 2002 chez Hermès, Madame X est licenciée en décembre 2011 pour faute grave. C'est-à-dire sans préavis ni aucune indemnité. Il faut dire que les reproches formulés par son employeur sont relativement sérieux.

La salariée est en effet accusée d'avoir ouvert en octobre 2011 un groupe Facebook intitulé « Les potins d'Hermès », sur lequel étaient relatées des « situations tenant à la vie privée de certains collaborateurs nommément désignés », « sous forme de messages et anecdotes ». C'est suite à des remontées internes que la direction a eu vent de ces commentaires jugés « profondément dégradants et injurieux » à l'égard des employés concernés, ce qui a poussé les responsables de l'entreprise à chercher à remonter jusqu'à leur auteur.

Problème : l'administrateur de ce groupe dispose d'un compte Facebook au nom de « Jules César ». Autrement dit, il s'agit d'un beau pseudonyme... Après enquête, l'employeur affirme que l'adresse IP de l'auteur de ces messages correspond à celle du domicile de Madame X. Dans un premier temps, la salariée reconnaît avoir eu connaissance de ce groupe, tout en niant en être à l'origine. Mais dans un second temps, elle finit par admettre que le compte « Jules César » et le groupe « Les potins d'Hermès » ont bien été créés depuis son ordinateur, mais par sa sœur...

« Même dans le cas où les déclarations de votre soeur (par ailleurs très limitées quant à son hypothétique implication personnelle) [seraient] avérées, et dans la mesure où vous nous avez déclaré avoir eu connaissance de la création de la page et de son contenu dès sa mise en ligne, vous auriez dû à tout le moins nous alerter au sujet d'une telle initiative dont la teneur et la portée ne pouvaient rester sans conséquence vis-à-vis de l'entreprise et de ses collaborateurs » retient ainsi l'employeur dans sa lettre de licenciement.

#### **Impossible d'identifier le créateur du groupe**

Sauf que l'ex-salariée estime avoir été remerciée à tort. Elle a donc tout d'abord saisi le conseil des prud'hommes de Lyon, lequel a confirmé le licenciement pour faute grave en novembre 2013. Madame X a ensuite saisi la cour d'appel de Lyon, qui a justement rendu sa décision le 20 octobre dernier.

Les magistrats se sont intéressés en particulier aux adresses IP fournies par Hermès. Ils ont cependant constaté que la connexion ayant servi à créer le profil Jules César et à alimenter « la plupart » des messages litigieux correspondait en fait à « une adresse IP algérienne dont l'employeur n'a pu identifier le titulaire ». En clair, il était impossible de prouver en l'état qu'il s'agissait de Madame X ou même de sa soeur.

Mais cela n'a pas empêché la cour d'appel de considérer qu'il y avait malgré tout eu faute grave de la part de la salariée. Cette faute ? Savoir que le groupe « Les potins d'Hermès » existait et n'avoir rien signalé. La décision, que nous avons pu consulter, retient en ce sens que « la faute commise par Mme X en n'alertant pas sa direction sur la création de ce groupe de discussion alors qu'à partir de son propre ordinateur étaient mis en ligne des propos déshonorants pour ses collègues de travail (...) est d'une gravité suffisante pour rendre impossible le maintien de cette salariée dans l'entreprise pendant la durée limitée du préavis ».

La cour d'appel n'a donc pas donné suite aux demandes de l'ex-salariée, qui réclamait plus de 40 000 euros d'indemnités.

La décision de la cour d'appel de Lyon évoquée dans l'article ci-dessus

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

**Quelques articles sélectionnés par nos Experts :**

Quels sont les droits et devoirs des salariés en matière de sécurité informatique

La durée du travail de tous les salariés peut être contrôlée par un système de géolocalisation ?

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

Une entreprise peut-elle être condamnée pour défaut de sécurisation de l'accès à ses outils informatiques ?

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)

---

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

**Besoin d'une formation pour apprendre à vous mettre en conformité avec le RGPD ?**

**Contactez-nous**

---



Notre Expert, Denis JACOPINI est Expert de justice en informatique spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Denis JACOPINI a 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 (CIL : Correspondant Informatique et Libertés) puis récemment Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il m'est ainsi facile pour moi d'expliquer le côté pragmatique de la démarche de mise en conformité avec le RGPD.

