

**Cybersécurité : quand les collectivités prennent la mesure du problème**

x	<b>Cybersécurité : quand les collectivités prennent la mesure du problème</b>
---	---

---

A l'heure où la cybersécurité est un enjeu croissant pour les acteurs publics, les collectivités semblent se prendre enfin en main. La ville de Marseille a mis en place une initiative pour tester ses défenses. Dans le même temps, la région Hauts-de-France a, elle, été choisie pour être le théâtre d'une expérimentation de l'ANSSI.

Pour de nombreuses collectivités locales, la cybersécurité reste encore aujourd'hui un enjeu abstrait. A quelques exceptions près, ces dernières ne sont pas armées pour résister à des attaques très virulentes et aveugles. Et pourtant, les offensives font de plus en plus mal. En témoignent les dégâts causés en mai dernier par le rançongiciel WannaCry, qui a paralysé plus de 200 000 machines à travers près de 150 pays, dont des opérateurs d'importance vitale en France.

L'ampleur de l'offensive n'a fait que confirmer ce que tout le monde savait depuis longtemps : personne n'est à l'abri. Des solutions commencent toutefois à être mises en place par les collectivités elles-mêmes. Un changement de paradigme plus que nécessaire.

## Marseille joue la carte prévention

La ville de Marseille a ainsi inauguré le 6 juin une initiative visant à permettre à la municipalité de tester l'efficacité de ses défenses à tous les niveaux. Concrètement, une vingtaine d'étudiants issus de l'école Polytech – l'initiative étant réalisée en partenariat avec l'Université Aix-Marseille – cherchera les éventuelles failles dont la municipalité n'aurait pas connaissance.

Les sites web, applications mais aussi les objets connectés seront passés au crible par ces « hackers éthiques ». Pour ce faire, ces derniers utiliseront SafeGouv, un service proposé par la start-up Net Guard...[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>



Réagissez à cet article

Source : *Cybersécurité : quand les collectivités prennent la mesure du problème*

---

**Données personnelles : « les collectivités vont devoir se lancer dans une démarche de mise en conformité »**

	<b>RGPD : « les collectivités vont devoir se lancer dans une démarche de mise en conformité »</b>
---	---

---

**A un an de l'entrée en vigueur du règlement européen sur la protection des données. Alice de La Mure, juriste au service Correspondants informatiques et libertés de la CNIL, revient sur les nouvelles obligations qui concernent largement les collectivités territoriales**

Le règlement général sur la protection des données (RGPD), adopté par le Parlement européen le 14 avril 2016, sera directement applicable dans les Etats membres le 25 mai 2018. Il sera alors le texte de référence concernant la protection des données à caractère personnel. Il consolide, voire renforce, les grands principes de la loi Informatique et Libertés.

Divers axes s'en dégagent, dont plusieurs concernent directement les collectivités territoriales :

- la responsabilisation globale de l'ensemble des acteurs ;
- le renforcement des droits des personnes, avec notamment l'avènement du droit à la portabilité et du droit à la limitation du traitement ;
- l'augmentation du montant des sanctions susceptibles d'être prononcées par la CNIL : la loi du 7 octobre 2016 pour une République numérique avait ...[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>



Réagissez à cet article

**Source :** *Données personnelles : « les collectivités vont devoir se lancer dans une démarche de mise en conformité »*

---

# Les collectivités territoriales cibles des Pirates Informatiques

x	Les collectivités territoriales cibles des Pirates Informatiques
---	--

---

**Si elles n'en ont pas toujours conscience, les collectivités territoriales peuvent bel et bien être victimes de cyberattaques. Et ce, pour de multiples raisons. En cas de faute avérée, les sanctions encourues peuvent devenir particulièrement difficiles à assumer.**

Par Pierre-Alexandre Conte

Une République numérique. C'est ainsi qu'a été baptisée la loi portée par l'actuelle secrétaire d'Etat chargée du numérique, Axelle Lemaire, parue le 8 octobre 2016 au « Journal officiel ». Un nom à combien symbolique et révélateur de la profondeur de la transformation vécue par l'ensemble de la société.

