

Lyrebird, une technologie pour faire dire n'importe quoi à n'importe qui

Lyrebird, une technologie pour faire dire n'importe quoi à n'importe qui

---

« Alors que l'IA commence à comprendre et synthétiser toutes sortes de choses, de la voix humaine au style des grands peintres, nous entrons dans une ère où tout ce qui peut être numérisé peut être imité par une IA », écrivent les chercheurs dans un article publié le 18 mai.

Ils en veulent pour preuve des avancées technologiques comme Lyrebird et Face2Face, qui rendent crédibles la possibilité de fabriquer des images et des sons difficiles à distinguer de la réalité dans un futur proche. « L'ère post-vérité ne fait que commencer », prennent-ils le soin de nous avertir.

Sources : DT R&D/Medium

---

**Notre métier :** Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

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



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

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)



Réagissez à cet article

Source : *Cet appareil vous avertit quand une IA tente de se faire passer pour un humain*

# **Les victimes de Cyberattaque sont aussi responsables de manquement à leur obligation de sécurité**



**Les victimes  
de  
Cyberattaque  
sont aussi  
responsables  
de  
manquement à  
leur  
obligation  
de sécurité**

**Demain, les sociétés victimes d'une cyberattaque pourront être plus facilement attaquées en responsabilité par les clients lésés. Ce sera la double peine...**

Difficile d'échapper à la nouvelle, les médias ont largement relayé l'information de la cyberattaque à large échelle perpétrée en fin de semaine dernière. Cette attaque a pris la forme pernicieuse d'un « ransomware », c'est-à-dire d'un cryptage de données couplé à une demande de rançon. Et gare à ceux qui ne voulaient pas obéir, la menace d'une destruction des données concernées était supposée les ramener dans le droit chemin.

Selon les informations disponibles par les médias, l'attaque aurait visé des entreprises qui utilisaient encore l'ancien système d'exploitation Windows XP, un système pour lequel Microsoft avait cessé de proposer des mises à jour depuis peu de temps. Mais comme le fait remarquer l'avocat Adrien Alberini au journal suisse *Le Temps*, cette situation complexe donne lieu à ce qu'on peut qualifier de « paradoxe de la cyberattaque »: aussi surprenant que cela puisse paraître, les entreprises cibles d'une cyberattaque s'exposeront au final à un risque de sanctions significatives.

Ce paradoxe – la victime doublement victime en quelque sorte – s'explique en réalité par le renforcement du droit de la protection des données. Mais ces nouvelles exigences en matière de protection de données ne seront pas faciles à respecter, d'où le risque d'une attaque en responsabilité pour les entreprises victimes d'une cyberattaque. En bref, peu de chefs d'entreprises le savent, mais une réglementation modernisée en matière de protection des données – dénommée GDPR (General Data Protection Regulation) – entrera en vigueur l'année prochaine en Europe...[lire la suite]

---

**Notre métier :** Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

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

---



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

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTF N°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Source : *Cyberattaque: le paradoxe de la double peine pour les entreprises – High-tech – Trends-Tendances.be*

---

# Journée de la Biométrie – 2ème édition le 7 juillet 2017 à l'ENSICAEN

The poster features the following text and logos:

- Logos of sponsors: ENSI CAEN, Pôle TES e-secure transactions, AD Normandie, Orange, and Normandie Université.
- Demonstrations and conferences.
- Logo: JOURNÉE DE LA BIOMÉTRIE SAVE THE DATE.
- Target audience: Public académique industriel.
- Visuals: A hand, a fingerprint, a green eye, and a profile of a person's head.
- Date and location: Le 7 juillet 2017, ENSICAEN, 6 boulevard Maréchal Juin, 14000 Caen.
- Logos of partners: GREYC, CNRS, and INGEM.

On the right side of the poster, the event details are repeated in large red text:

Journée de la Biométrie  
2ème édition le 7 juillet 2017 à l'ENSICAEN

**Suite au succès de The Biometrics Day In Normandy de novembre 2014, le Laboratoire GREYC en partenariat avec l'ENSICAEN, le Pôle TES, l'AD Normandie, Orange et Normandie Université organise la seconde édition le 7 juillet prochain.**

La journée dédiée aux acteurs de la Biométrie, enseignants-chercheurs et partenaires industriels, sera ponctuée de conférences, de démonstrations et de temps d'échanges. L'occasion de faire connaître les activités de recherche dans ce domaine, mettre à l'honneur les innovations et la vision de demain de la Biométrie.