*« Mon objectif, vous transmettre mon savoir, vous dévoiler ma technique et mes outils car c'est bien ce qu'attendent les personnes qui font appel à nos services. ».*

Source :  
<http://www.nextinpath.com/news/91031-propos-injurieux-sur-face-book-ne-pas-avertir-son-employeur-peut-etre-faute-grave.htm>

# Les grands principes de la cryptologie et du chiffrement

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

 <p><b>LE NET EXPERT</b> AUDITS &amp; EXPERTISES</p>	 <p><b>LENETEXPERT</b> fr EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES</p>	 <p><b>LE NET EXPERT</b> MISES EN CONFORMITE</p>	 <p><b>SPY DETECTION</b> Services de détection de logiciels espions</p>	 <p><b>LE NET EXPERT</b> FORMATIONS</p>	 <p><b>LE NET EXPERT</b> ARNAQUES &amp; PIRATAGES</p>
 <p><b>Denis JACOPINI</b> vous informe LCI</p>	<p><b>Les grands principes de la cryptologie et du chiffrement</b></p>				

Historiquement, la cryptologie correspond à la science du secret, c'est-à-dire au chiffrement. Aujourd'hui, elle s'est élargie au fait de prouver qui est l'auteur d'un message et s'il a été modifié ou non, grâce aux signatures numériques et aux fonctions de hachage. À l'occasion du mois européen de la cybersécurité, la CNIL vous explique ce que c'est et à quoi ça sert.

Etymologiquement, la cryptologie est la science (λόγος) du secret (κρυπτός). Elle réunit la cryptographie (« écriture secrète ») et la cryptanalyse (étude des attaques contre les mécanismes de cryptographie).

La cryptologie ne se limite plus aujourd'hui à assurer la **confidentialité** des secrets. Elle s'est élargie au fait d'assurer mathématiquement d'autres notions : assurer l'**authenticité** d'un message (qui a envoyé ce message ?) ou encore assurer son **intégrité** (est-ce qu'il a été modifié ?).

Pour assurer ces usages, la cryptologie regroupe quatre principales fonctions : le hachage avec ou sans clé, la signature numérique et le chiffrement.

Pour expliquer la cryptologie, nous utiliserons dans nos exemples les personnages traditionnels en cryptographie : Alice et Bob.

Pour découvrir les grandes phases de l'histoire de la cryptologie, rendez-vous sur le webdocumentaire réalisé par l'ANSSI.

## Pourquoi la cryptologie existe-t-elle ?

### 1. Pour assurer l'intégrité du message : le hachage

La cryptologie permet justement de détecter si le message, ou l'information, a été involontairement modifié. Ainsi, une « **fonction de hachage** » permettra d'associer à un message, à un fichier ou à un répertoire, une empreinte unique calculable et vérifiable par tous. Cette empreinte est souvent matérialisée par une longue suite de chiffres et de lettres précédées du nom de l'algorithme utilisé, par exemple « SHA2 » ou « SHA256 ».

Il ne faut pas confondre le chiffrement, qui permet d'assurer la confidentialité, c'est-à-dire que seules les personnes visées peuvent y avoir accès (voir « **Pour assurer la confidentialité du message** »), et le hachage qui permet de garantir que le message est intégrale, c'est-à-dire qu'il n'a pas été modifié.

#### Le hachage, pour quoi faire ?

Pour sauvegarder vos photos sur votre espace d'hébergement (de type « *cloud* » par exemple) et vérifier que votre téléchargement s'est bien déroulé ?

Pour synchroniser vos dossiers et détecter ceux qu'il faut sauvegarder à nouveau et ceux qui n'ont pas été modifiés ?

Il existe aussi des « **fonctions de hachage à clé** » qui permettent de rendre le calcul de l'empreinte différent en fonction de la clé utilisée. Avec celles-ci, pour calculer une empreinte, on utilise une clé secrète. Pour deux clés différentes l'empreinte obtenue sur un même message sera différente. Donc pour qu'Alice et Bob calculent la même empreinte, ils doivent tous les deux utiliser la même clé.

C'est parmi ces fonctions de hachage à clé que l'on trouve celles utilisées pour stocker les mots de passe de façon sécurisée.

