



LES ENJEUX DE LA PROTECTION DES DONNÉES PERSONNELLES DANS NOS COMMUNES

LA SÉCURITÉ DES DONNÉES PERSONNELLES DE NOS CITOYENS- UN ENJEU CROISSANT

La cybersécurité est devenue un enjeu de sécurité majeur pour nos institutions. Face à l'augmentation constante des cyberattaques et de leur intensité, les institutions publiques doivent faire preuve d'une vigilance accrue au quotidien.

En effet, le rapport annuel sur la cybercriminalité en France publié en 2024 fait état d'une hausse de 40 % du nombre d'attaques numériques en seulement cinq ans.

Les collectivités territoriales ne sont pas épargnées : l'ANSSI (Agence nationale de la sécurité des systèmes d'information) recense 218 attaques ciblant ces structures en 2024, soit une moyenne de 18 par mois, affectant principalement les communes et les établissements publics de coopération intercommunale (EPCI).

Les élus locaux ont une responsabilité majeure en matière de cybersécurité. Dépositaires de nombreuses informations personnelles concernant leurs administrés, ils ont le devoir de protéger ces données contre les cyberattaques, les usages malveillants et toute divulgation non autorisée.

Se doter des bons outils et apprendre à se défendre est donc devenu une priorité pour les élus locaux, qui jouent désormais un rôle clé dans la cybersécurité française.

I. LA CYBERSÉCURITÉ, UNE PRIORITÉ GRANDISSANTE POUR LES ÉLUS

- **Protéger nos systèmes et les données des citoyens :**

La cybersécurité regroupe l'ensemble des mesures techniques, technologiques et organisationnelles visant à protéger les systèmes informatiques contre les attaques malveillantes (piratage, vols de données, rançongiciels). Son objectif est d'empêcher les cyberattaques avant qu'elles n'atteignent les données sensibles de la collectivité. Les élus sont directement concernés : les communes détiennent des données personnelles (état civil, santé, cartes d'identité, listes électorales...) qui permettent d'identifier les citoyens. Ces informations doivent être strictement protégées.

- **Pourquoi les élus-doivent-ils agir face aux cybermenaces ?**

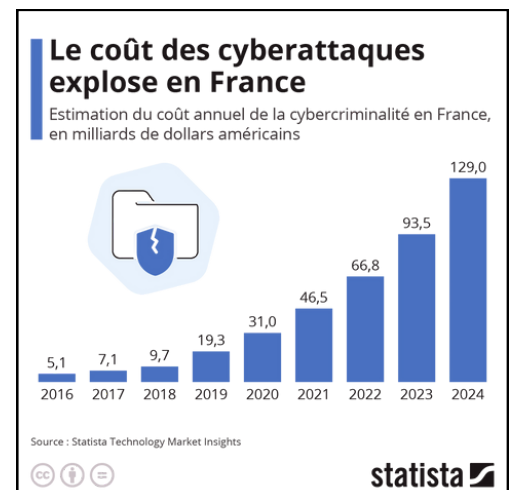
Les mairies sont des cibles privilégiées pour les cyberattaques :

- Vols de données personnelles.
- Blocage des services publics.
- Demandes de rançon.

Protéger ces données, c'est protéger les citoyens et garantir la continuité des services municipaux. Le nombre de cyberattaques contre les communes est en forte progression. Il est donc urgent d'anticiper et de sécuriser les systèmes pour éviter les vols et les blocages.

Par ailleurs, les élus ont une obligation légale : le RGPD impose depuis le 25 mai 2018 la protection des données personnelles à toutes les collectivités publiques. En cas de manquement, la responsabilité des élus peut être engagée.

Le coût moyen d'une cyberattaque pour une commune peut atteindre plusieurs centaines de milliers d'euros, sans compter les dommages sur la continuité des services publics. En 2023, 24% des cyberattaques visaient les collectivités territoriales. Face à ces risques croissants, il est devenu indispensable pour les collectivités de renforcer leur protection numérique.



