RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR

Assistance et prévention en sécurité numérique

FRANCE RELANCE

GUIDE
OBLIGATIONS ET RESPONSABILITÉS DES COLLECTIVITÉS LOCALES EN MATIÈRE DE CYBERSÉCURITÉ

CNIL.

COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

SOMMAIRE

INTRODUCTION

Malgré une profonde transformation numérique des collectivités locales, l'angle de la cybersécurité reste encore peu appréhendé. Pourtant, les collectivités de toutes tailles sont la cible d'actes de cybermalveillance de plus en plus nombreux et dont les conséquences ne sont pas négligeables : systèmes d'information bloqués, vol de données personnelles, missions de service public interrompues, etc. Un incident de sécurité numérique peut se produire à tout moment et dans n'importe quelle collectivité.

Dans ce contexte et dans le cadre du volet relatif à la cybersécurité des collectivités locales du plan France Relance, Cybermalveillance.gouv.fr a réalisé une **étude relative à la sécurité numérique dans les collectivités françaises de moins de 3 500 habitants**. Parmi les enseignements significatifs, l'étude révèle que ces publics sont peu informés ou sensibilisés à la cybersécurité et qu'ils ont de **nombreux préjugés** sur le sujet.

Il apparaît également que la majorité des personnes interrogées n'ont pas connaissance du cadre juridique en vigueur, à l'exception du Règlement Général sur la Protection des Données (RGPD), et qu'elles jugent la réglementation en matière de cybersécurité, complexe.

Afin de lever ces freins, Cybermalveillance.gouv.fr a rédigé en collaboration avec la Commission Nationale de l'Informatique et des Libertés (CNIL), ce guide, qui a pour objectif d'informer les élus locaux et les agents territoriaux quant aux obligations et aux responsabilités des collectivités locales et de leurs établissements publics en matière de cybersécurité.

1. OBLIGATIONS DES COLLECTIVITÉS LOCALES ET DE LEURS ÉTABLISSEMENTS PUBLICS EN MATIÈRE DE CYBERSÉCURITÉ

Les collectivités locales et leurs établissements publics sont tenus à plusieurs obligations en matière de cybersécurité, dans leurs relations avec les administrés et dans l'exercice de leurs compétences.

1.1 DES OBLIGATIONS LIÉES À LA PROTECTION DES DONNÉES PERSONNELLES

Qu'est-ce qu'une donnée personnelle ?

Il s'agit d'une information se rapportant à une personne physique identifiée ou identifiable, directement (ex. : avec un nom et un prénom) ou indirectement (ex. : avec un numéro de téléphone, une plaque d'immatriculation d'un véhicule, un numéro de sécurité sociale, une adresse postale, une adresse électronique, une voix, une photographie, etc.).

POUR ALLER PLUS LOIN

La notion de donnée personnelle fait l'objet de textes juridiques de référence applicables aux collectivités locales et à leurs établissements publics :

- la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite « **loi Informatique et Libertés** » ;
- le règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, dit « **RGPD** »
- le guide de sensibilisation au RGPD établi par la CNIL pour les collectivités locales avec des modèles de mentions légales et des fiches pratiques.

A. En quoi les collectivités locales sont-elles concernées par l'obligation de protection des données personnelles ?

Au titre de l'exercice de leurs compétences et dans leurs relations avec les administrés, les collectivités locales et leurs établissements publics sont tenus d'appliquer la réglementation relative aux données personnelles. **Ces données sont nombreuses au sein des collectivités locales, qu'il s'agisse d'une utilisation interne (ressources humaines, vidéosurveillance, etc.) ou externe (état civil, listes électorales, inscriptions scolaires, etc.).**

Les collectivités locales sont soumises aux règles relatives à la protection des données personnelles dès lors que les données considérées font l'objet de l'une des opérations suivantes : collecte, enregistrement, stockage, extraction, adaptation ou modification, communication, etc. Il est important de noter qu'un traitement n'est pas nécessairement automatisé et qu'il peut résulter d'une simple liste tenue sur un registre manuel (ex. : fichier papier des usagers de la médiathèque).

Qu'est ce qu'un traitement de données à caractère personnel ?

Un traitement de données personnelles est une opération, ou un ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement organisation, conservation, adaptation, modification, extraction consultation, utilisation...).