Celle-ci touche naturellement les collectivités territoriales, qui bénéficient des multiples avantages qu'elle génère, mais qui doivent, dans le même temps, composer avec de nouvelles obligations. Parmi elles, figure en tête de liste la sécurisation de leur système d'information.

En préambule de son rapport d'activité annuel paru en 2016, l'Agence nationale de la sécurité des systèmes d'information (Anssi) introduisait le sujet comme suit : « Les technologies numériques procurent des gains de productivité et sont donc source de richesse et de compétitivité pour notre pays, mais elles induisent également des vulnérabilités nouvelles. La cybersécurité est devenue, de ce fait, une condition structurante, non seulement de la sauvegarde de notre patrimoine économique et intellectuel, mais aussi de la protection physique de nos concitoyens. » Des propos signés Louis Gautier, secrétaire général de la défense et de la sécurité nationale.

#### FOCUS

Dans son rapport d'activité concernant l'année 2015, l'Anssi explique avoir reçu 4 000 signalements, soit 50 % de plus qu'en 2014. L'Agence a aussi dû traiter une vingtaine d'incidents de sécurité majeurs.

### Les sites web en première ligne

La première erreur en matière de sécurité informatique consiste à penser qu'une collectivité, quelle que soit sa nature, n'a aucune raison d'être la cible d'une attaque. C'est pourtant un raisonnement fréquemment rencontré au sein des petites et moyennes communes, qui considèrent parfois qu'elles ne détiennent rien qui puisse intéresser d'hypothétiques assaillants. « Comme tout un chacun qui dispose d'une visibilité sur internet, les collectivités territoriales peuvent faire partie des victimes d'une vague d'attaques, précise Guy Flament, référent de l'Anssi au sein de la région Nouvelle Aquitaine.

Leur présence sur internet, notamment par le biais de leurs sites web, offre des surfaces pour les attaquants, qui peuvent leur permettre d'afficher des messages de revendication ou de propagande. Ensuite, les collectivités subissent des attaques par des « rançongiciels » qui prennent en otage leur système d'information et offrent de le libérer contre une rançon. En ce qui concerne les autres menaces informatiques que peuvent être le sabotage ou l'espionnage, elles ne sont pas, pour le moment, particulièrement visées. Mais elles pourraient le devenir, notamment à cause du nombre de données à caractère personnel qu'elles hébergent. »

#### À LIRE AUSSI

- Plusieurs milliers de sites Internet de communes mal sécurisés

Les collectivités territoriales brassent en effet de plus en plus de données, dont certaines s'avèrent particulièrement sensibles. Elles sont au cœur de toutes les préoccupations, comme en témoignent les nombreux articles qui leur sont consacrés au sein de la loi pour une République numérique. Il convient donc de les protéger.

« Les collectivités détiennent notamment l'état civil. Il ne faudrait pas qu'un jour ces fichiers puissent être modifiés par des attaquants. Les comptes de la commune intéressent aussi les gens et tout ce qui touche aux dossiers de consultation publique », lance Guy Flament.

#### À LIRE AUSSI

Notre dossier : Données personnelles, un gisement sous haute protection

### Sanctions pénales

La protection des données du citoyen est garantie par la loi « informatique et libertés ». C'est évidemment la Commission nationale de l'informatique et des libertés (Cnil) qui veille au respect de cette dernière. Ses compétences ont été élargies par la loi pour une République numérique.

Sur le plan financier, les collectivités encouruent une amende pouvant s'élever jusqu'à 3 millions d'euros ; ce n'est pas rien ! La Cnil peut aussi ordonner que l'organisme sanctionné informe à ses frais les victimes. La loi prévoit par ailleurs la possibilité de sanctionner pénalement les maires, les présidents de conseils régionaux et de conseils généraux en cas de manquement grave, comme le fait de ne pas prendre les mesures nécessaires pour garantir la confidentialité des informations ou l'utilisation de ces dernières à d'autres fins.

A partir du mois de mai 2018, les collectivités devront appliquer le règlement européen sur le sujet. Concernant ce dernier, selon Pierre Deprez, avocat du cabinet DS avocats dans le département « droit de la propriété intellectuelle, technologies numériques et data », on parle d'un « changement de paradigme ». Cela signifie le passage « d'un régime de déclaration et d'autorisation des traitements à un régime d'accountability, d'autoresponsabilité ».