#### Le hachage à clé, pour quoi faire ?

Votre service préféré reconnaît votre mot de passe quand vous vous connectez ?

Vous voulez pouvoir détecter si quelqu'un modifie des documents sans vous le dire ?

Et

### 2. Pour assurer l'authenticité du message : la signature

Au même titre que pour un document administratif ou un contrat sur support papier, le mécanisme de la « **signature** » – numérique – permet de vérifier qu'un message a bien été envoyé par le détenteur d'une « **clé publique** ». Ce procédé cryptographique permet à toute personne de s'assurer de l'identité de l'auteur d'un document et permet en plus d'assurer que celui-ci n'a pas été modifié.

#### La signature numérique, pour quoi faire ?

Vous voulez garantir être l'émetteur d'un courriel ?

Vous voulez vous assurer qu'une information provient d'une source sûre ?

Pour pouvoir signer, Alice doit se munir d'une paire de clés :

- l'une, dite « **publique** », qui peut être accessible à tous et en particulier à Bob qui est le destinataire des messages qu'envoie Alice ;
- l'autre, dite « **privée** », qui ne doit être connue que d'Alice.

En pratique, Alice génère sa signature avec sa clé privée qui n'est connue que d'elle. N'importe quelle personne ayant accès à la clé publique d'Alice, dont Bob, peut vérifier la signature sans échanger de secret.

Et

3.

### Pour assurer la confidentialité du message : le chiffrement

Le chiffrement d'un message permet justement de garantir que seuls l'émetteur et le(s) destinataire(s) légitime(s) d'un message en connaissent le contenu. C'est une sorte d'enveloppe scellée numérique. Une fois chiffré, faute d'avoir la clé spécifique, un message est inaccessible et illisible, que ce soit par les humains ou les machines.

#### Le chiffrement, pour quoi faire ?

Vous voulez vous assurer que seul le destinataire ait accès au message ?

Vous souhaitez envoyer ces informations sous enveloppe numérique et non lisible par tous comme sur une carte postale ?

Il existe deux grandes familles de chiffrement : le chiffrement symétrique et le chiffrement asymétrique.

Le **chiffrement symétrique** permet de chiffrer et de déchiffrer un contenu avec la même clé, appelée alors la « **clé secrète** ». Le chiffrement symétrique est particulièrement rapide mais nécessite que l'émetteur et le destinataire se mettent d'accord sur une clé secrète commune ou se la transmettent par un autre canal. Celui-ci doit être choisi avec précautions, sans quoi la clé pourrait être récupérée par les mauvaises personnes, ce qui n'assurerait plus la confidentialité du message.

Le **chiffrement asymétrique** suppose que le (futur) destinataire est muni d'une paire de clés (clé privée, clé publique) et qu'il a fait en sorte que les émetteurs potentiels aient accès à sa clé publique. Dans ce cas, l'émetteur utilise la clé publique du destinataire pour chiffrer le message tandis que le destinataire utilise sa clé privée pour le déchiffrer.

Parmi ses avantages, la clé publique peut être connue de tous et publiée. Mais attention : il est nécessaire que les émetteurs aient confiance en l'origine de la clé publique, qu'ils soient sûrs qu'il s'agit bien de celle du destinataire.

Autre point fort : plus besoin de partager une même clé secrète ! Le chiffrement asymétrique permet de s'en dispenser. Mais il est malheureusement plus lent.

Pour cette dernière raison, il existe une technique combinant chiffrements « **symétrique** » et « **asymétrique** », mieux connue sous le nom de « **chiffrement hybride** ».

Cette fois, une clé secrète est déterminée par une des deux parties souhaitant communiquer et celle-ci est envoyée chiffrée par un chiffrement asymétrique. Une fois connue des deux parties, celles-ci communiquent en chiffrant symétriquement leurs échanges. Cette technique est notamment appliquée lorsque **vous visitez un site dont l'adresse débute par « https »**.

[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 :  
<https://www.cnil.fr/fr/comprendre-les-grands-principes-de-la-cryptologie-et-du-chiffrement>

---

# **Conseils clé pour se protéger contre la cybercriminalité | Denis JACOPINI**

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> <i>fr</i>	 <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>#Conseils clé pour #se protéger contre la #cybercriminalité</b>				



L'avis d'expert de Jean-Philippe Sanchez, Consultant Sécurité chez NetIQ France.

