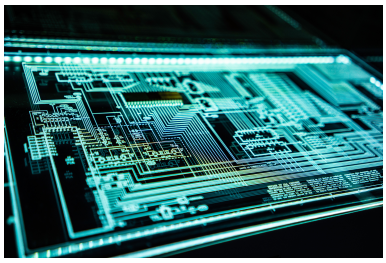
https://www.observatoire-collectivites.org/spip.php?article9013

Cyberattaques : quelles responsabilités pour les collectivités, les agents et les élus ?

- Actualité -



Publication date: mercredi 13 juillet 2022

Pas un jour sans que la presse ne se fasse l'écho d'une cyberattaque contre une collectivité territoriale. Avec de lourds impacts en termes de continuité du service public et des dommages qui peuvent être irréversibles. Mais qu'en est-il des responsabilités ? Si les pirates sont les premiers responsables, des négligences dans la sécurité du système informatique ne peuvent-elles pas engager la responsabilité de la collectivité, voire la responsabilité personnelle des agents ou des élus ?

[1]

Entre le vol, la divulgation ou la perte de données personnelles ou confidentielles, l'interruption préjudiciable de services publics ou le piratage de systèmes ayant de possibles impacts de sécurité (ex : système des feux tricolores, vannes pour gérer le débit d'un cours d'eau, régulation d'un système de distribution d'eau potable ou d'une station d'épuration, transports autonomes, coupures d'alimentation électrique...) les dommages potentiels d'une attaque informatique peuvent être très lourds et dans certains cas irréversibles. Sans évoquer l'hypothèse de complicités internes au sein de la collectivité, des négligences peuvent avoir facilité la tâche des cybercriminels. La responsabilité de la collectivité, voire la responsabilité personnelle (civile et/ou ou pénale) des agents (et pas uniquement des informaticiens) ou des élus de la collectivité peut-elle être engagée ?

Qui doit réparer le préjudice ?

La responsabilité première est bien entendu celle des cybercriminels. Encore faut-il qu'ils puissent être identifiés et appréhendés. La collectivité victime est quant à elle connue et facilement atteignable.

Si l'attaque informatique a été facilitée par des négligences internes (ex : système informatique mal sécurisé, gestion des mots de passe défaillante, logiciels informatiques périmés ou non mis à jour, anti-virus inexistant ou obsolète...), la responsabilité de la collectivité peut le cas échéant être engagée en cas de dommages causés à des administrés, des entreprises ou des usagers.

La responsabilité civile personnelle d'un élu ou d'un agent négligent peut également être envisagée. La faute personnelle ne se résume pas en effet à l'hypothèse d'un agent ou d'un élu qui a recherché un intérêt personnel (ex : agent corrompu qui prêterait son aide, contre rémunération, pour faciliter un piratage informatique). Elle peut aussi être caractérisée par une « faute d'une particulière gravité » (**Conseil d'Etat, 30 décembre 2015, NÂ° 391798 & NÂ° 391800**) avec la dose de subjectivité attachée à cette notion (pour une illustration en matière d'urbanisme voir : **Cour de cassation, chambre civile 1, 25 janvier 2017, NÂ° 15-10852**).

Un agent qui, lors d'une visite de chantier, laisse les clefs du véhicule sur le contact, ou un maire qui, restant seul le soir en mairie, ne ferme pas l'hôtel de ville en quittant les locaux, ne commettent-ils pas une faute d'une particulière gravité en cas de vol consécutif à leur négligence ? Sans trace d'effraction, un débat peut s'ouvrir... Il pourrait en

être de même pour un agent qui laisserait son ordinateur accessible et ouvert sans penser à le verrouiller. La question pourrait aussi se poser pour un agent ou un élu qui clique sur une pièce jointe dans un mail dont le caractère suspect aurait dû manifestement attirer son attention, qui connecte une clé USB externe sur le réseau informatique de la collectivité, qui utilise un mot de passe non sécurisé ou qui le divulgue à des personnes non habilitées... Si dans toutes ces situations, le juge ne retiendrait pas nécessairement l'existence d'une faute personnelle, le débat pourrait s'ouvrir et se conclure défavorablement pour le fautif notamment en cas d'accumulations de négligences de ce type. L'occasion de rappeler que la prévention n'est pas l'apanage des spécialistes mais qu'elle est l'affaire de tous et suppose l'engagement de chacun au service de la sécurité informatique.