Les communes devront conserver « une trace des moyens techniques et organisationnels qu'elles auront mis en œuvre pour assurer la sécurité des données », dans le but de montrer patte blanche en cas de contrôle.

Mais les données ne sont pas l'unique préoccupation des collectivités. D'autres domaines requièrent leur attention, à l'image des objets connectés. Ce sont de formidables outils, mais ils peuvent aussi se retourner contre ceux qui les utilisent.

« Les objets connectés, comme les smartphones il y a quelques années, représentent une augmentation de la surface d'attaque puisqu'ils sont, par nature, connectés à internet. Si ces objets ne sont pas correctement configurés et sécurisés, ils offrent une porte d'entrée à d'éventuels attaquants », précise Guy Flament.

### Des risques divers

« L'émergence des outils connectés implique de prendre ses précautions, déclare de son côté Olivier Fouqueau, directeur général des services d'Infocom94, syndicat intercommunal informatique du Val-de-Marne. Quand une direction générale des services techniques, voire un élu, décide que c'est super d'équiper toutes les places de parking d'un capteur pour permettre de savoir, à distance, par le biais de son téléphone portable, s'il y a une place pour se garer, mais qu'il n'y a pas de sécurité autour, cela peut très vite devenir difficile à gérer. »

Les rapports affirmant que la cybercriminalité est en constante augmentation sont rendus publics de manière quasi quotidienne. Pour autant, il n'est pas si évident de trouver une collectivité territoriale qui accepte de faire part d'une mauvaise expérience. La raison est simple : elle relève de la peur de voir son image se détériorer. C'est là l'un des principaux risques encourus, notamment par les villes.

« Il ne se passe pas une journée sans qu'il y ait un site internet défiguré dans la région », déplore le référent de l'Anssi en Nouvelle Aquitaine. En cas de pertes de données et de responsabilité avérée, le règlement européen demandera également aux collectivités, en 2018, d'informer le public quant à ses failles de sécurité. Si les communes sont concernées par leur image, elles doivent en plus composer avec l'inaccessibilité de leur site. Ce qui peut altérer de manière plus ou moins grave la mission de service public.

La perte peut aussi être financière, notamment s'il y a demande de rançon, les sommes demandées étant, la plupart du temps, élevées.

« Le sujet de la sécurité est souvent diabolisé, regrette Frank Mosser, expert dans le domaine de la cybersécurité et président de MGDIS, société éditrice de services logiciels de pilotage et de valorisation de l'action publique, basée à Vannes. Quand ça fait trop peur, on a tendance à mettre la tête dans le sac et à faire l'autruche. Il y a quelques années, ce n'était pas si grave que cela. Là, ça le devient un peu plus. »

#### FOCUS

### Le « rançongiciel », fléau international en pleine expansion

Extorsion Tout le monde ou presque a entendu parler de Locky. Ce « ransomware » « rançongiciel » en français – s'est rendu populaire en faisant de nombreuses victimes au cours de l'année passée. Une fois activé sur l'ordinateur de la personne visée, ce dernier chiffre les données et demande une somme d'argent en échange de leur restitution. S'il reste l'exemple le plus connu, Locky n'est pas un cas unique. Loïn de là.

290 millions de dollars – Le FBI estime que durant le premier trimestre de l'année 2016, environ 209 millions de dollars ont été extorqués par le biais de « rançongiciels ». Aux Etats-Unis, le Hollywood Presbyterian Medical Center a fait partie des victimes au mois de février 2016. Paralysé pendant plus d'une semaine, il avait fini par déboursar la somme de 17 000 dollars pour reprendre une activité normale. Et ce, après avoir dû envoyer de nombreux patients vers d'autres établissements.

Une mésaventure similaire est arrivée trois mois plus tard au Kansas Heart Hospital. Mais cette fois, après avoir payé la rançon, l'hôpital n'a pas pu récupérer ses fichiers. Pire, une seconde somme d'argent lui a été demandée. Fin janvier, c'est la police de Washington qui s'est aperçue que le réseau de vidéosurveillance de la ville ne fonctionnait plus correctement.