**La cybercriminalité est souvent médiatisée lorsque d'énormes failles de sécurité sont révélées et que les dommages sont significatifs pour les entreprises touchées. L'attaque massive organisée par des pirates informatiques russes il y a quelques semaines à une échelle mondiale en est un très bel et marquant exemple, avec plus de 1,2 milliard de mots de passe volés.**

Mais les hackers ne se limitent pas aux attaques massives, et des petites brèches de sécurité d'apparence anodines peuvent pourtant s'avérer avoir de lourdes conséquences, tant pour les grandes entreprises que pour les plus petites organisations possédant des données sensibles ou à forte valeur ajoutée.

**Ne perdez pas votre temps à anticiper, sachez surtout détecter les failles et limiter les dégâts**  
La meilleure chose qu'un directeur informatique ou un responsable de la sécurité puisse faire pour protéger son entreprise est de comprendre et d'accepter l'impossibilité de maintenir les attaques à l'écart. Tout le monde est tôt ou tard victime d'une faille de sécurité. Le plus important est de savoir dans quel délai vous la détecterez et dans quelle mesure vous pourrez limiter les dommages. Il convient de mettre l'accent sur la réduction du risque dans les domaines clés et la surveillance des événements au niveau du pare-feu pour détecter le plus rapidement possible l'intrusion d'un attaquant et la tentative de vol de données. Toute autre action ne reviendra qu'à reproduire des stratégies qui ont déjà montré leurs limites dans le passé, pour un coût encore plus élevé.

**Avez votre stratégie de sécurité sur l'identité et les données, et non plus l'infrastructure**

Le mode de pensée centré sur le réseau et les appareils est de plus en plus délaissé en faveur d'une sécurité axée sur l'identité et les données.

Désormais, tenter de protéger l'infrastructure de l'entreprise n'apparaît plus comme une solution gagnante. Avec l'usage croissant de l'informatique mobile et du Cloud computing, cette tâche s'avère souvent trop complexe et n'est plus entièrement maîtrisée par le personnel informatique et de sécurité. En revanche, le personnel chargé de la sécurité réfléchit de plus en plus à la protection des données transférées d'un endroit à un autre, y compris dans le cloud, et à l'acquisition d'une meilleure connaissance de l'identité des individus qui ont accès à ces données. Néanmoins, suis-je certain de savoir qui accède actuellement à notre base de données de patients ? Est-il normal que ce salarié ouvre ce fichier de données clients ? Ces décisions sont de plus en plus complétées par l'introduction d'un contexte du type : dois-je permettre à ce salarié d'accéder à ces données sensibles alors qu'il est en vacances dans le Sud et qu'il se connecte depuis sa tablette dans un cybercafé ? Il s'agit là d'une façon plus intelligente (et efficace) d'appréhender les risques du comportement surveillé, en répondant aux problèmes de sécurité fondamentaux liés aux utilisateurs privilégiés, aux attaques internes et aux menaces persistantes avancées.

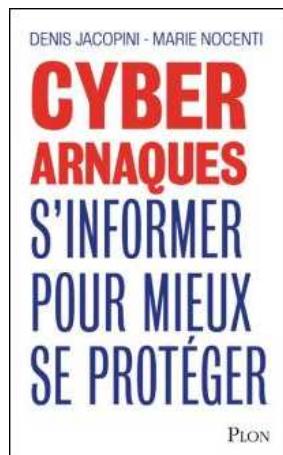
**Ne misez pas tout sur la technologie, sensibilisez vos collaborateurs car ils sont les véhicules de vos données !**

Il est toujours possible d'améliorer l'éducation – bien que je sois convaincu qu'il faille en changer le ton pour passer du « ne faites pas ceci » au « comme vous le ferez de toute façon, voici comment procéder pour éviter de prendre des risques ». Le pouvoir dans le monde de l'informatique professionnelle a changé de mains : il n'est plus dévolu au service IT autoritaire et centralisé, avec le personnel qui lui est associé, mais relève désormais des dirigeants de l'entreprise et des responsables métiers. Aujourd'hui plus que jamais, l'utilisateur de l'entreprise décide lui-même de la technologie à employer et de la façon de procéder. Dans ce contexte, l'éducation doit être recentrée sur les conseils et le choix de solutions sûres pour cesser de s'apparenter à une liste d'actions à éviter, qui sera de toute façon rarement respectée.