L'inscription est gratuite mais obligatoire : inscription

Journée de la Biométrie – vendredi 7 juillet 2017, de 9h30 à 17h

ENSICAEN – 6 Boulevard Maréchal Juin – Caen

#### Téléchargez l'affiche

---

**Notre métier :** Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

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

---



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

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Source : *Journée de la Biométrie – AD Normandie*

# EternalRocks, le successeur de WannaCry encore plus inquiétant ?

 <p>Denis JACOPINI VOUS INFORME LCI</p>	<p>EternalRocks, le successeur de WannaCry encore plus inquiétant ?</p>
--	---

**Après l'attaque du ransomware WannaCry, les chercheurs ont identifié le ver de réseau EternalRocks. Celui-ci utilise jusqu'à 7 outils de hacking ayant été volés à la NSA puis exposés par le groupe Shadow Brokers.**

Selon Malwarebytes, WannaCry a recherché les ports SMB vulnérables avant d'utiliser EternalBlue pour rentrer sur le réseau et le backdoor DoublePulsar pour installer le ransomware. EternalRocks utilise aussi ces deux outils. (crédit : D.R.)

Une semaine après l'attaque perpétrée par le ransomware WannaCry au niveau mondial, un autre logiciel d'exploitation de failles fait parler de lui. Selon des chercheurs en sécurité, il y a au moins une personne qui utilise 7 des outils d'attaque volés à la NSA dans un ver de réseau dénommé EternalRocks par ceux qui l'ont identifié. Les chercheurs ont constaté que ce ver ciblait la même vulnérabilité du protocole SMB de Windows, en s'avérant plus menaçant et plus difficile à contrer. Comme WannaCry, EternalRocks utilise EternalBlue, l'un des outils de la NSA.

Malwarebytes pense que WannaCry n'a pas été diffusé par une campagne de spams malveillants mais par une opération de scanning qui a d'abord recherché les ports SMB accessibles publiquement et vulnérables avant d'utiliser EternalBlue pour rentrer sur le réseau et d'utiliser la porte dérobée DoublePulsar pour installer le ransomware...[lire la suite]

---

**Notre métier :** Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

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

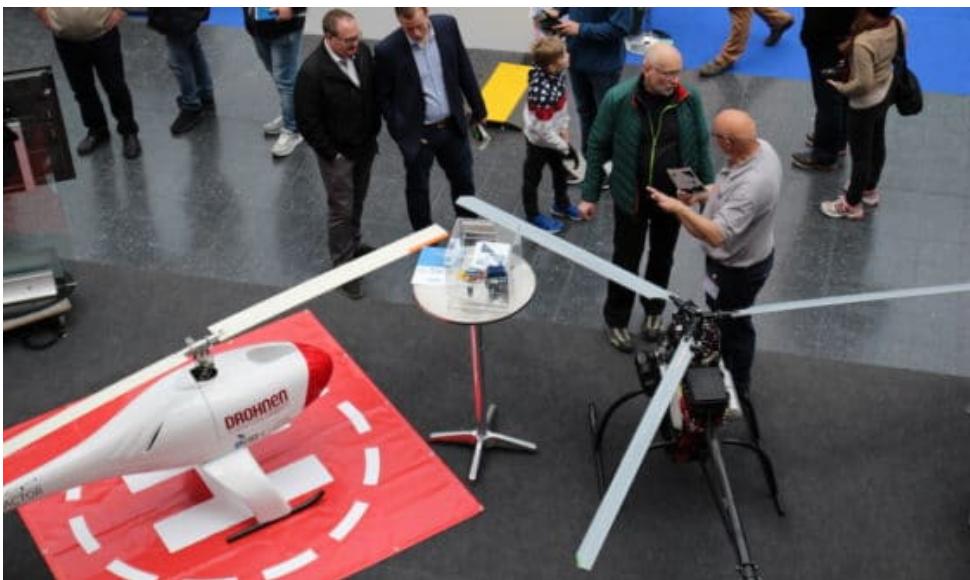
---



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

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

# Les drones civils aussi devront répondre au concept de « Privacy by Design »



Les  
drones  
civils  
aussi  
devront  
répondre  
au  
concept  
de  
« Privacy  
by  
Design »

D'ici un an, les opérateurs de drones comme les fabricants, auront l'obligation de mettre en œuvre des « mesures techniques et opérationnelles appropriées » afin protéger les droits des personnes et des données. Laurent Archambault, avocat à la Cour, explique ici comment les acteurs de la filière drone, en Europe à partir du 25 mai 2018, devront non seulement acheter ou concevoir des drones qui prennent en compte cette question, planifier leurs missions dans cet état d'esprit, mais aussi adopter une organisation qui permette une protection maximisée des tiers et de leurs données.