B. Qui supervise les questions relatives à la protection des données personnelles au sein des collectivités locales et de leurs établissements publics ?

Toute collectivité locale ou établissement public local, **quelle que soit sa taille, est tenu(e) de désigner un délégué à la protection des données (DPO)** qui devra exercer en toute indépendance et en étant à l'abri des conflits d'intérêts.
Ce délégué peut être :

- un agent de la collectivité locale ;
- plusieurs collectivités locales peuvent également **mutualiser la désignation** d'un délégué à la protection des données, qui pourra donc être commun à un ensemble de communes ou d'établissements (ex. : organismes publics de services numériques OPSN) ;
- un conseil externe (cabinet de conseil, avocat) désigné dans le cadre d'un contrat de prestations de services.

Attention, les fonctions de Directeur Général ou bien de Responsable du Service Informatique sont susceptibles de donner lieu à un conflit d'intérêts avec la fonction de DPO.

Pour une collectivité locale, en pratique et en général, **le responsable de traitement de données à caractère personnel est son représentant légal** : maire, président d'un établissement public de coopération intercommunal (EPCI), directeur d'un établissement (ex. : centre hospitalier). **Pour chaque traitement opéré, ce dernier est responsable de la conformité de l'ensemble des traitements de sa collectivité** à l'égard des principes et obligations prévus par le RGPD (ex. : tenue du registre).

Pour aller plus loin : la fiche ***Désigner un délégué à la protection des données dans une collectivité*** *réalisée par la CNIL.*

C. Que recouvre l'obligation de protection des données personnelles par les collectivités locales ?

a/ Avant la collecte et le traitement des données

Avant toute mise en œuvre d'un traitement, le responsable définit les mesures techniques et organisationnelles appropriées afin de respecter les principes relatifs à la protection des données (finalité explicite et légitime, nécessité de l'exploitation des données, minimisation de leur recueil, définition d'une durée de conservation, respect des droits des personnes concernées, mesures de sécurité adaptées etc.).

Lorsqu'un type de traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, **le responsable du traitement des données doit effectuer au préalable une analyse de l'impact des opérations envisagées,** dite « étude d'impact sur la vie privée » ou bien encore « analyse d'impact relative à la protection des données ». **Cette analyse en amont est rendue obligatoire par le RGPD** dans certaines situations particulières, à l'instar d'une collecte de données sensibles (ex. : données biométriques) ou de l'utilisation d'une nouvelle technologie.

S'agissant des collectivités locales, plusieurs traitements nécessitent ainsi une analyse d'impact en amont : système de vidéo surveillance de la voie publique sur le territoire d'une commune, instruction des demandes et gestion des logements sociaux, prise en charge des personnes par les établissements de santé ou médico-sociaux, etc.

b/ Pendant le traitement des données

Les collectivités locales et leurs établissements publics ont l'obligation de mettre en œuvre des procédures internes au plan technique et au plan organisationnel permettant de démontrer le respect des règles relatives à la protection de données et ainsi être en conformité avec le droit. S'agissant plus spécifiquement de l'obligation d'assurer la sécurité des données, **il revient aux collectivités locales de mettre en œuvre des mesures de sécurité adaptées aux éventuels risques susceptibles de peser sur les données personnelles** (destruction, perte, altération, diffusion ou accès non autorisé, piratage, fuite de données…) et appropriées à la nature des données considérées.

Les collectivités locales et leurs établissements publics sont tenus de ne collecter, d'utiliser et de stocker des données personnelles que dans la mesure où cela est strictement nécessaire, conformément au principe de minimisation.

Le traitement de données doit se fonder sur au moins une des bases légales possibles au titre du RGPD (consentement, contrat, obligation légale, mission d'intérêt public, intérêt légitime, etc.).

Les finalités poursuivies par le traitement doivent être explicitées par les collectivités locales et leurs établissements publics :

- gestion de la paie ;
- gestion des lettres d'information ;
- inscription à un service municipal ;
- inscription à une liste électorale ;
- inscription à l'école ;
- demande de permis de construire, etc.