II. LES RESPONSABILITÉS DES ÉLUS POUR PROTÉGER SES ADMINISTRÉS

- **Les mesures obligatoires :**

- **La RGPD**

Depuis le 25 mai 2018, la Réglementation Générale de Protection des Données est une mesure obligatoire qui s'applique à tous les organismes publics, qu'ils soient français ou européens.

Son objectif est simple : permettre aux citoyens de vérifier et faire valoir leurs droits sur leurs données personnelles, dans le but d'accroître à la fois la protection des personnes concernées par un traitement de données et la responsabilisation des acteurs de ce traitement.

Les droits concernés :

- Droit à l'information sur les données collectées et dans quel but.
- Droit d'accès à ces données.
- Droit d'opposition : s'opposer à la collecte de données (sauf obligation légale).
- Droit de rectification des données transmises à la collectivité.
- Droit à l'oubli et à la suppression des données.
- Droit à la portabilité des données de façon lisible.

Les données concernées sont : les dossiers scolaires ou médicaux, cartes d'identité, passeports, état civil, RIB, documents d'imposition...

- **Désigner un DPO**

La désignation d'un Délégué à la Protection des Données (DPO) est obligatoire pour les autorités et organismes publics. Son rôle est de diagnostiquer, prioriser les actions à mener, accompagner dans la gestion des risques et organiser les procédures internes en lien avec la protection des données. Le DPO peut être :

- Un agent de la collectivité locale.
- Un conseiller externe désigné dans le cadre d'une prestation de service.
- Un DPO peut être désigné par plusieurs collectivités : il agira alors sur un ensemble défini de communes.

- **Sur la mise en place de caméra de vidéosurveillance**

La mise en place de caméras de vidéosurveillance nécessite une Analyse d'Impact sur la Protection des Données (AIPD) faite au préalable. Cette mission peut alors être remplie par le DPO. À la suite de l'installation de ces dispositifs, une protection des données récoltées est exigée, ce qui inclut la sécurisation de l'accès physique à l'enregistreur ainsi que l'accès aux images.

● NIS 2

La directive NIS 2 (Network & Information Security) est une loi européenne qui impose aux communes de mieux protéger leurs systèmes informatiques contre les cyberattaques. Elle s'ajoute à la mesure RGPD et fixe des obligations concrètes aux communes et communautés de communes excédant 30 000 habitants depuis 2024 :

1. Sécuriser vos systèmes informatiques :

- Antivirus, sauvegarde, gestion des accès
- Mise à jour des logiciels
- Sécurisation des réseaux internet et Wi-Fi

2. Organiser la cybersécurité :

- Désigner un DPO
- Établir un plan d'action en cas de cyberattaque

3. Déclarer les incidents

- Toute cyberattaque grave doit être signalée à l'ANSSI sous 24 heures

ATTENTION ! La directive NIS 2 s'applique **UNIQUEMENT** aux communes et communautés de communes comptant plus de **30 000** habitants au total, bien que cette limite puisse potentiellement évoluer à l'avenir.

● Sur la publication d'informations dans le bulletin municipal

Les dispositions de l'article 9 du Code civil, selon lesquelles chacun a droit au respect de sa vie privée, s'opposent à la divulgation par les autorités publiques, à des tiers, de tout élément de la vie privée d'une personne sans son consentement. Ainsi, un accord écrit est obligatoire pour publier une naissance dans le bulletin municipal, sous peine de poursuites judiciaires. Ce cadre juridique interdit la publication d'informations personnelles sans accord préalable des individus concernés.

L'accord des personnes concernées doit être présenté sous la forme d'un document officiel, tel qu'une autorisation de communication d'un acte d'état civil dans le bulletin municipal et en version numérique de la commune.

Sans cet accord écrit, la publication d'une naissance dans le bulletin municipal est interdite et expose la collectivité à des sanctions judiciaires.