Les drones sont par essence des appareils permettant des prises de vue ou la captation de données, discrètement. La grande majorité de ces aéronefs est de petite taille. Ils peuvent voler près du sol, longer des édifices ou encore suivre une personne de jour comme de nuit. Comme souligné par Edouard Geffray, Secrétaire général de la CNIL, la problématique du drone pour la vie privée et la protection des données réside d'ailleurs, non pas tant dans l'emport de capteurs, mais bien dans la mobilité et la discréetion du drone.

A cet égard, le concept de « *Privacy by Design* » pourrait constituer un moyen de limiter, voire de supprimer tant les atteintes à la vie privée que la captation de données personnelles par drone (ces dernières pouvant être grossièrement définies, comme des «*données non anonymes* »). Insistons sur le fait qu'à l'ère du numérique, ces deux domaines sont poreux entre eux..[lire la suite]

---

#### A Lire aussi :

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

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

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

Comprendre le Règlement Européen sur les données personnelles en 6 dessins

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

---

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

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

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

---



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

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Source : *Le concept de « Privacy by Design » à la rescousse des drones civils européens* – Aerobuzz

---

## Mieux protéger les TPE/PME du cyber-risque



Mieux  
protéger les  
TPE/PME du  
cyber-risque

---

**Les cyberattaques concernent tous les acteurs de la société: particuliers, entreprises ou administrations. Mais force est de constater que les principaux impactés sont généralement les entreprises de petite ou de moyenne taille.**

Une étude IFOP montre que, en France, près de **77% des cyberattaques toucheraient les TPE/PME**. Par ailleurs, les dommages de ces attaques numériques peuvent se révéler d'une importance telle qu'elle pourrait compromettre l'avenir même de l'entité touchée. Outre la **baisse ou l'interruption des activités** pendant une certaine durée, une cyberattaque peut également **impacter la réputation ainsi que les relations contractuelles** de l'entreprise touchée, notamment celles avec ses partenaires et/ou sa clientèle.

Pourtant, seulement un tiers des entreprises de petite ou moyenne taille se dit consciente des dangers d'une cyberattaque et prend les précautions de prévention nécessaires. Pour les autres, elles disposeraient de systèmes vulnérables et facilement accessibles aux hackers.

### **Les assureurs : nouveaux acteurs de la cybersécurité**

Si la plupart des assureurs proposent désormais aux professionnels des assurances cyber-risques et e-reputation, un assureur a décidé d'aller plus loin. Generali s'associe à ENGIE Ineo et Europ Assistance pour lancer une offre d'assurance spécifique pour les TPE/PME. Cette dernière vise la réparation et l'indemnisation de ces entreprises en cas de cyberattaque. Le partenariat entre les trois sociétés a pour but d'optimiser au maximum la prise en charge de l'entreprise touchée. Elle sera axée sur trois points :

#### **Europ Assistance assurera une prise en charge immédiate :**

Europ Assistance dispose d'un service d'assistance informatique disponible à tout moment. Elle prendra en charge l'entreprise victime d'une cyberattaque dans les plus brefs délais. Les chargés d'assistance travailleront en collaboration avec les experts informatiques d'Engie Ineo. Ils mettent également en place un accompagnement humain de l'entreprise afin de s'assurer qu'elle comprenne les différentes étapes du processus de restauration.

#### **La réparation des données par Engie Ineo**

Une fois la cyberattaque avérée, la société Engie Ineo sera chargée de restaurer les données informatiques. A cet effet, son équipe technique devra effectuer une enquête pour établir un diagnostic et déceler les preuves de l'attaque. Ils doivent ensuite reconstituer et restaurer les différentes données volées ou cryptées par les hackers. Le contrat d'assurance prévoit une garantie « temps d'intervention » d'une heure. Enfin, les services informatiques de l'entreprise devront étroitement collaborer avec la société Engie Ineo.

#### **Generali indemnisera les dommages**

Pour l'assureur Generali, sa mission tiendra à l'indemnisation des dommages matériels mais aussi des pertes financières découlant de l'attaque. Elle prendra donc en charge les frais d'expertise et de restauration des données, les pertes d'exploitation ainsi que la responsabilité civile et autres frais générés par la cyberattaque. Pour couvrir exactement chaque entreprise assurée, Generali prévoit de mettre en place un questionnaire spécifique afin d'évaluer le niveau d'exposition de l'entreprise au risque d'attaque numérique et d'adapter la protection selon sa taille.