*Pour aller plus loin : la fiche pratique **dédiée aux bases légales** réalisée par la CNIL.*

En cas de violation de données personnelles

Toute atteinte aux données personnelles faisant l'objet d'un traitement de données doit être signalée à la CNIL dans un délai de 72 heures si elle présente un risque pour les droits et libertés des personnes concernées (exemples : panne accidentelle d'un serveur informatique conduisant à la destruction des fichiers de demande d'inscription à un service ; cyberattaque conduisant à une fuite d'informations bancaires d'usagers ou à une perte de confidentialité des données). Les personnes concernées doivent en être informées si les risques sont élevés (en cas de doute sur le niveau de risque, la CNIL pourra être sollicitée).

*Pour aller plus loin : la fiche **Notifier une violation de données personnelles** réalisée par la CNIL.*

c/ Conservation et archivage des données

Le cycle de vie des données à caractère personnel peut se décomposer en 3 phases successives :

- **l'utilisation courante** (base active avec l'intégralité des données) ;
- **l'archivage intermédiaire** pour répondre à l'obligation légale de conservation durant une durée limitée (base avec les données indispensables) ;
- **l'archivage définitif** (pour plus de précisions, consulter le site francearchives.fr).

La durée de conservation des données doit être proportionnée, en adéquation avec les finalités du traitement et doit être inscrite dans le registre du délégué à la protection des données pour chacun des traitements concernés. Si certaines durées de conservation sont fixées par la loi (ex. : 5 ans s'agissant des bulletins de paie), la durée de conservation de nombreux types de données sera laissée à la libre appréciation du responsable de traitement en l'absence de texte spécifique.

Focus sur les mesures de sécurité à mettre en place

Les mesures de sécurité à mettre en place dépendent des situations et doivent être déterminées en conduisant une analyse des risques (ou une Analyse d'impact relative à la protection des données, AIPD). Les mesures les plus élémentaires qui sont requises dans la quasi-totalité des cas sont :

- la sécurisation des postes de travail (antivirus, EDR, etc.) ;
- la sécurisation des éléments réseau (pare-feu, proxy, etc.) ;
- la mise à jour régulière et suivie des systèmes et logiciels utilisés ;
- la mise en place de sauvegardes régulières et régulièrement testées ;
- la mise en place d'un système d'authentification fiable et robuste des utilisateurs ;
- le chiffrement des flux réseau à travers internet (par HTTPS) et des supports de stockage (notamment les ordinateurs portables et les clés USB) ;
- la définition d'une politique d'habilitation clairement définie pour limiter les accès aux données ;
- la mise en place de journaux de connexion et leur supervision afin de détecter une compromission.

*Pour aller plus loin : la fiche **Les 10 mesures essentielles pour assurer votre sécurité numérique** réalisée par Cybermalveillance.gouv.fr.*

1.2 DES OBLIGATIONS LIÉES À LA MISE EN ŒUVRE DES TÉLÉSERVICES LOCAUX

La mise en œuvre de téléservices locaux impose des obligations aux collectivités locales et à leurs établissements publics. **À partir de 5 000 € de recettes annuelles, la mise à disposition de services de paiement en ligne auprès des usagers par les collectivités locales est obligatoire.**

Qu'est-ce qu'un téléservice ?

Il s'agit d'un guichet d'accueil numérique proposé par une collectivité permettant aux usagers de procéder par voie électronique à des démarches ou formalités administratives.

A. En quoi les collectivités locales sont-elles concernées par les obligations liées aux téléservices ?

Les téléservices recouvrent l'ensemble des services offerts par des moyens de communication électronique permettant aux usagers de formuler une demande en vue d'obtenir une prestation, de faire une déclaration, de solliciter une autorisation, de télé-payer un service, etc.

Au sein des collectivités, il peut s'agir des services suivants : demande de permis de construire, demande de logement social, demande de pièces extraites de l'état civil, inscription à la cantine scolaire, etc.

L'ensemble des téléservices offerts par les collectivités locales doivent satisfaire aux exigences du Référentiel Général de Sécurité, dit « RGS », édicté par **le décret n° 2010-112 du 2 février 2010.**

B. Quel est le champ des obligations liées au respect du RGS ?

Le RGS fixe un ensemble de **règles de sécurité applicable à l'ensemble des collectivités ainsi qu'aux prestataires qui les assistent dans leur démarche de sécurisation de leurs systèmes d'information.**

Le RGS impose une démarche impliquant plusieurs étapes :

- réaliser une analyse des risques ;
- définir les objectifs de sécurité ;
- choisir et mettre en œuvre des mesures appropriées de protection et de défense du système d'information ;
- procéder à une homologation du système d'information ;
- et assurer son suivi opérationnel.