En tout état de cause, la responsabilité de la collectivité pourrait dans ces hypothèses être engagée sur le fondement d'une faute de service ou sur celui d'une faute personnelle non dépourvue de tout lien avec le service. Dans ce dernier cas, la victime dispose en effet d'un droit d'option et peut actionner à son choix la responsabilité de la collectivité (avec recours contre l'agent) ou celle de l'agent ou de l'élu fautif.

Un exemple : l'attaque d'un réseau d'eau potable d'une ville

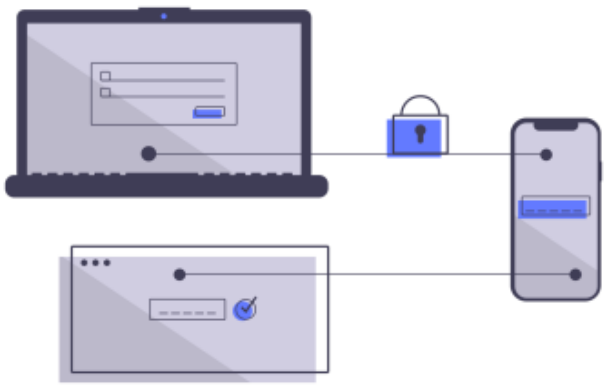
En Floride (Etats-Unis), en février 2021, une attaque informatique s'est traduite par la manipulation de la composition chimique des eaux de la ville. Le cybercriminel a augmenté le taux de soude caustique (le hacker a multiplié par dix la concentration de ce produit dans l'eau potable). Cette modification aurait pu avoir des conséquences graves si les employés de la station de traitement des eaux n'avaient pas réagi à temps. Or la cyberattaque n'a rien eu de très sophistiquée : le pirate s'est servi du logiciel TeamViewer, outil professionnel de prise de contrôle à distance des machines et utilisé par l'équipe de la station. L'enquête a mis à jour plusieurs négligences :

– tous les ordinateurs de la station disposaient du même et unique mot de passe pour TeamViewer ;

– il n'existait pas de pare-feu de sécurité entre Internet et le système d'information de la structure ;

– Le réseau informatique était basé sur le système d'exploitation Windows 7 dont Microsoft a arrêté les mises à jour le 14 janvier 2020... Une faille qui était connue puisque les autorités avaient averti toute organisation utilisant encore Windows 7 qu'elle s'exposait à attirer les cybercriminels prompts à exploiter les fins de mises à jour de systèmes d'exploitation et de logiciels.

Le même incident se serait produit en France avec des incidences sur la santé publique, on ne peut écarter l'hypothèse d'une recherche en responsabilité contre la collectivité, voire une recherche en responsabilité personnelle contre les décideurs (élus et/ou services de la DSI) qui n'ont pris les précautions élémentaires pour se prémunir de ce type d'attaques prévisibles.



Un acte de malveillance exonère-t-elle la

collectivité de toute responsabilité ?

Pas automatiquement. Le juge peut en effet estimer que les négligences commises par la commune ont permis l'acte de malveillance et sont constitutives d'un défaut d'entretien normal de l'ouvrage public. C'est par exemple ce qu'a jugé la cour administrative d'appel de Bordeaux (**Cour administrative d'appel de Bordeaux, 19 mars 2013, NÂ° 11BX01253**) concernant un dommage subi par un professionnel dont le matériel de sonorisation a été endommagé en raison d'une surtension électrique dans la salle des fêtes. L'expertise avait établi que la surtension provenait du compteur électrique de la commune dont les cosses avaient été desserrées. La commune déclinait toute responsabilité en invoquant cet acte de malveillance. La cour administrative d'appel de Bordeaux confirme la responsabilité de la comune (moins de 500 habitants) dès lors que le sinistre a été occasionné par une surtension imputable au desserrage des cosses du compteur situé sur la partie supérieure du tableau électrique communal placé sur le mur extérieur de la mairie. En effet « cet équipement n'était protégé par aucun système de fermeture et pouvait ainsi être manipulé par n'importe quelle personne ».