Avant de prendre connaissance du problème : depuis le 12 janvier, un « ransomware » avait commencé à faire son œuvre, paralysant 123 des 187 caméras utilisées. En cherchant la source du dysfonctionnement, des enquêteurs sont tombés un peu plus tard sur un message les invitant à payer une somme. Ce qui n'a pas été fait. Le réseau a été réinstallé dans l'urgence.

#### FOCUS

### L'expérience traumatisante d'une commune piratée

Chaque jour ou presque, des collectivités découvrent qu'elles ont été victimes d'une attaque informatique. Mais difficile de témoigner à visage découvert. Voici ce qu'une victime raconte, sous couvert d'anonymat : « Nous sommes arrivés un matin et nos postes informatiques étaient bloqués, explique cette directrice générale des services. Impossible de travailler dans ces conditions. Sur les écrans était affiché un message énigmatique et surtout, une demande de rançon. »

Si la police a rapidement été prévenue, la commune a dû se résoudre à trouver une solution au plus vite pour reprendre une activité normale. « Nous ne pouvions pas payer la somme, explique-t-elle. Nous avons appelé notre prestataire informatique qui a fait le déplacement et nous a indiqué qu'une grande partie de nos données, notamment les plus récentes, étaient perdues.

Personne n'avait anticipé le problème. Cela a créé beaucoup de remous au sein de la collectivité, dans la mesure où nous ne savons pas qui est responsable de l'attaque. L'enquête est toujours en cours. Plusieurs pistes ont été évoquées, dont des personnes hostiles à certaines décisions locales. C'est une expérience qui reste encore assez traumatisante pour nous. »

Si le prestataire informatique a fourni une solution d'appoint pour que les données soient plus fréquemment sauvegardées, aucun changement en profondeur, en termes de sécurité, n'a été apporté à ce jour.

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>



Réagissez à cet article

Source : *Cybersécurité : les collectivités territoriales, des cibles potentielles sous surveillance*

---

# La moitié des écoles de Bordeaux victimes d'un ransomware

x	La moitié des écoles de Bordeaux victimes d'un ransomware
---	---

---

**Les ransomwares font de nouvelles victimes. Un établissement de santé gérant 5 hôpitaux de l'est de Londres et une quarantaine d'écoles de Bordeaux sont tombés dans leurs filets.**

Selon nos confrères de Sud-Ouest, pas loin d'une école bordelaise sur deux a été la victime d'une attaque informatique. Le phénomène a démarré en septembre et s'est accéléré jusqu'aux vacances de Noël, pour toucher au total les serveurs d'environ 40 établissements sur les 101 écoles que compte la préfecture de la Gironde. Un audit est en cours pour tenter de déterminer l'origine de l'infection. L'adjointe au maire en charge de l'éducation, Emmanuelle Cuny, parle d'une attaque « *sans précédent* ».

S'il est encore trop tôt pour se montrer catégorique, l'infection semble provenir d'un ransomware qui s'est diffusé de machine en machine. Comme le note le site spécialisé DataSecurityBreach, l'Académie de Bordeaux dispose d'un contrat avec l'éditeur d'antivirus TrendMicro, pour le produit Internet Security. Reste à savoir si cette protection a été dupée par les cybercriminels ou si – comme c'est plus probable –, elle n'a pas été correctement installée dans les établissements victimes du fléau. Selon Sud-Ouest, les données pédagogiques sont menacées par cette épidémie...[lire la suite]

Denis JACOPINI : Nous allons rentrer en contact avec l'adjointe au maire en charge de l'éducation à la Mairie de Bordeaux pour voir comment nous pouvons leur venir en aide.