**Notre métier :** Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

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



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

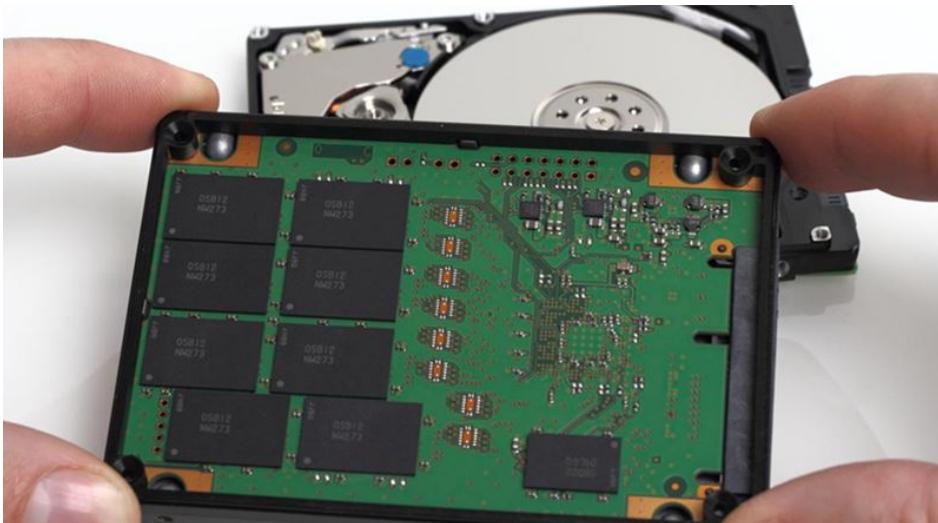
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRETEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondant Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Réagissez à cet article

Source : *Cyberattaques: l'assurance se développe*

# SSD : une faille de sécurité les rend vulnérables aux attaques de hackers !



SSD : une faille de sécurité les rend vulnérables aux attaques de hackers !

Les SSD sont vulnérables aux attaques de hackers en raison d'une faille de sécurité affectant la mémoire flash NAND MLC, rapporte une étude...[Lire la suite ]

---

**Notre métier :** Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur cette page.

---



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

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



[Contactez-nous](#)

Réagissez à cet article

---

# La Russie enfin favorable à une coopération Internationale



La Russie  
enfin favorable à  
une coopération  
internationale

**Moscou a mis au point un projet de convention internationale sur la lutte contre la criminalité informatique qui doit faciliter la coopération entre divers pays en la matière.**

La Russie a présenté aux Nations unies un projet de convention, sur la coopération dans la lutte contre la cybercriminalité, censé protéger les technologies informatiques face à l'intensification des cyberattaques et simplifier la traduction des contrevenants en justice.

Selon Ioulia Tomilova, responsable du ministère russe des Affaires étrangères, le document proposé par Moscou se base sur les dispositions de plusieurs conventions déjà adoptées, dont la Convention de Budapest sur la cybercriminalité de 2001, la Convention de l'Onu contre la corruption, et d'autres.



© PHOTO. IMAGO SPORT AND NEWS

Le texte russe introduit au niveau législatif des États signataires la responsabilité pénale pour les actes de cybercriminalité et explicite la nécessité de développer la coopération internationale dans ce domaine, notamment par l'échange d'informations.

Les dispositions du nouveau document permettront également d'extrader les criminels d'un pays vers un autre même en l'absence de traité d'extradition entre les États concernés.

Au total, le projet de convention criminalise 14 différents types d'activités criminelles, dont l'accès illégal aux informations sur un ordinateur, la création et l'utilisation de logiciels malveillants, l'envoi de courriers électroniques non sollicités et la diffusion de la pornographie juvénile, explique Mme Tomilova...[lire la suite]

---

**Notre métier :** Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

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



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

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Source : *Cybercriminalité: Moscou veut mobiliser les Nations unies*

---

# La cyberattaque ‘‘WannaCry’’ aurait déjà coûté... 1 Milliard de dollars



La  
cyberattaque  
WannaCry  
aurait déjà  
coûté...  
1  
Milliard de  
dollars

**La cyberattaque globale WannaCry a causé des dégâts s'élevant à 1 milliard de dollars, relate le cabinet spécialisé ‘‘McClatchyDC’’. Ces dommages ont été causés par l’immobilisation de la production de grandes entreprises dans le monde entier.**

Une situation liée à la perte de données, à la réduction de la productivité, à des perturbations du travail, au préjudice porté à la réputation, ainsi qu'à plusieurs autres facteurs.

La cyberattaque utilisant le virus WannaCry est considérée comme le plus grand piratage à rançon de l'histoire.

L'attaque a fait, selon Europol, 300 000 victimes dans au moins 150 pays depuis le 12 mai.