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



CYBERARNAQUES - S'informer pour mieux se protéger (Le Livre)  
Denis JACOPINI Marie Nocenti (Plon) ISBN :  
2259264220



Denis Jacopini, expert judiciaire en informatique diplômé et spécialisé en cybercriminalité, raconte, décrypte et donne des parades contre toutes les cyberarnaques dont chacun peut être victime.

Il est témoin depuis plus de 20 ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillements de comptes bancaires et d'autres arnaques toujours plus sournoisement élaborées.

Parce qu'il s'est rendu compte qu'à sa modeste échelle il ne pourrait sensibiliser tout le monde au travers des formations et des conférences qu'il anime en France et à l'étranger, il a imaginé cet ouvrage afin d'alerter tous ceux qui se posent la question : Et si ça m'arrivait un jour ?

Plutôt que de présenter une longue liste d'arnaques Internet recensées depuis plusieurs années, Denis Jacopini, avec la collaboration de Marie Nocenti, auteur du roman *Le sourire d'un ange*, a souhaité vous faire partager la vie de victimes d'arnaques Internet en se basant sur des faits réels, présentés sous forme de nouvelles suivies de recommandations pour s'en prémunir. Et si un jour vous rencontrez des circonstances similaires, vous aurez le réflexe de vous méfier sans risquer de vivre la fin tragique de ces histoires et d'en subir les conséquences parfois dramatiques.

Pour éviter de faire entrer le loup dans votre bergerie, il est essentiel de le connaître pour le reconnaître !

Commandez sur [Fnac.fr](http://Fnac.fr)

---

<https://www.youtube.com/watch?v=lDw3kI7ra2s>

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 2010 (Symantec) 13,8 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 risque ? 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.

---

Commandez sur Fnac.fr

---

[https://youtu.be/usg12zkRD9I?list=UUoHqj\\_HKcbzRuvIPdu3FktA](https://youtu.be/usg12zkRD9I?list=UUoHqj_HKcbzRuvIPdu3FktA)

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 coécrit 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

Source

: <http://www.generation-nt.com/cybercriminalite-hacker-netiq-jean-philippe-sanchez-actualite-1905811.html>

---

# Si un courriel personnel n'est pas identifié comme tel, l'employeur peut-il l'examiner ?

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

 <b>LE NET EXPERT</b> AUDITS & EXPERTISES	 <b>LENETEXPERT</b> fr	 <b>LE NET EXPERT</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>Si un courriel personnel n'est pas identifié comme tel, l'employeur peut-il l'examiner ?</b>		

Si un courriel personnel n'est pas identifié comme tel, l'employeur peut-il l'examiner ?

Si le courriel n'est pas intitulé «Personnel», mais, par exemple, «félicitations pour la naissance de...» Il est évident que c'est personnel.

[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 : Connaissez-vous vos droits sur les données personnelles au travail (VRAI-FAUX) ? – La Voix du Nord

# Les documents enregistrés dans un fichier « Mes documents », sont-ils inaccessibles à l'employeur ?

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
 <b>LE NET EXPERT</b> AUDITS & EXPERTISES	 <b>LENETEXPERT</b> .fr EXPERTISES DE SYSTÈMES DE VOTES ELECTRONIQUES	 <b>LE NET EXPERT</b> MISES EN CONFORMITÉ	 <b>SPY DETECTION</b> Services de détection de logiciels espions	 <b>LE NET EXPERT</b> FORMATIONS	 <b>LE NET EXPERT</b> ARNAQUES & PIRATAGES



## Les documents enregistrés dans un fichier « Mes documents », sont-ils inaccessibles à l'employeur ?

### Les documents enregistrés dans un fichier « Mes documents », sont-ils inaccessibles à l'employeur ?

« Mes documents » est un terme générique. C'est encore une fois la mention « Personnel » qui permet de protéger un dossier ou un fichier. L'employeur ne peut donc pas en faire état, au risque d'avoir à payer des dommages et intérêts à son salarié. »

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"]

---

Source : *Connaissez-vous vos droits sur les données personnelles au travail (VRAI-FAUX) ? – La Voix du Nord*