**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 : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Original de l'article mis en page : La moitié des écoles de Bordeaux victimes d'un ransomware



**Les collectivités territoriales aussi concernées par la cybersécurité**

	<p><b>Les collectivités territoriales aussi concernées par la cybersécurité</b></p>
---	---

---

**Pour mieux appréhender la transition numérique, les écoles de Saint-Cyr Coëtquidan organisent un colloque régional destiné aux collectivités territoriales,**

**Trois questions à...**

**Gérard de Boisboissel**, ingénieur au centre de recherche des écoles Saint-Cyr Coëtquidan, organisateur du colloque.

#### **En quoi la cybersécurité concerne les collectivités territoriales ?**

La transformation numérique touche tout le monde, donc la protection des données aussi. Il y a des enjeux et des risques, les petites communes comme la région sont vulnérables car elles détiennent des données personnelles.

#### **Quels types d'attaques sont les plus fréquentes ?**

On observe plusieurs types d'attaques : le piratage ou cryptage de données mais aussi une prise de contrôle des sites Internet par des hackers. En janvier 2015, plusieurs sites bretons, dont celui de la mairie de Port-Louis (56), ont été piratés et présentaient une page d'accueil avec un message islamiste.

#### **Comment se protéger ?**

Si toutes les collectivités territoriales sont conscientes de la transformation numérique, les élus n'avancent pas tous au même rythme. Pendant le colloque, nous aborderons les bons réflexes à adopter : sauvegarder ses données en double, changer ses mots de passe régulièrement, et pourquoi pas désigner une personne dédiée à cette question. Vannes apportera son témoignage demain, car la ville a un référent cybersécurité et consacre 25 000 € à ce sujet...[lire la suite]

---

Notre métier : Sensibiliser les décideurs et les utilisateurs. Vous apprendre à vous protéger des pirates informatiques, vous accompagner dans votre mise en conformité avec la CNIL et le règlement Européen sur la Protection des Données Personnelles (RGPD). (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Denis JACOPINI anime dans toute la France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.

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



Réagissez à cet article

**Original de l'article mis en page : Vannes. Les petites communes aussi concernées par la cybersécurité**

# Comment demander le retrait de votre image sur Internet ?

✖	Comment demander le retrait de votre image sur Internet ?
---	---

---

Vous constatez qu'une photo/vidéo de vous est diffusée sur internet sans votre consentement ? La CNIL vous explique comment exercer vos droits.

Une personne qui conteste la diffusion de son image sur un site web peut s'adresser soit au responsable de site en application du droit d'opposition prévu par la loi informatique et libertés, soit au juge en s'appuyant sur les principes du droit à l'image (obligation de recueil du consentement). Deux procédures existent : l'une dans le cas où vous souhaitez que le gestionnaire des droits de l'image supprime votre image, l'autre dans le cas où vous souhaitez demander au site de dépublier votre photo/vidéo. Vous pouvez effectuer ces demandes en parallèle.

#### « DEMANDER AU PHOTOGRAPHE LE RETRAIT D'UNE PHOTO AU NOM DU DROIT A L'IMAGE »

**Situation type** : « J'ai donné mon accord pour être pris en photo et ne souhaite plus voir ma photo en ligne aujourd'hui » Il faut bien dissocier la protection des données personnelles – champ qui relève de la loi informatique et libertés – du « droit à l'image », qui est en fait le droit à la vie privée prévu dans le code pénal \*\*. Le « droit à l'image » permet à toute personne de faire respecter son droit à la vie privée. Un internaute pourra par exemple refuser que son image ne soit reproduite ou diffusée sur n'importe quel support sans son autorisation expresse.

#### Étape 1 – Assurez vous que cette photo permet de vous identifier

#### Étape 2 – Assurez vous que vous n'avez à aucun moment consenti à cette prise de vue

Le fait d'autoriser l'exploitation de votre image restreint votre capacité de contester sa diffusion ou sa réutilisation sauf si les termes de l'accord écrit ne correspondent pas au cadre prévu par la loi.

Forme de l'accord écrit : ce « contrat » passé entre le photographe/vidéaste est le plus souvent un engagement écrit daté et signé de votre part et qui vous demande votre consentement à être photographié/filmé et votre autorisation à ce que votre image soit diffusée et ce , dans un cadre bien précis : quels supports seront diffusés les photos ? Quels sont les objectifs de cette diffusion ? Sur quelle durée porte cette autorisation ? Pour en savoir plus ...