La commune ne rapportait donc pas la preuve de l'entretien normal de l'ouvrage. En outre « le maître d'ouvrage ne pouvant s'exonérer de sa responsabilité en invoquant le fait d'un tiers, la commune ne saurait se prévaloir utilement ni des actes de malveillance qui auraient été commis sur le tableau électrique accessible au public, ni de la faute commise par le comité des fêtes en fournissant l'électricité sans vérifier préalablement le bon état du système électrique ».

Appliqué ici à un compteur électrique, le juge ne serait-il pas tenté de suivre le même raisonnement s'agissant d'un réseau informatique trop perméable qui aurait permis des actes de malveillance ?

> Vous les attendiez ? Les voici ! Découvrez en exclusivité la nouvelle édition des #Actes https://t.co/XFK8C20f2r. Le thème : "les collectivités territoriales face aux cyberattaques". L'occasion de revenir sur le 20e colloque de l'@ObsSmacl et de répondre à vos interrogations pic.twitter.com/NzWBRq98Jb
>
> â€" Smacl Assurances (@SmaclAssurances) May 19, 2022

>

Qu'en est-il de la responsabilité pénale ?

Il n'y a pas que dans les hôpitaux où un piratage informatique peut avoir des conséquences sur la vie ou la santé. Les collectivités territoriales gèrent de nombreux services publics qui peuvent, en cas de défaillance, causer des dommages aux personnes et/ou à l'environnement. Que l'on songe au piratage d'un feu tricolore, d'une station d'épuration, d'une usine de traitement des déchets, d'un réseau d'eau ou de transport public... Sans parler du développement des véhicules autonomes où certaines collectivités sont pionnières.

En cas d'accident provoqué par un acte de malveillance, la responsabilité pénale des auteurs de négligence peut être envisagée. Bien sûr ce ne sont pas eux qui ont directement commis le dommage. Ce sont les cybercriminels les premiers responsables. Mais les élus et les fonctionnaires qui « ont créé ou contribué à créer la situation qui a permis la réalisation du dommage ou qui n'ont pas pris les mesures permettant de l'éviter », peuvent engager leur responsabilité pénale non intentionnelle s'ils ont commis une faute qualifiée :
– soit en cas de violation manifestement délibérée d'une obligation de prudence ou de sécurité imposée par la loi ou le règlement ;

– soit en cas de faute caractérisée et qui exposait autrui à un risque que le l'élu ou l'agent ne pouvait ignorer.

C'est ce second type de faute qui pourrait conduire à l'engagement de la responsabilité d'un élu ou d'un fonctionnaire lorsque les attaques informatiques se sont traduites par des conséquences corporelles ou pour l'environnement. L'exemple de l'accumulation de négligences évoquées dans l'attaque d'un réseau d'eau potable d'une ville de Floride (voir encadré précédent) pourrait ainsi avoir une traduction pénale. En effet, une accumulation de fautes, qui isolément semblent anodines, peut caractériser une faute qualifiée engageant la responsabilité pénale de son auteur. La Cour de cassation a en effet confirmé qu'une série de négligences et d'imprudences, qui entretiennent chacune un lien de causalité certain avec le dommage, permet d'établir l'existence d'une faute caractérisée d'une particulière gravité dont les prévenus ne pouvaient ignorer les conséquences (Cass. crim. 10 janvier 2006 : pourvoi nÂ° 04-86.428). Le juge pourrait suivre le même raisonnement après une attaque informatique avec des conséquences corporelles ou environnementales qui aurait été facilitée par un système de sécurité informatique obsolète et par des contrôles de sécurité insuffisants.

Les collectivités peuvent aussi engager leur responsabilité pénale en qualité de personne morale s'agissant des activités susceptibles de délégation de service public (ce qui n'empêche pas des poursuites concomitantes contre des élus et/ou des fonctionnaires). En ce qui concerne les personnes morales, il n'est pas nécessaire de prouver une faute qualifiée. Une négligence simple suffit. Et en matière de sécurité informatique, une négligence peut être facilement caractérisée. Cependant, comme pour les personnes physiques, il faudrait établir un lien de causalité certain entre la négligence imputée à la collectivité et le dommage corporel ou environnemental résultant de l'attaque informatique.

Et en cas de destruction ou détournement de données personnelles ?

La CNIL veille à la protection des données personnelles. En cas de piratage informatique ou de problèmes techniques ayant engendré une perte ou une divulgation de données personnelles, la collectivité devra être réactive et opérer un signalement à la CNIL. En effet Le règlement général sur la protection des données (RGPD) impose aux responsables de traitement de documenter, en interne, les violations de données personnelles et de notifier les violations présentant un risque pour les droits et libertés des personnes à la CNIL et, dans certains cas, lorsque le risque est élevé, aux personnes concernées.