Et parmi les organisations touchées par cette attaque, on retrouve notamment Vodafone, FedEx, Renault, le National Health Service britannique ou encore la Deutsche Bahn.

Rédaction Infomédiaire

#### **Remarques de Denis JACOPINI**

L'évolution de ce virus et les dégâts qu'il produit sont à la mesure du nombre d'ordinateurs interconnectés dans le monde.

Pour ma part, ce virus n'a à ce stade, rien d'exceptionnel en terme d'ampleur. Il suffit de se renseigner un peu et découvrir que le virus Conficker, un ver informatique exploitant une faille de Windows, apparu en 2008 a touché, d'après les estimations 15 millions de victimes alors qu'il y avait 2 milliards d'internautes en moins (57% en moins car aux alentours de 3.5 milliard aujourd'hui et seulement aux alentours de 1,5 milliard en 2018 <http://www.journaldunet.com/ebusiness/le-net/1071539-nombre-d-internautes-dans-le-monde>)

---

**Notre métier :** Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

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

---



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

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Source : *Economie mondiale : La cyberattaque ‘‘WannaCry’’ a coûté... 1 MM\$ | Infomédiaire*

[http://www.liberation.fr/futurs/2017/05/15/guillaume-poupart-la-cybercriminalite-devient-une-question-de-securite-nationale\\_1569743](http://www.liberation.fr/futurs/2017/05/15/guillaume-poupart-la-cybercriminalite-devient-une-question-de-securite-nationale_1569743)

---

# Les recommandations de Microsoft pour se protéger de WannaCry



**Il fait le buzz à travers les systèmes d'exploitation de Microsoft, Windows, son nom c'est WannaCry.**  
**VOICI LES ÉTAPES POUR SE PROTÉGER DE CETTE MENACE :**  
En mars dernier, nous avons publié une mise à jour de sécurité (MS17-010) qui corrige la vulnérabilité exploitée par ces attaques. Tous les clients ayant Windows Update activé sur les versions de Windows supportées, sont donc protégés contre cette attaque.

**1.D éployer le bulletin de sécurité MS17-010 :**  
Nous conseillons d'ailleurs à toutes les organisations qui n'ont pas encore appliqué cette mise à jour de sécurité, de déployer immédiatement le Bulletin de sécurité Microsoft MS17-010.  
Nous savons aussi que certains de nos clients entreprises et utilisateurs grand public exploitent encore des versions de Windows qui ne sont plus supportées. Ils n'ont donc pas reçu cette mise à jour de sécurité en mars. Compte-tenu de l'impact potentiel de cette attaque et afin d'en limiter la propagation, Microsoft a pris la décision de publier pour tous nos clients, même s'ils ne disposent pas d'un Custom Support Agreement, les mises à jour de sécurité permettant de corriger cette vulnérabilité pour Windows XP SP3, Windows 8 et Windows Server 2008 SP2.

**2. Mettre à jour votre antivirus**  
Windows Defender, System Center Endpoint Protection, et Forefront Endpoint Protection détectent cette famille de virus sous le nom de Ransom:Win32/WannaCrypt.  
En complément, l'outil Microsoft Safety Scanner <http://www.microsoft.com/security/scanner/> disponible gratuitement, a été mis à jour pour détecter aussi cette famille de virus.

**En cas de menace avérée :**  
Si vous êtes victimes par cette attaque contacter le support Microsoft

**3. Procédez à la restauration de votre machine**  
<https://blogs.technet.microsoft.com/mmpc/2016/05/18/the-5ws-and-1h-of-ransomware/>  
<https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx>

**Liens utiles :**  
1. Microsoft Guidance for WannaCrypt  
2. Microsoft Malware Prevention Center Technical Details about the ransomware worm  
3. MS17-010 Update Catalogue

**Notre métier :** Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.  
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement... (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)  
Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis JACOPIN est Expert Judiciaire en Informatique spécialisé en « Sécurité » < Cybercriminalité > et en protection des données à caractère Personnel ».  
→ Auteur de plusieurs ouvrages :  
• Expertises techniques et judiciaires (Avis techniques, Recherche de preuves, téléphones, tablettes, ordinateurs, serveurs, documents numériques, analyses d'identité...);  
• Expertises sur les systèmes de vote électronique ;  
• Formations et conférences en cybersécurité ;  
• Accompagnement à la mise en place d'un CIL (Correspondant Informatique et Libertés);  
• Accompagnement à la mise en conformité RGPD de votre établissement.



Contactez-nous

Réagissez à cet article

**Source : Les recommandations de Microsoft pour se protéger de WannaCry – Socialnetlink-La référence technologique en Afrique**