**A noter** : dans le cas d'images prises dans les lieux publics, seule l'autorisation des personnes qui sont isolées et reconnaissables est nécessaire. **Votre enfant est mineur ?** Soyez particulièrement vigilants à ce que le photographe vous demande une autorisation écrite parentale. Quelques modèles sont téléchargeables depuis le site [educol.education.fr](https://www.educol.education.fr)

#### Étape 3 (Facultative) – Contactez l'auteur de la diffusion

Dans le cas d'une initiative d'un particulier, il peut s'agir du photographe à l'origine de la photo ou de la personne qui a publié votre image. Dans un contexte plus professionnel (clip musical, spot publicitaire ...) il peut s'agir de l'organisme qui utilise ces images à des fins de communication. Si le photographe/vidéaste refuse de dépublier/flouter votre image, vous avez la possibilité de saisir le juge civil/pénal\*\* afin qu'il prononce des sanctions à l'encontre de l'auteur de la diffusion litigieuse. Vous disposez d'un délai de 3 ans à partir de la diffusion de l'image.

#### Les sanctions prévues en cas de non-respect

- \* Sur le fondement de l'article 9 du code civil, « Chacun a droit au respect de sa vie privée »
- \*\* L'article 226-1 du code pénal punit d'un an d'emprisonnement et 45 000 € d'amende le fait de porter atteinte à l'intimité de la vie privée d'autrui en fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé.
- \* Par ailleurs, l'article 226-8 du code pénal punit d'un an d'emprisonnement et de 15 000€ d'amende le fait de publier, par quelque voie que ce soit, le montage réalisé avec l'image d'une personne sans son consentement, s'il n'apparaît pas à l'évidence qu'il s'agit d'un montage ou s'il n'en est pas expressément fait mention.

#### « JE SOUHAITE DEMANDER AU SITE DE DÉPUBLIER MA PHOTO »

**Situation type** : « Je n'ai pas donné mon accord pour être pris en photo », « J'ai donné mon accord pour me faire photographier mais pas pour une diffusion en ligne. ».

#### Étape 1 – Assurez vous que cette photo permet de vous identifier ...

Dès lors qu'elle se rapporte à une personne identifiée ou identifiable, l'image d'une personne est une donnée à caractère personnel. Pour vous appuyer sur les droits prévus par la loi « informatique et libertés » vous devez prouver que l'on vous reconnaît.

#### Étape 2 – contactez le responsable du site sur lequel est publiée l'image

\* Écrire au site/réseau social/service en ligne pour lui demander de dépublier l'image. \* Conformément à l'article 38 de la loi informatique et libertés, je souhaite m'opposer à ce que cette image – qui constitue une donnée personnelle – fasse l'objet d'un traitement pour le(s) motif(s) suivant(s) (..) :

- **Il est important d'indiquer les motifs légitimes** de votre demande d'opposition. Votre courrier doit être signé et vous devez préciser l'adresse à laquelle doit parvenir la réponse de l'organisme.
- **Joindre un justificatif d'identité.** Votre demande doit – en principe – être accompagnée de la photocopie d'un titre d'identité comportant votre signature. Attention, le responsable du fichier ne doit pas vous demander des pièces justificatives disproportionnées par rapport à votre demande. **Remarque** : Le droit d'opposition est un droit personnel ! Vous ne pouvez en aucun cas exercer ce droit au nom d'une autre personne sauf les cas de représentation de mineurs ou de majeurs protégés.

#### Étape 3 (facultative) – Si la réponse n'est pas satisfaisante

\* Si aucune réponse satisfaisante n'a été formulée par le site sous deux mois, contactez la CNIL, via son formulaire de plainte en ligne, en n'oubliant pas de joindre une copie des démarches effectuées auprès du site.

\* Vous avez également la possibilité de saisir une juridiction.

#### Situations particulières

**Usage domestique.** La loi « informatique et libertés » ne s'applique pas pour l'exercice d'activités purement personnelles ou domestiques. Par exemple, la photographie d'un parent ou d'un ami prise depuis un smartphone puis diffusée à un nombre limité de correspondants sur un site dont l'accès est restreint, ne rentre pas dans le champ de compétence de la CNIL.