Si des données personnelles ont fait l'objet d'une violation (perte de disponibilité, d'intégrité ou de confidentialité de données personnelles) que ce soit de manière accidentelle ou illicite, la collectivité doit documenter en interne l'incident en déterminant :

– la nature de la violation ;
– si possible, les catégories et le nombre approximatif de personnes concernées par la violation ;
– les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
– décrire les conséquences probables de la violation de données ;
– décrire les mesures prises ou envisagées pour éviter que cet incident se reproduise ou atténuer les éventuelles conséquences négatives.

Référentiel général de sécurité : peu de collectivités en conformité !

Depuis un décret 2010-112 du 2 février2010 les collectivités qui ont mis en place des téléservices ont l'obligation de réaliser un référentiel général de sécurité (RGS). Ce référentiel fixe les règles auxquelles les systèmes d'information mis en place par les autorités administratives doivent se conformer pour assurer la sécurité des informations échangées, et notamment leur confidentialité et leur intégrité, ainsi que la disponibilité et l'intégrité de ces systèmes et l'identification de leurs utilisateurs.
Il appartient notamment à la collectivité :

– d'identifier l'ensemble des risques pesant sur la sécurité du système et des informations qu'il traite, eu égard notamment aux conditions d'emploi du système ;

– de fixer les objectifs de sécurité, notamment en matière de disponibilité et d'intégrité du système, de confidentialité et d'intégrité des informations ainsi que d'identification des utilisateurs du système, pour répondre de manière proportionnée au besoin de protection du système et des informations face aux risques identifiés ;

– d'en déduire les fonctions de sécurité et leur niveau qui permettent d'atteindre ces objectifs et respecter les règles correspondantes du référentiel général de sécurité.

– de réexaminer régulièrement la sécurité du système et des informations en fonction de l'évolution des risques.

Très peu de collectivités sont en conformité.

Si l'incident constitue un risque au regard de la vie privée des personnes concernées, le responsable du traitement doit notifier l'incident à la CNIL via le téléservice dédié dans les meilleurs délais et au plus tard dans les 72 heures (si ce délai est dépassé la collectivité devra expliquer le retard) sachant qu'il est possible ensuite de faire une déclaration complémentaire s'il n'est pas possible de fournir toutes les informations requises dans ce délai car des investigations

complémentaires sont nécessaires.

> Attention : le fait de ne pas de ne pas procéder à la notification d'une violation de données à caractère personnel à la CNIL est passible de 5 ans d'emprisonnement et de 300 000 euros d'amende (Article 226-17-1 du code pénal modifié par l'ordonnance nÂ°2018-1125 du 12 décembre 2018). On peut également se demander, en cas de perte de données confiées à la collectivité, si le délit de l'article 432-16 du code pénal passible d'un an d'emprisonnement et de 15 000 euros d'amende (détournement ou destruction de biens publics par négligence) ne pourrait pas être caractérisé. Le texte est en effet relativement large et vise la destruction d'un « acte ou un titre, ou des fonds publics ou privés, ou effets, pièces ou titres en tenant lieu, ou tout autre objet » qui a été remis à l'agent public en raison de ses fonctions ou de sa mission. En matière d'abus de confiance qui vise le détournement « des fonds, des valeurs ou un bien quelconque », la Cour de cassation a bien estimé que « l'utilisation, par un salarié, de son temps de travail à des fins autres que celles pour lesquelles il perçoit une rémunération de son employeur » pouvait rentrer dans le champ de l'incrimination de l'article 314-1 du code pénal (Cour de cassation, chambre criminelle, 19 juin 2013, NÂ° 12-8303).

En cas de risque élevé, la collectivité devra également notifier les personnes concernées (en cas de doute sur la gravité du risque, la CNIL indiquera aux collectivités s'il est nécessaire d'informer les personnes).