Les produits et services utilisés pour mettre en place leur système d'information doivent être choisis parmi ceux qualifiés par l'Agence Nationale de Sécurité des Systèmes d'Information – ANSSI : il s'agit des produits de sécurité et des prestataires de confiance (PSCO). Leur liste est consultable à l'adresse suivante : https://www.ssi.gouv.fr/uploads/liste-produits-et-services-qualifies.pdf

Le recours à ces produits et/ou ces prestataires est requis pour toute prestation visant à assurer la certification électronique (ex. : signature électronique), l'horodatage et l'audit de la sécurité des systèmes d'information.

La collectivité locale ou l'établissement public doit attester de la conformité de son système d'information par une décision d'homologation prise par l'autorité compétente (assemblée délibérante, directeur d'établissement) qui sera rendue publique. Cette décision, dénommée « attestation formelle », est prise sur la base d'un dossier technique (ou dossier d'homologation) élaboré préalablement par ses services pour déterminer les fonctionnalités du téléservice, ses risques et les mesures de sécurité envisagées en cas d'incident. L'attestation formelle, prise pour une durée limitée, engage la collectivité qui garantit ainsi aux usagers que le téléservice respecte la réglementation en matière de protection des données.

Une fois le téléservice mis en place, **le RGS impose un maintien en condition opérationnelle pour assurer la protection du système d'information, sa surveillance et ainsi détecter les anomalies et réagir au mieux aux incidents de sécurité.**

*Pour aller plus loin : la **fiche sur la sécurité des données des administrés** réalisée par la CNIL explique l'obligation des collectivités locales de sécuriser l'accès à leurs téléservices et de protéger les données des administrés.*

Le cas particulier des téléservices nécessitant une identification, une authentification ou une signature électronique des usagers

Pour ce cas particulier, des spécifications techniques sont imposées par l'eIDAS (règlement européen sur l'identification électronique et les services de confiance pour les transactions électroniques au sein de l'Union Européenne).

Ce règlement impose aux collectivités locales de recourir à des **solutions d'identification compatibles avec l'ensemble des standards d'identification des autres pays européens** et ainsi garantir l'accès au service à l'ensemble des ressortissants de l'Union européenne. Le service en ligne d'identification et d'authentification « France Connect », développé par la direction interministérielle du numérique de l'État, peut être une solution.

De même, lorsque le téléservice offre un **système de signature électronique, il devra être compatible avec ceux émanant d'autres pays membres** de l'Union européenne équivalant ou présentant un niveau de sécurité supérieur à celui proposé par le téléservice.

1.3 DES OBLIGATIONS LIÉES À L'HÉBERGEMENT DES DONNÉES DE SANTÉ

Quelles données sont concernées ?

La réglementation relative à l'hébergement des données s'applique aux données de santé recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social.

A. En quoi les collectivités locales sont-elles concernées par les obligations liées à l'hébergement des données de santé ?

Les collectivités locales et leurs établissements publics sont doublement concernés par l'hébergement des données de santé : d'une part, au titre de **la protection des données personnelles** (voir 1.1) ; d'autre part, au titre d'**une réglementation spécifique s'appliquant aux activités consistant à héberger des données de santé, lorsqu'elles sont externalisées auprès d'un tiers.**

Nombreuses et définies par le Code de la santé publique de manière précise et exhaustive, ces activités sont fréquemment mises en œuvre par les collectivités locales (départements au titre de la gestion des aides sociales, communes au titre des centres communaux d'action sociale), les établissements de santé ou les établissements médico-sociaux (ex : centres hospitaliers, établissements d'hébergement pour personnes âgées dépendantes).

L'hébergement des données de santé peut être assuré directement par l'établissement concerné ou bien externalisé et confié à un prestataire. La liste des hébergeurs de santé certifiés est consultable à l'adresse suivante : https://esante.gouv.fr/offres-services/hds/liste-des-herbergeurs-certifies.