Modèle à télécharger ici :

https://www.canva.com/design/DAGna9Jqx64/xbI_d0Y508WQiPhjf72lew/view?utm_content=DAGna9Jqx64&utm_campaign=designshare&utm_medium=link2&utm_source=uniquelinks&utlId=h241a60ffdc

AUTORISATION DE COMMUNICATION D'UN ACTE D'ETAT-CIVIL DANS LE BULLETIN MUNICIPAL ET EN VERSIONS NUMERIQUES DE LA COMMUNE	
A retourner au service communication	
Je soussigné(e) M./ Mme (royer la mention inutile)	
Agissant en qualité de	
Ayant connaissance des dispositions de l'article 9 du Code Civil, aux termes desquelles chacun a droit au respect de sa vie privée et qui s'opposent notamment à la divulgation par des autorités publiques, telles les municipalités, à des tiers, quelle qu'en soit la qualité, de tout élément de vie privée d'une personne sans le consentement de celle-ci.	
Autorise l'annonce dans le bulletin municipal de la commune de Canet (34) et en versions numériques :	
☐	De la naissance de ma fille / mon fils (royer la mention inutile) Nom : Prénom Né(e) le à
☐	De mon mariage avec Célébré le en la mairie de Canet.
☐	Du décès de M./ Mme (royer la mention inutile) Nom : Prénom Epouse à l'âge de ans. Date du décès
Fait à	le Signature
Mairie de CANET rue de la Poste - 34800 CANET ☎ : 04.67.88.91.40 📠 : 04.67.96.79.67 ✉ : canet.mairie@orange.fr Site Internet : www.canet-herault.com	

- **Les sanctions possibles en cas de manquement :**

Les élus sont garants des données personnelles des administrés selon le Code du patrimoine. À ce titre, tout manquement, erreur, fraude ou action volontairement malveillante est condamnable.

Les risques en cas de non-respect des réglementations précédemment énoncées sont les suivants :

- **Conséquences juridiques** : les individus dont les données ont été compromises peuvent engager des actions en justice pour obtenir réparation, ce qui peut mener à une amende. *Exemple : en 2020, la CNIL a infligé une amende de 3 000 € à une commune n'ayant pas réalisé d'AIPD avant la mise en place de caméras de vidéosurveillance dans les écoles.*
- **Sanctions administratives** : les autorités de protection des données, comme la CNIL, peuvent prononcer des sanctions telles que des restrictions ou des interdictions de traitement des données. *Exemple : la CNIL a administré une amende de 4 000 € à une commune pour avoir publié des données personnelles sans consentement préalable dans un bulletin municipal en 2021.*
- **Conséquences financières** : les coûts liés à la réparation d'une violation des données peuvent être élevés pour la collectivité.
- **Pertes de confiance des électeurs** : une mauvaise gestion des données personnelles peut nuire à la réputation des élus et entraîner une perte de crédibilité auprès des citoyens.

Retrouvez ici les différentes sanctions imposées par la CNIL :

<https://www.cnil.fr/fr/les-sanctions-prononcees-par-la-cnil>



III. OBTENIR DE L'AIDE DANS L'INSTALLATION DE SA PROTECTION CYBER, ET EN CAS D'ATTAQUE

- Être aidé dans la mise en place de sa cybersécurité :

● CSIRT régionaux

Computer Security Incident Response Team : une équipe d'experts mobilisée pour analyser les menaces potentielles, développer des procédures de réponse aux incidents et coordonner les actions lors d'une attaque informatique. Ce dispositif propose des centres pour vous aider à trouver des prestataires proches de votre commune, qui vous accompagneront dans les démarches de sécurisation de vos systèmes informatiques.



Tel : 0 806 700 111

<https://csirt-hdf.fr>

● ANSSI

L'Agence Nationale de la Sécurité des Systèmes d'Information propose un programme d'accompagnement et de formation gratuit à destination des collectivités. Elle offre également des guides pour durcir le matériel et le réseau des communes, afin qu'elles soient aptes à se défendre en cas de cyberattaque.



<https://cyber.gouv.fr>

● Cyber Malveillance.gouv

Cette plateforme participe à la sécurisation des systèmes d'information des organisations. Le programme « Mon expert cyber » vous mettra en relation avec des professionnels qualifiés du cyberspace pour la sécurisation de vos infrastructures.