**Usage artistique.** La publication de photographies de personnes identifiables aux seules fins d'expression artistique n'est pas soumise aux principales dispositions de la loi informatique et libertés.

**Droit à l'oubli des mineurs.** L'article 40 modifié de la loi informatique et Libertés – au même titre que futur Règlement européen sur la protection des données – consacre un droit à l'oubli spécifique pour les mineurs. Un internaute âgé de moins de 18 ans au moment de la publication ou de la création d'un compte en ligne peut directement demander au site l'effacement des données le concernant et ce, dans les meilleurs délais. En pratique, si le responsable de traitement n'a pas effacé les données ou répondu à la personne dans un délai d'un mois, la personne concernée peut saisir la CNIL. Des exceptions existent, notamment dans le cas où les informations publiées sont nécessaires à liberté d'information, pour des motifs d'intérêt public ou pour respecter une obligation légale.

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Denis JACOPINI anime dans toute la France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.

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



Réagissez à cet article

Original de l'article mis en page : Demander le retrait de votre image en ligne | CNIL

# Introduction au Règlement Européen sur la Protection des Données



**Le Règlement Général de l'Union Européenne sur la Protection des Données (RGPD) impose aux entreprises d'effectuer un suivi de toutes les occurrences des données à caractère personnel des clients au sein de leur organisation, d'obtenir le consentement des clients concernant l'utilisation de leurs informations personnelles (y compris le « droit à l'oubli ») et de documenter l'efficacité de cette gouvernance des données pour les auditeurs.**

Deux tiers (68 %) des entreprises, selon Compuware, risquent de ne pas être en conformité avec le RGPD, en raison d'une augmentation de la collecte des données, de la complexité informatique grandissante, de la multiplicité des applications, de l'externalisation et de la mobilité. Ce risque tient aussi aux politiques laxistes concernant le masquage des données et l'obtention d'une autorisation explicite des clients en matière de données. Les entreprises européennes comme américaines doivent, par conséquent, adopter une série de bonnes pratiques, notamment un masquage plus rigoureux des données de test et de meilleurs pratiques concernant le consentement des clients, afin d'éviter des sanctions financières et une altération possible de leur image de marque résultant d'une non-conformité.

Le RGPD de l'Union européenne a été adopté en avril 2016, afin d'unifier des obligations auparavant réparties à travers différentes juridictions européennes concernant l'utilisation, la gestion et la suppression des informations personnellement identifiables (IPI) des clients par les entreprises. Toutes les entreprises dans l'UE, aux États-Unis et ailleurs, qui collectent des IPI relatives à des citoyens de l'UE, ont jusqu'en mai 2018 pour se conformer à ces dispositions. Tout non-respect du RGPD expose les entreprises à des amendes pouvant atteindre 20 millions € ou 4 % du chiffre d'affaires mondial...[lire la suite]

---

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>



Réagissez à cet article

Original de l'article mis en page : Retour sur le RGPD, le Règlement Général de l'Union Européenne sur la Protection des Données – Data Security BreachData Security Breach

# Le site de la Gironde infiltré par des pirates informatiques



**Des pirates informatiques s'infiltrèrent et installent des pages malveillantes sur le site du Département de la Gironde. Un espace dédié aux personnes handicapées.**

Un piratage classique, malheureusement, mais qui démontre que même face à des internautes à la culture et au savoir informatiques faibles, les dégâts peuvent être importants. Le site du Département de la Gironde en est un parfait exemple. Il est pris pour une grande cours de récréation par des « pirates ». Pour preuve, la page « Troll » John Cena n'est pas l'unique passage malveillant que j'ai pu constater. D'autres pages ont été cachées, en ce mois de septembre, par des pirates informatiques différents [SirXL3 aka Kartz], avec plus ou moins de réussite. Les archives Zone H rappellent aussi que ce même site web avait été maltraité en avril 2016 par un barbouilleur baptisé Sneaky. En avril 2015, je vous expliquais comment d'autres malveillants du numérique s'étaient invités dans le site de l'association des maires de la Gironde...[lire l'article complet]

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>



Réagissez à cet article

Original de l'article mis en page : ZATAZ Le site Culture Accessible de la Gironde infiltré par des pirates informatiques – ZATAZ