La formation restreinte de la CNIL peut prononcer les sanctions suivantes en cas de manquement au RGPD ou à la loi « Informatique et Libertés » :
– un rappel à l'ordre ;
– une injonction de mettre en conformité le traitement avec les obligations prévues par les textes ou une injonction de satisfaire aux demandes d'exercice des droits des personnes. Cette injonction peut être assortie d'une astreinte dont le montant ne peut excéder 100 000 € par jour de retard ;
– une limitation temporaire ou définitive du traitement, son interdiction ou le retrait d'une autorisation ;
– le retrait d'une certification ;
– la suspension des flux de données adressées à un destinataire situé dans un pays tiers ou à une organisation internationale ;
– une suspension partielle ou totale de la décision d'approbation des règles d'entreprise contraignantes ;
– une amende administrative qui peut s'élever jusqu'à 20 millions d'euros dans le cas les plus graves (en cas de non-respect des principes fondamentaux du RGPD, des droits des personnes, des dispositions sur les transferts ou de non-respect d'une injonction d'une autorité) et 10 millions d'euros en cas de non-respect des obligations du responsable de traitement ou du sous-traitant (en matière de sécurité, d'analyse d'impact, de tenue du registre des activités, de désignation d'un DPO, ...).

Article 226-17-1 du code pénal

Le fait pour un fournisseur de services de communications électroniques ou pour un responsable de traitement de ne pas procéder à la notification d'une violation de données à caractère personnel à la Commission nationale de l'informatique et des libertés ou à l'intéressé, en méconnaissance des articles 33 et 34 du règlement (UE) 2016/679 du 27 avril 2016 précité ou des dispositions du II de l'article 83 et de l'article 102 de la loi nÂ° 78-17 du 6 janvier 1978, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.

Est puni des mêmes peines le fait pour un sous-traitant de ne pas notifier cette violation au responsable de traitement en méconnaissance de l'article 33 du règlement (UE) 2016/679 du 27 avril 2016 précité ou de l'article 102 de la loi nÂ° 78-17 du 6 janvier 1978 précitée.

Le piratage informatique n'est pas la seule cause possible d'atteinte à l'intégrité de données personnelles. La CNIL (**Délibération CNIL nÂ°2018-003 du 21 juin 2018**) a ainsi sanctionné une association en tant que responsable de traitement suite à un incident de sécurité sur son site internet rendant librement accessibles les données personnelles de ses utilisateurs, et ce, alors même que le site a été développé par une société prestataire.
L'ampleur de la violation (plus de 40 000 documents accessibles) et le degré de sensibilité des données concernées (références bancaires, numéros de sécurité sociale, salaires, passeports...) ont justifié la décision prise par la CNIL de sanctionner l'association à hauteur de 75 000 euros et de rendre publique cette décision, alors même que celle-ci était de bonne foi et faisait preuve de coopération avec ses services.

h2 class="spip">Le paiement des rançons est-il légal ?

Le paiement des rançons a été longtemps dans une zone grise. Dans une interview accordée à l'Argus de l'assurance (*Valeria Faure-Muntian (LREM) : "Il faut légiférer" pour interdire le paiement des rançons en cas de cyberattaque*, propos recueillis par Marie-Caroline Carrère, Argus de l'Assurance 6 mai 2021), Valeria Faure-Muntian alors députée et présidente du groupe d'études assurance de l'Assemblée (sous la législature 2017/2022), souhaitait que le législateur intervienne pour interdire cette pratique.

Le 13 octobre 2021 Valeria Faure-Muntian avait rendu public son rapport parlementaire sur la cyber-assurance. Il y était notamment préconisé d'inscrire dans la loi l'interdiction pour les assureurs de garantir, couvrir ou d'indemniser la rançon et se porter davantage vers la prévention, l'accompagnement et l'assurance des conséquences pour une entreprise ou la collectivité. Il était également proposé de sanctionner les entreprises, administrations ou collectivités qui procèdent au paiement des rançons à l'aide d'un tiers ou de manière direct, à l'instar de ce qui se pratique outre-atlantique. Le rapport préconisait également d'inscrire dans le code des assurances la subordination de l'activation des garanties de cyber-assurance à un dépôt de plainte auprès des services compétents.

L'Agence nationale de la sécurité des systèmes d'information (Anssi) déconseille toujours fortement de payer les rançons pour ne pas contribuer à alimenter le système. Ce d'autant que le paiement de la rançon n'est jamais un gage de restauration des données et peut alimenter des réseaux mafieux ou terroristes.