<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/securisation-cybersecurite-professionnels>

● Somme numérique

Cette plateforme propose des offres comprenant un service d'assistance informatique, un antivirus et un coffre-fort de mots de passe, pour accompagner chaque collectivité dans la sécurisation de son environnement numérique.



Tel : 03 22 22 27 27

<https://www.sommenumerique.fr/services/>

● CNIL

La Commission Nationale de l'Informatique et des Libertés met à disposition des outils pour renforcer la protection des données personnelles. En cas de difficulté persistante, de réponse insatisfaisante ou d'absence de réponse des services concernés, vous pouvez saisir la CNIL.



Tel : 01 53 73 22 22

<https://www.cnil.fr/fr>

- **Être aidé en cas d'attaques :**

- **Les premiers gestes sont décisifs**

Si vous pensez être victime d'une attaque, la démarche suivante est recommandée :

1. **Limiter la propagation** : désactivez le wifi pour déconnecter l'ordinateur du réseau. NE PAS ÉTEINDRE
2. **Déterminer la source de l'intrusion et les données concernées** : appelez le CSIRT et déposez plainte à la gendarmerie ou la Police.
3. **Prévenir de la perte de données** : informez le DPO et les propriétaires des données compromises.

- **THESEE**

THESEE est la première plateforme permettant de déposer une plainte en ligne. Elle concerne exclusivement les escroqueries sur internet.



Pour déposer plainte :

<https://www.service-public.fr/particuliers/vosdroits/N31138>

- **Diagnostic 17Cyber**

Ce dispositif permet d'effectuer un diagnostic en ligne pour identifier votre problème et accéder à des conseils pour y remédier. Il constitue une démarche complémentaire à Cybermalveillance.gouv.



<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/page/17cyber-mon-assistance-en-ligne>

- **L'ANSSI**

L'ANSSI propose une assistance aux entités essentielles et aux structures exposées à des cyberattaques sensibles.

Ses quatre missions principales :



CONNAÎTRE



PARTAGER



ACCOMPAGNER



DÉFENDRE

III. OBTENIR DE L'AIDE DANS L'INSTALLATION DE SA PROTECTION CYBER, ET EN CAS D'ATTAQUE

- Être aidé dans la mise en place de sa cybersécurité :

● CSIRT régionaux

Computer Security Incident Response Team : une équipe d'experts mobilisée pour analyser les menaces potentielles, développer des procédures de réponse aux incidents et coordonner les actions lors d'une attaque informatique. Ce dispositif propose des centres pour vous aider à trouver des prestataires proches de votre commune, qui vous accompagneront dans les démarches de sécurisation de vos systèmes informatiques.



Tel : 0 806 700 111

<https://csirt-hdf.fr>

● ANSSI

L'Agence Nationale de la Sécurité des Systèmes d'Information propose un programme d'accompagnement et de formation gratuit à destination des collectivités. Elle offre également des guides pour durcir le matériel et le réseau des communes, afin qu'elles soient aptes à se défendre en cas de cyberattaque.



<https://cyber.gouv.fr>

● Cyber Malveillance.gouv

Cette plateforme participe à la sécurisation des systèmes d'information des organisations. Le programme « Mon expert cyber » vous mettra en relation avec des professionnels qualifiés du cyberspace pour la sécurisation de vos infrastructures.



<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/securisation-cybersecurite-professionnels>

● Somme numérique

Cette plateforme propose des offres comprenant un service d'assistance informatique, un antivirus et un coffre-fort de mots de passe, pour accompagner chaque collectivité dans la sécurisation de son environnement numérique.



Tel : 03 22 22 27 27

<https://www.sommenumerique.fr/services/>

● CNIL

La Commission Nationale de l'Informatique et des Libertés met à disposition des outils pour renforcer la protection des données personnelles. En cas de difficulté persistante, de réponse insatisfaisante ou d'absence de réponse des services concernés, vous pouvez saisir la CNIL.



Tel : 01 53 73 22 22

<https://www.cnil.fr/fr>