B. Quel est le champ des obligations liées à l'hébergement des données de santé ?

Les activités d'hébergement des données de santé, lorsqu'elles sont réalisées par un prestataire externe, **sont soumises à des exigences de certification préalable** délivrée par un organisme de certification agréé. Le référentiel de certification est consultable à l'adresse suivante : https://esante.gouv.fr/services/hebergeurs-de-donnees-de-sante/les-referentiels-de-la-procedure-de-certification
Les centres hospitaliers, groupements de coopération sanitaires ou EPCI sont eux-mêmes soumis à cette certification lorsqu'ils réalisent des activités d'hébergement pour le compte d'autres collectivités ou établissements.

L'audit de certification auquel est soumis le futur hébergeur doit permettre de vérifier le respect de plusieurs normes garantissant la protection des données, ainsi que des exigences spécifiques à l'hébergement des données de santé.

2. RESPONSABILITÉ DES COLLECTIVITÉS LOCALES ET DE LEURS ÉTABLISSEMENTS PUBLICS EN MATIÈRE DE CYBERSÉCURITÉ

Certaines conséquences d'actes de cybermalveillance sont aujourd'hui bien identifiées pour les collectivités locales victimes de cyberattaque. Les conséquences liées à la désorganisation et/ou à l'indisponibilité de plusieurs services publics peuvent engendrer :

- **des préjudices pour les administrés et fragilisation du lien de confiance :** en cas d'indisponibilité des services (ex. : état civil), du site internet de la collectivité ou d'une fuite de données ;
- **des préjudices financiers directs :** coûts liés à la reconfiguration du système d'information touché (réinstallation et reconfiguration des serveurs, modification d'une architecture réseau, intervention de prestataires spécialisés en urgence, etc.) ;
- **des préjudices financiers indirects :** coûts liés à l'indisponibilité d'équipements publics (ex. : fermeture contrainte d'une piscine municipale, d'un musée, d'une bibliothèque ou d'un parking public de stationnement) ;
- **des dommages aux personnes et/ou aux biens** (ex. : accident du fait d'un dysfonctionnement affectant la signalisation ou l'éclairage public).

Pour aller plus loin : le témoignage de deux collectivités locales victimes de cybermalveillance.

D'autres conséquences sont encore peu connues des élus locaux et des agents territoriaux, à l'instar de l'engagement de la responsabilité juridique des collectivités en cas de dommages résultant de cyberattaques ou de mesures de sécurité non conformes au RGPD. Il existe différentes formes de responsabilité : administrative, civile et pénale.

2.1 RESPONSABILITÉ ADMINISTRATIVE : LA RESPONSABILITÉ DE LA COLLECTIVITÉ

S'agissant de la responsabilité administrative, il convient de distinguer :
- les sanctions administratives de la CNIL ;
- la responsabilité pour faute ;
- et la responsabilité pour dommage de travaux publics.

A. Les sanctions administratives de la CNIL

Lorsqu'il est constaté, dans le cadre d'un contrôle opéré par la CNIL et à l'issue d'une procédure contradictoire, que des dispositions relatives à la loi dite Informatique et Libertés et/ou au RGPD ont été méconnues, la CNIL a la faculté de prononcer des sanctions administratives à l'encontre des responsables de traitement. Pour les collectivités ayant commis des manquements graves à ces réglementations, le montant des sanctions pécuniaires susceptibles d'être infligées au responsable de traitement peut s'élever jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires du contrevenant. Cela concerne les collectivités locales et leurs établissements, mais également leurs satellites lorsqu'ils prennent la forme de sociétés commerciales (sociétés publiques locales, sociétés d'économie mixte) générant un chiffre d'affaires.

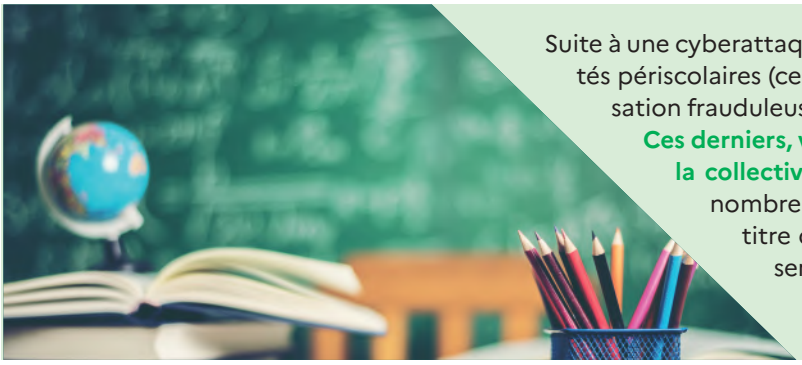
Ainsi, dans l'hypothèse d'une cyberattaque frappant une collectivité locale et occasionnant une fuite de données personnelles (ex. : données issues des comptes utilisateurs d'un téléservice), **la CNIL pourrait décider de sanctions pécuniaires dès lors qu'elle considérerait que cette fuite de données résulte en partie de manquements graves aux mesures de sécurité nécessaires à la protection des données personnelles.**