La direction générale du Trésor a mis en place, en juin 2021, un groupe de travail portant sur le développement d'une offre assurantielle de couverture des risques cyber, associant, outre les services de l'État, des représentants des entreprises, des organismes d'assurance et de réassurance et des experts du monde académique.

À l'issue des travaux, la direction générale du Trésor a publié un rapport le 7 septembre 2022 sur le développement de l'assurance du risque cyber. Il est notamment préconisé de permettre l'assurabilité d'une cyber-rançon (conditionnée par un dépôt de plainte préalable) ainsi qu'un principe général d'inassurabilité des sanctions administratives. Il est aussi préconisé de faciliter la transmission d'informations entre assureurs au sein d'une plateforme de partage de données sur les incidents cyber issue d'un partenariat public/privé, afin de disposer de davantage de données sur ce risque et d'accroître les efforts de sensibilisation de l'ensemble des acteurs au risque cyber.

La mesure dédiée aux cyber-rançons (avec obligation de dépôt de plainte pour être indemnisé) a été intégrée l'article 5 de la loi Lompi (LOI nÂ° 2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'intérieur) qui a inséré un nouvel article L. 12-10-1 dans le code des assurances autorisant les assureurs à couvrir le paiement des rançons. Cette prise en charge est toutefois conditionnée par un dépôt de plainte au plus tard dans les 72 heures après la connaissance de l'atteinte par la victime. Cette couverture d'assurance s'applique uniquement aux personnes morales et aux personnes physiques dans le cadre de leur activité professionnelle.

À la suite d'une concertation avec les acteurs concernés, la @DGTresor propose, dans un rapport dédié, un plan d'actions pour développer l'assurance du risque #cyber.
Plus d'infos https://t.co/S8uLXc1VM4 pic.twitter.com/t27v6PMoCm

â€" Ministère de l'Économie et des Finances (@Economie_Gouv) September 7, 2022

>

Comment prévenir les cyber-risques ?

Les nombreuses attaques récentes le démontrent : commune rurale, intercommunalité, métropole, région, centre hospitalier..., aucune structure n'est épargnée. Les conséquences des attaques de fichiers vulnérables peuvent être irrémédiables si elles conduisent à la destruction d'un fichier vulnérable ou à l'indisponibilité d'une ou plusieurs ressources névralgiques. C'est pourquoi en partenariat avec l'Association des ingénieurs territoriaux de France et CNPP Cybersecurity, SMACL Assurances a publié un guide de bonnes pratiques consacré à la prévention des cyber-risques. Pour accompagner les décideurs dans la mise en œuvre de leur plan de prévention, SMACL Assurances et ses partenaires exposent les points de vigilance et présentent plusieurs bonnes pratiques à appliquer par les collectivités territoriales. La cybermalveillance appelle une cybervigilance à tous les niveaux de la collectivité !

Découvrez le guide préparé en partenariat avec CNPP Cybersecurity :

La prévention des cyber-risques
Un guide pratique de SMACL Assurances en en partenariat avec l'AITF et CNPP Cybersecurity

Bon à savoir ! Cybermalveillance.gouv.fr a pour missions d'assister les particuliers, les entreprises, les associations, les collectivités et les administrations victimes de cybermalveillance, de les informer sur les menaces numériques et les moyens de s'en protéger. Il est également recommandé de consulter le site Internet de l'ANSSI qui précise les démarches qu'il convient d'engager en cas d'incident (plainte auprès des services de police ou de gendarmerie, saisine de la plateforme d'assistance aux victimes de cybermalveillance, notification auprès de la CNIL…).

Pour aller plus loin

Cybermalveillance.gouv.fr et la CNIL ont publié un guide sur les obligations et les responsabilités des collectivités locales en matière de cybersécurité (4 juillet 2022)

A télécharger sur le site de l'ANSSI :
– Attaques par rançongiciels, tous concernés – Comment les anticiper et réagir en cas d'incident ?
– Collectivités territoriales : face à la menace, saisissez-vous des enjeux cyber
– Sécurité numérique des collectivités territoriales : l'essentiel de la réglementation
– Cybersécurité : toutes les communes et intercommunalités sont concernées (en partenariat avec l'AMF)

A télécharger sur le site de la CNIL :
– Guide de sensibilisation au RGPD pour les collectivités territoriales

Le rapport parlementaire sur la cyber-assurance (PDF)

---

[1] Photo : Adi Goldstein sur Unsplash