---

# Quand les pirates s'attaquent à l'éducation

✖	Quand les pirates s'attaquent à l'éducation
---	---

---

**Le milieu scolaire n'est pas épargné par les hackers, certains étudiants piratent les examens, les notes ou leurs professeurs, tirant profit d'outils prêts à l'emploi mais aussi d'un manque de moyens et de sensibilisation des principaux concernés.**

De nombreux collèges, écoles ou lycées sont les cibles de cyber-attaques perpétrées par des étudiants. Des offensives qui : *«sont réalisées par des digital natives, des jeunes à l'aise avec l'informatique qui sont nés avec un ordinateur entre les mains»*, explique Jean-Charles Labbat, directeur général France, Belgique, Luxembourg et Afrique francophone chez Radware, société spécialisée en sécurité informatique.



## **Des attaques basiques**

Trois secteurs sont principalement visés par ces hacks : les examens, les notes, puis les systèmes informatiques des institutions ou des professeurs. Et les méthodes utilisées ne sont pas des plus sophistiquées.

Un étudiant pas suffisamment préparé pour passer un examen (comme les QCM en ligne dans certains pays) peut essayer de bloquer le site. Pour ce faire, il utilise le déni de service, il se connecte à ce serveur et se rend au point de connexion pour y envoyer une surcharge d'informations et boucher l'accès à l'application. Un hack très simple puisque, comme l'explique Jean-Charles Labbat, *« des outils sont disponibles sur internet comme Slowloris, ou il suffit de rentrer l'adresse du serveur pour le faire tomber »*.

Pour les systèmes de notation, rien de bien compliqué non plus. Les notes sont rangées dans une base de données et pour consulter ses résultats il faut se connecter avec ses identifiants. Le pirate va recourir à une injection SQL pour rentrer sans mot de passe, accéder directement à la base de données et modifier les informations renseignées. En novembre 2014, un élève du Tarn avait augmenté sa moyenne la faisant passer de 8,76 à 10,62.

Les enseignants sont également ciblés, via l'envoi de spams par exemple. *« Les enseignants recourent de plus en plus à l'outil informatique pour leurs cours. Un étudiant malveillant peut très bien s'il le souhaite accéder à un ordinateur mal protégé, spammer son professeur mais aussi ses contacts ou affecter tout le réseau de l'école »*...[lire la suite]

---

Denis JACOPINI est **Expert Informatique assermenté et formateur** (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-en-cybercriminalite-et-en-protection-des-donnees-personnelles>



Réagissez à cet article

**Original de l'article mis en page : Quand les pirates s'attaquent à l'éducation > Mag-Securs**



# Une garantie d'un million de dollars contre les ransomwares



Un éditeur de logiciels de cybersécurité propose de reverser jusqu'à un million de dollars à ses clients qui seraient, malgré ses protections, victimes d'un virus informatique.

Ce n'est pas une incitation à payer les rançonneurs informatiques. Hier, l'éditeur de logiciels de cybersécurité SentinelOne a annoncé proposer à ses clients professionnels une garanti d'un montant maximum d'un million de dollars contre toute menace qui percerait ses défenses. Notamment les ransomwares, ses programmes malveillants qui coupent l'accès aux données stockées dans les ordinateurs touchés et invitent à payer pour les récupérer. La police conseille de ne jamais céder à ce chantage.

SentinelOne compte sur sa technologie de machine learning pour protéger ses clients. En cas de manquement à ses devoirs, l'éditeur dédommagerait les entreprises à hauteur de 1.000 dollars par postes de travail et dans la limite d'un million de dollars. « Avec cette assurance financière, nous devenons vraiment responsables de la sécurité de nos clients, souligne Scott Gainey, le patron du marketing de SentinelOne, jusqu'ici, les entreprises victimes qui voulaient se retourner contre leurs éditeurs d'anti-virus ne pouvaient pas, c'est injuste. » D'après lui, cette garantie est une première au monde...[lire la suite]

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](https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles) sur [: https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles](https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles)



Réagissez à cet article

Original de l'article mis en page : Une garantie d'un million de dollars contre les ransomwares, Cybersécurité – Les Echos

Business