B. La responsabilité administrative pour faute

Les citoyens peuvent engager la responsabilité de l'administration pour faute lorsque cette dernière a manqué à ses obligations et que le manquement leur a causé un préjudice. La responsabilité d'une collectivité peut, à titre d'exemple, être engagée en raison des manquements du maire dans l'exercice de ses pouvoirs de police : nuisances sonores, troubles à l'ordre public, etc.

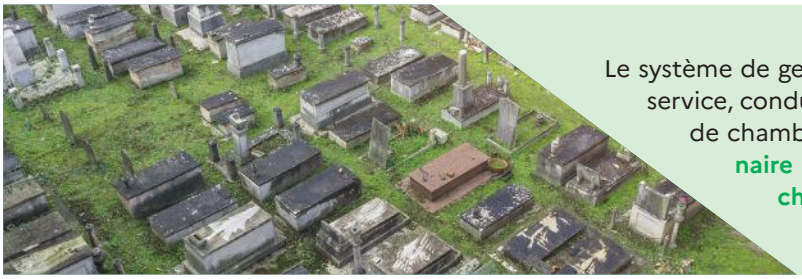
À l'avenir, l'application de ce régime de responsabilité pour faute en cas de cyberattaque n'est pas à exclure. **Des entreprises ou des administrés pourraient réclamer, auprès d'une collectivité locale ou d'un établissement public, l'indemnisation des préjudices subis du fait des conséquences d'une cyberattaque**, s'il peut être établi que les conséquences dommageables de l'attaque sont imputables à des manquements de l'administration dans l'application de la réglementation relative aux systèmes d'information.

Exemples plausibles de mise en cause de la responsabilité pour faute en cas de cyberattaque



Suite à une cyberattaque affectant un téléservice de paiement des activités périscolaires (centre de loisirs), un vol de données conduit à l'utilisation frauduleuse des coordonnées bancaires de plusieurs usagers. **Ces derniers, victimes d'achats frauduleux, se retournent contre la collectivité**, un contrôle de la CNIL ayant mis au jour de nombreux manquements aux règles de sécurité prévues au titre de la réglementation RGS pour ce téléservice : absence d'analyse de sécurité, homologation défaillante.

Une cyberattaque paralyse le système d'appel d'urgence des soignants dans un établissement d'hébergement pour personnes âgées dépendantes (EHPAD) et conduit au décès d'un pensionnaire. Les failles de sécurité identifiées après enquête résultent de manquements graves à la sécurité des systèmes d'information : maintenance et mise à jour défaillantes des systèmes d'infogérance ayant conduit à une panne globale. **La famille de la victime demande réparation auprès de l'EHPAD.**



Le système de gestion du service d'inhumation d'une ville est hors service, conduisant pour les familles à des frais supplémentaires de chambre mortuaire. **Les familles demandent au gestionnaire et aux services de la collectivité de prendre en charge ces frais qu'elles estiment injustifiés.**

C. La responsabilité de l'administration pour dommage de travaux publics

Lorsque des usagers subissent des dommages en raison du défaut d'entretien d'un équipement ou d'un ouvrage public, **la collectivité peut être condamnée à réparer les préjudices subis par les usagers** : c'est le principe de la responsabilité administrative pour dommage de travaux publics, qui s'applique notamment aux dommages causés aux usagers par les ouvrages publics et leurs accessoires.

Dans des cas exceptionnels, **une cyberattaque de grande ampleur pourrait conduire à la mise en cause de la responsabilité pour dommages de travaux publics d'une collectivité locale** si elle entraîne le dysfonctionnement d'une installation ou d'un ouvrage public et que cela occasionne des dommages aux usagers.

Exemples plausibles de mise en cause de la responsabilité pour dommage de travaux publics en cas de cyberattaque

Une cyberattaque conduit au piratage des automates et des systèmes de communication des stations de gestion locale d'un réseau d'épuration (eau potable) qui pourrait modifier les composants chimiques et conduire à un vrai danger pour la population locale. Cela a été le cas en Floride aux États-Unis en février 2021.

Une cyberattaque conduit à une panne de signalisation lumineuse d'un carrefour ou d'une voie publique, entraînant un accident.

2.2 RESPONSABILITÉ CIVILE : LA RESPONSABILITÉ PERSONNELLE DES ÉLUS ET AGENTS PUBLICS

Traditionnellement, un maire, un élu, ou un agent public peut voir sa responsabilité civile engagée sur son patrimoine personnel pour réparer des dommages causés aux tiers. Cela suppose toutefois l'existence d'une faute « détachable du service », qui se trouve caractérisée lorsque les faits reprochés révèlent des préoccupations d'ordre privé, procèdent d'un comportement incompatible avec les obligations qui s'imposent dans l'exercice de fonctions publiques ou revêtent une particulière gravité.

Une même faute peut à la fois être considérée comme une faute de service et comme une faute personnelle. C'est le cas lorsque la faute personnelle a été commise avec l'autorité et dans l'exercice des fonctions. Ce cumul de fautes peut conduire à la mise en jeu de la responsabilité pour faute de la collectivité locale ; à charge pour cette dernière d'engager une action récursoire à l'encontre de l'élu ou de l'agent en cause.

Cette responsabilité civile personnelle des élus et agents publics pourrait, à l'avenir, être engagée en cas de cyberattaque.

Exemple plausible de mise en cause de la responsabilité civile des élus et des agents en cas de cyberattaque

Un élu procède à l'homologation d'un nouveau téléservice sans que les analyses de sécurité les plus élémentaires aient été mises en œuvre et nonobstant les mises en garde techniques qui lui ont été adressées par l'agent responsable de l'informatique.

Une cyberattaque conduit à des fuites de données, notamment des vols de coordonnées bancaires.

La CNIL, lors de son contrôle, met en lumière les graves failles de sécurité du système, non conformes au RGS.

Les victimes de ces vols de données entendent obtenir réparation auprès de la collectivité locale gestionnaire du service.

En application du principe de cumul de responsabilités, la collectivité engage une action récursoire contre l'élu, la gravité de la faute commise par ce dernier dans l'exercice de ses fonctions conduisant à lui imputer une faute personnelle détachable du service.

2.3 RESPONSABILITÉ PÉNALE DES ÉLUS ET DES AGENTS

La mise en cause de la responsabilité pénale des agents et élus des collectivités locales et de leurs établissements publics peut résulter de la **violation des règles relatives à la protection des données personnelles,** mais aussi de la **commission de fautes d'imprudence ou de négligence**.

A. Les sanctions pénales résultant de la violation des règles relatives à la protection des données personnelles*

Le Code pénal réprime les atteintes les plus graves aux règles du RGPD. Par exemple, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures destinées à garantir la sécurité des données ou de ne pas tenir de registre des traitements. **Ainsi, un élu ou un agent pourrait faire l'objet d'une condamnation pénale à ce titre si les circonstances de la violation des règles du RGPD révèlent une faute personnelle.**

B. Les sanctions pénales résultant de fautes d'imprudence et de négligence**

Les agents publics, les élus ou l'organe exécutif des collectivités locales et de leurs établissements publics peuvent faire l'objet de poursuites pénales en cas de faute d'imprudence ou de négligence conduisant à des atteintes à l'intégrité physique des personnes. C'est le cas lorsque, sans être directement à l'origine du dommage, sa réalisation a été rendue possible par la violation manifeste d'une règle de prudence ou de sécurité ou en cas de faute caractérisée exposant autrui à un risque grave et immédiat.

Ainsi, un maire peut être condamné pour ne pas s'être assuré de la stabilité d'une cage de but mobile dont la barre transversale avait blessé un enfant ou pour avoir pris un arrêté d'ouverture d'une station de ski, sans vérifier le respect des règles de balisage des pistes, conduisant à des accidents. **Ce régime de responsabilité pénale pourrait trouver à s'appliquer au cas de cyberattaque conduisant à des atteintes aux personnes, s'il s'avère que des manquements graves à la sécurité des systèmes d'information les ont rendus particulièrement vulnérables à une cyberattaque et ont contribué aux dommages**: dysfonctionnement d'une barrière de parking blessant un usager, panne de signalisation conduisant à un accident, sabotage d'un réseau d'épuration conduisant à une contamination de l'eau potable et à un vrai danger pour la population locale…

* Article 226-16 du Code pénal
** Article 121-3 du Code pénal

EN CONCLUSION

Les collectivités locales et leurs établissements publics sont tenus à plusieurs obligations en matière de cybersécurité, tant dans leurs relations avec les usagers que dans l'exercice de leurs compétences.

Des obligations liées :
- à la protection des données personnelles ;
- mais aussi à la mise en œuvre de téléservices locaux ;
- et à l'hébergement de données de santé.

Dans ce contexte, les élus, dirigeants et les agents publics dans les collectivités locales et leurs établissements publics doivent avoir au cœur de leurs préoccupations :

- le respect des différentes réglementations présentées ;
- l'analyse préalable des risques pesant sur les systèmes d'information ;
- et la détermination des solutions techniques et organisationnelles.

En cas de cyberattaque et/ou de dommages liés, la responsabilité des collectivités locales et/ou de leurs agents peut être engagée, sur le plan administratif, civil ou pénal.

Pour aller plus loin, retrouvez sur :

Cnil.fr
- les conseils et recommandations pour les collectivités territoriales
- le guide sur la sécurité des données personnelles

ainsi que de nombreux conseils pour vous accompagner dans vos démarches.

L'ANSSI
- le guide sur la sécurité numérique des collectivités territoriales : l'essentiel de la réglementation

Cybermalveillance.gouv.fr
- des outils et un programme de sensibilisation dédié aux collectivités
- des ressources sur les principales cybermenaces et les bonnes pratiques pour s'en protéger (vidéos, fiches, affiches etc.)
- un accompagnement par des prestataires de confiance, avec un niveau d'expertise et de compétences reconnu en cybersécurité : en savoir plus sur le label ExpertCyber
- un service en ligne de diagnostic et d'assistance en cas de cyberattaque

EN RÉSUMÉ

LES OBLIGATIONS ET RESPONSABILITÉS DES COLLECTIVITÉS LOCALES EN MATIÈRE DE CYBERSÉCURITÉ

Les collectivités locales et leurs établissements publics sont tenus à 3 obligations en matière de cybersécurité, dans leurs relations avec les administrés et dans l'exercice de leurs compétences.

LES 3 OBLIGATIONS

	LA PROTECTION DES DONNÉES PERSONNELLES	LA SÉCURISATION DES TÉLÉSERVICES LOCAUX	LA SÉCURISATION DE L'HÉBERGEMENT DES DONNÉES DE SANTÉ
DÉFINITIONS	Une donnée personnelle est une information se rapportant à une personne physique identifiée ou identifiable : **nom, n° de téléphone, n° de sécurité sociale, photographie, etc.**	Un téléservice est un guichet d'accueil numérique permettant de procéder par voie électronique à des démarches administratives : **demande de permis de construire, inscription à la cantine scolaire, etc.**	Une donnée de santé est une donnée personnelle sensible. Elle est recueillie à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social : **radios, résultats de laboratoire, comptes rendus médicaux, etc.**
OBLIGATIONS	Dès lors que des données personnelles sont traitées (collecte, enregistrement, stockage, etc.), les collectivités sont soumises aux règles relatives à la protection des données personnelles.	Tout téléservice doit suivre au préalable un ensemble de règles de sécurité (réalisation d'une analyse des risques, définition des objectifs de sécurité, homologation du système d'information, etc.).	Les activités d'hébergement des données de santé sont soumises à des exigences de certification préalable.
TEXTES	• La loi Informatique et Libertés. • Le Règlement Général sur la Protection des Données (RGPD).	Le Référentiel Général de Sécurité : RGS.	Le Code de la santé publique.

LES RESPONSABILITÉS

En cas de cyberattaque, de dommages et/ou de méconnaissance de ces trois obligations, **la responsabilité des collectivités locales et/ou de leurs agents peut être engagée :**

Pour aller plus loin :
Cybermalveillance.gouv.fr
Cnil.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS