« GESTION DU RISQUE NUMÉRIQUE ET DES DONNÉES PAR LES COLLECTIVITÉS TERRITORIALES »

Maître Cécile DOUTRIAUX, avocate fondatrice du cabinet Jurisdéfense Avocats, membre de la Chaire Cyberdéfense des écoles de Saint Cyr - Sogeti - Thalès

Victimes de 1.223 attaques en 2019, les collectivités territoriales sont devenues la cible privilégiée des cybercriminels.[1]

En ce début d'année 2020, la région Grand-Est a été victime d'une cyber-attaque d'ampleur, avec le piratage de 7.500 ordinateurs des élus et agents, en Champagne-Ardenne, Lorraine et Alsace, qui a nécessité l'intervention d'une quarantaine d'agents, pour restaurer le fonctionnement des systèmes d'information.[2]

Ces attaques pourraient se multiplier et être plus dévastatrices car les régions, départements, communes et EPCI[3] sont devenus de plus en plus dépendants du numérique, avec la dématérialisation des marchés publics, la multiplication des sites internet, des réseaux sociaux et des services en ligne pour permettre aux citoyens d'effectuer toutes sortes de démarches.

En effet, les collectivités territoriales connaissent un processus de modernisation continue de leur administration qui s'inscrit dans la réorganisation territoriale de la République, voulue par la loi NOTRe n° 2015-991 du 7 août 2015, pour renforcer les compétences des régions et des établissements publics de coopération intercommunale.

Pour assurer la gestion de leurs nombreux services (état-civil, inscriptions scolaires, inscription sur liste électorale, action sociale, gestion foncière et urbanisme, etc.), les collectivités territoriales doivent collecter des informations nominatives et organiser des fichiers manuels ou informatiques.

Parallèlement, les dispositifs de contrôle liés aux nouvelles technologies se multiplient (vidéo protection, applications biométriques, géolocalisation, etc.), sans oublier l'utilisation d'Internet, tant par les agents municipaux que par les usagers, pour simplifier et faciliter les services

La transformation numérique induit néanmoins de nouvelles menaces. Les applications ou fichiers utilisés par les collectivités recensent de nombreuses informations sur les administrés dont la divulgation est susceptible de porter atteinte aux droits et libertés des personnes ou à leur vie privée.

Les données des citoyens représentent un enjeu important dans le développement de l'intelligence artificielle et des villes intelligentes et si l'ouverture gratuite des données a été envisagée pour les

[1] Selon les déclarations de M. Jérôme NOTIN, du 17 février 2020 au Journal du Net https://www.journaldunet.com/economie/services/1489037-jerome-notin-cybermalveillance/

[2] https://www.francetvinfo.fr/france/grand-est/la-region-grand-est-touchee-par-une-cyber-attaque-de-grande-ampleur-7-500-agents-concernes_3834377.html

[3] Selon l'article L 5214-1 du code général des collectivités territoriales, un établissement public de coopération intercommunale (EPCI) est une structure administrative française regroupant plusieurs communes, afin d'exercer certaines de leurs compétences en commun

citoyens par la Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, les délinquants sauront tout autant utiliser ces données et les détourner, pour augmenter leurs profits.

A l'heure du RGPG, entré en vigueur le 28 mai 2018, pour renforcer la protection des données personnelles, les collectivités territoriales doivent se prémunir de l'engagement de leur responsabilité, pour défaut de sécurisation des systèmes d'information et atteinte à la confidentialité des données de leurs administrés.

L'altération des données ou des systèmes, leur destruction, leur chiffrement, ou leur vol par des personnes mal intentionnées est problématique.

Il est donc nécessaire d'anticiper, dès à présent, ces cyber-risques et sécuriser les données de la collectivité est fondamental, tant la demande de protection et de transparence des administrés est forte**.**

La mise en place d'une stratégie efficace s'impose en matière de cybersécurité et les collectivités peuvent bénéficier de l'aide de nombreux acteurs sur le terrain (ANSSI, AMF, CNIL, mission ECOTER, SOLURIS).

I. L'état des lieux des cyber-risques relatifs aux collectivités territoriales

A. Les chiffres

Selon un sondage IFOP, réalisé en avril 2019 pour la CNIL,[4] 70 % des Français se déclarent plus sensibles que ces dernières années à la protection de leurs données personnelles.

Les citoyens redoutent principalement le vol de données et les atteintes à la réputation sur les réseaux sociaux, mais aussi l'usurpation d'identité numérique, commise dans l'objectif de réaliser des actes délictueux à leur détriment.

Le rapport du ministère de l'intérieur du 9 juillet 2019, sur l'état de la menace numérique,[5] révèle que les atteintes aux systèmes de traitement automatisé de données (STAD), enregistré par la police et la gendarmerie, ont baissé de 9 % entre 2016 et 2018, mais que le vol de données est en hausse de 14 % en 2018.

Le vol physique de données (ex : par clé USB) est marginal (15%) et l'essentiel des fuites de données (69,8%) résulte d'un piratage en ligne, via le rançongiciel et l'hameçonnage.[6]

Ces chiffres sont en réalité sous-estimés car toutes les victimes ne portent pas plainte systématiquement, soit par crainte d'une atteinte à leur image, soit par résignation, puisqu'elles pensent que la condamnation des auteurs de l'infraction est impossible.

Effectivement, il s'avère parfois que l'identification et la poursuite pénale des auteurs de ces attaques est laborieuse, en raison du recours à des Botnets[7] et du caractère transnational de ces infractions.

D'où l'impérieuse nécessité, pour les collectivités territoriales, de sécuriser leurs systèmes d'information, en amont, pour éviter des difficultés.

---

[4] https://www.cnil.fr/fr/1-de-rgpd-une-prise-de-conscience-inedite

[5] https://www.interieur.gouv.fr/fr/Actualites/Communiques/L-etat-de-la-menace-liee-au-numerique-en-2019

[6] Selon le baromètre Data Breach publié au Forum International de la Cybersécurité en janvier 2020.

[7] Les botnets sont des réseaux de machines infectées contrôlés par un groupe de cybercriminel. Ces machines (souvent des PC) peuvent être infectés par des programme malveillants différents, mais au final, contrôlés par le même opérateur

Les motivations à l'origine de ces cyber-attaques sont principalement de nature économique avec le vol d'argent via des courriels pièges incitant à fournir des identifiants bancaires, et politique avec des campagnes de dénigrement ou d'influence visant à orienter le résultat d'un vote.

Bien évidemment, il faut réprimer ces agissements et la CNIL a enregistré 11.900 plaintes depuis l'application du RGPD,[8] ce qui représente une augmentation de 30 % par rapport aux années précédentes.

Manifestement, la sensibilisation au RGPD a fonctionné et les citoyens ont exprimé le souhait de voir la collecte déloyale et les atteintes à la confidentialité de leurs données sanctionnées.

B. Les secteurs et les types d'attaques

Les plaintes déposées auprès de la CNIL en 2019 concernent principalement :

- la diffusion non souhaitée de données sur internet (35,7 %),
- le déréférencement (+ 11,3 %),
- le secteur commerce/marketing (21 %),
- le secteur du travail (16,5 %),
- le secteur de la banque/Crédit (8,9 %),
- le secteur santé/social (4,2 %),
- les libertés publiques et les collectivités (3,7 %).

Le « top 5 » des secteurs les plus touchés en nombre de notifications (1282) de juin 2018 à juin 2019[9] sont :

- le domaine scientifique et technique (297),
- le commerce (279),
- la finance (275),
- l'administration publique (229),
- l'hébergement et la restauration (202).

Il peut sembler rassurant que les collectivités territoriales apparaissent en dernière position des plaintes déposées auprès de la CNIL, pour violation des données personnelles.

Toutefois, il est évident que les 1.223 attaques informatiques, perpétrées à l'encontre des collectivités territoriales en 2019, comprennent des captations de données, lesquelles n'ont pas nécessairement faite l'objet d'une notification d'incident.

Par conséquent, il existe certainement un décalage entre le nombre élevé de cyber-attaques dont ont fait l'objet les collectivités territoriales et le nombre réduit des plaintes déposées.

En effet, les plaintes ayant visé les collectivités territoriales mettent principalement en cause, pour le moment, les dispositifs de vidéo protection de la voie publique et la collecte excessive de données personnelles, lors de démarches administratives (par exemple, pour l'accès aux déchetteries ou l'inscription de son enfant à des activités).

[8] https://www.cnil.fr/fr/1-de-rgpd-une-prise-de-conscience-inedite
[9] Selon le baromètre Data Breach publié au Forum International de la Cybersécurité en janvier 2020.

De plus, il s'agit de sanctions administratives prononcées par la CNIL exclusivement, en qualité d'autorité administrative indépendante et les sanctions judiciaires des tribunaux ne sont pas intégrées à ces chiffres.

C. Les attaques proprement dites

Concernant les attaques visant les collectivités territoriales, elles consistent principalement en la défiguration de sites et le déni de service.

Ainsi, le site internet des collectivités est directement visé, soit pour bloquer son fonctionnement, soit pour le décrédibiliser, en affichant un message différent sur la page d'accueil.

A la suite des attentats de 2015, de nombreux de sites internet de mairies, de conseils généraux et régionaux (21.000) avaient été défaçés par des hackers.

Le tribunal correctionnel de Nancy avait d'ailleurs condamné trois internautes de la mouvance Anonymous en 2015 à des peines de prison avec sursis (jusqu'à 8 mois) et à une amende, pour avoir bloqué des sites internet de la région Lorraine, du conseil départemental de la Meuse et de l'Andra (Agence nationale de gestion des déchets radioactifs).[10]

Ces attaques qualifiées de « bas niveau » n'engendrent pas de préjudice financier important, puisqu'il s'agit principalement d'une atteinte à l'image.

Toutefois, ce type d'attaque par déni de service pourrait avoir des conséquences beaucoup plus importantes à l'avenir, car le mode opératoire, consistant à rendre indisponible l'accès à un serveur pourra entraver le bon fonctionnement de certains services (transports, électricité, eau, …) instaurés pas la ville intelligente.

En effet, en juin 2014, la commune de Nice a dû suspendre le paiement sans contact du stationnement en voirie, à la suite du détournement de données par un individu.[11]

Mais la principale attaque, la plus pernicieuse et la plus dangereuse, reste le rançongiciel, qui consiste à chiffrer les données des serveurs informatiques de la collectivité et à exiger le paiement d'une rançon, pour les récupérer.

Outre le préjudice financier et la captation de données, l'atteinte à l'image existe aussi.

Certaines attaques ont été relayées dans l'actualité, par exemple la mairie de Nuits Saint Georges et la communauté de communes de Gevrey-Nuits ont été victimes d'un rançongiciel le 14 novembre 2019, qui paralysé les sites municipaux et 64 sites communautaires, la demande de rançon s'étant élevée à 2.200 €.[12]

[10] https://www.zdnet.fr/actualites/nancy-trois-anonymous-condamnes-pour-des-attaques-contre-des-sites-web-39828566.htm

[11] http://www.territoires-intelligents.fr/analyses/cybersecurite-et-territoires-intelligents-les-collectivites-territoriales-sont-devenues-des-cibles-de-choix

[12] Selon l'article de Charlotte DELEY du 20 nov. 2019 publié dans le Journal de Saône et Loire et consultable sur le lien /www.lejsl.com/faits-divers-justice/2019/11/20/la-communaute-de-communes-et-la-mairie-de-nuits-victimes-d-une-cyberattaque

Ce montant, peu élevé, peut inciter les communes à payer la rançon, ce qui serait une erreur puisque cela revient à entretenir les réseaux criminels et rien ne peut garantir la restitution des données.

De plus, à défaut de paiement, par la collectivité, de la rançon exigée, les délinquants menacent de diffuser les données collectées sur internet, ce qui conduirait alors à placer ces collectivités en tête de liste des plaintes déposées auprès de la CNIL, pour atteinte à la confidentialité des données.

D. La multiplication des risques et l'augmentation massive des vulnérabilités

Les attaques visant les collectivités vont certainement augmenter en raison de l'externalisation massive de données via le nuage informatique, du développement des villes intelligentes et du recours à l'intelligence artificielle, qui nécessite l'exploitation massive de données.

En effet, les collectivités ont pour la plupart l'objectif de réunir en un réseau unique toutes leurs données éparses pour les traiter à un niveau général, afin d'améliorer la vie quotidienne des citoyens.

Echanges de données en temps réel, réactivité pour adapter la ville aux contraintes des usagers et aux attentes de citoyens, contrôle de la pollution, assainissement des déchets, surveillance des locaux et des équipements, construction de bâtiments écologiques, planification des services urbains tels que l'éclairage des rues, la gestion des déchets, des ressources en eau, coordination des différents services sont les avantages procurés par la ville intelligente.

L'utilisation des TIC est intéressante puisqu'elle permet d'optimiser la gestion des services urbains et de réaliser des économies, ce qui permettra de mieux financer la cybersécurité des collectivités territoriales !

Ces solutions offrent donc des avantages financiers, pour le citoyen, grâce à une meilleure information sur sa consommation en temps réel. Il lui serait alors possible de réduire sa facture d'électricité, grâce aux compteurs intelligents, comme Linky développé par ERDF et pour les collectivités, d'économiser des ressources limitées, gérer les dépenses énergétiques, connaître les zones et les périodes de consommation pour mieux en adapter la production et effectuer le relevé des compteurs à distance.

En définitive, les avantages pour la collectivité sont l'optimisation du fonctionnement des services, l'économie des coûts de gestion, l'efficacité accrue des services municipaux et la réponse, rapide, aux demandes des usagers.

La ville intelligente, pour être performante, doit recueillir massivement des données extrêmement diversifiées, grâce à des dispositifs équipés de puces, de codes-barres et de capteurs qui permettent de collecter et de diffuser de nombreuses données, sans que leur sécurisation ne soit garantie.

Or, assurer la cybersécurité de la ville intelligente est fondamental pour bénéficier de la confiance des citoyens utilisateurs et pour assurer la pérennité de telles structures, d'autant plus que leur mise en place nécessite de lourds investissements financiers pour les collectivités.

Cette confiance n'est pas acquise puisque les citoyens sont de plus en plus susceptibles d'engager la responsabilité de leur commune, de leur département ou de leur région pour violation de leurs données personnelles.

Ainsi, la justice est régulièrement saisie pour sanctionner des dispositifs qui n'offrent pas des garanties suffisantes.

A ce titre, le tribunal administratif a suspendu la décision de la ville de Marseille de mettre en place un vaste dispositif de surveillance automatisée, en s'opposant au projet voté par la région PACA

d'expérimenter aux abords du lycée Ampère à Marseille et du lycée des Eucalyptus à Nice, un système de reconnaissance faciale, pour mieux contrôler les allers et venues aux abords de ces deux établissements.[13]

Comment faire alors que l'utilisation massive des technologies nous rend plus vulnérables face à des délinquants soucieux d'étendre leur « terrain de jeu » ?

En réalité, des dispositifs insuffisamment sécurisés pourraient révéler et compromettre la confidentialité des données collectées.

De plus, le danger viendrait aussi de l'utilisation de nos données par les collectivités ou par les entreprises qu'elles ont désignées, en qualité de sous-traitants, pour assurer la connectivité des villes intelligentes.

On comprend donc l'importance de sécuriser les systèmes d'information et les données des collectivités territoriales.

II. La protection des données des collectivités : un enjeu majeur

A. La protection des données

1. L'identification des différentes données collectées par la collectivité

Il est fondamental, pour la collectivité territoriale, d'effectuer en amont, un tri entre les différentes données, sensibles et personnelles, pour connaître les obligations et la responsabilité susceptible d'être engagée, en cas d'incident ou de traitement illégal de ces données.

La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, a été modifiée par la par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelle, puis par son décret d'application du 1er août 2018.

Ensuite par ordonnance du 12 décembre 2018 et par un décret d'application n° 2019-536 du 29 mai 2019 de la loi, a mis la loi française en conformité avec le Règlement européen n° 2016/679 sur la protection des données (RGPD) du 27 avril 2016, entré en vigueur le 25 mai 2018.

Ainsi, les données « personnelles »[14] sont celles qui permettent d'identifier directement ou indirectement une personne. Cela peut concerner les informations directement nominatives (nom et prénom) mais aussi celles qui le sont indirectement, comme un numéro de téléphone, un numéro de plaque minéralogique, une empreinte digitale ou l'ADN d'une personne physique.

Toutes les données rattachées à une personne sont donc concernées, comme par exemple le nombre de repas de cantine facturés aux parents d'un enfant ou encore l'adresse IP avec laquelle l'internaute se connecte au site de la commune.

Les données « sensibles » sont, quant à elles, des données qui, directement ou indirectement, font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, les appartenances syndicales, ou encore les données relatives à la santé ou à la vie sexuelle des personnes. Le numéro de Sécurité sociale est par exemple une donnée sensible.

[13]Article de Mathilde Ceilles publié le 27/02/20 consultable sur https://www.20minutes.fr/societe/2728331-20200227-paca-malgre-interdiction-justice-region-envisage-abandon-reconnaissance-faciale-abords-lycees
[14] Selon l'article 2 de la loi « Informatique et libertés » n°78 – 17 du 6 janvier 1978

En principe, la collecte et le traitement des données sensibles sont interdits.[15]

Par exception, on peut enregistrer des données sensibles dans un fichier si elles sont pertinentes par rapport à la finalité du traitement (par exemple, l'appartenance syndicale des agents de la mairie, qui ont droit à des délégations d'heures, peut être enregistrée dans le fichier de gestion du personnel) et si la personne concernée a donné son accord écrit, préalablement à l'enregistrement de cette information, ou si ce traitement est justifié par un intérêt public général.

2. Les obligations des collectivités liées à l'informatique

Les collectivités sont amenées à traiter quotidiennement des données personnelles, ce qui comprend notamment la collecte, l'enregistrement, la conservation, la modification, l'extraction, la consultation, la communication, le transfert, l'interconnexion mais aussi le verrouillage, l'effacement ou la destruction des données à caractère personnel.

Ce traitement des données des administrés est soumis à différentes obligations qui doivent être respectées par les régions, les départements et les communes, pour qu'il soit licite.

a. Responsable de traitement et sous-traitant

Le responsable de traitement est la personne morale ou physique qui détermine les finalités et les moyens d'un traitement, c'est à dire l'objectif et la façon de le réaliser. En pratique, il s'agit généralement de la personne morale incarnée par son représentant légal.

Les maires et présidents des départements et des régions sont responsables des traitements informatiques et de la sécurité des données personnelles qu'ils contiennent.

Ces traitements sont nombreux et très variés et concernent le recensement de la population, la gestion des listes électorales, de l'état civil, de l'aide sociale, du cadastre, des transports, des crèches municipales, écoles, restaurants scolaires, centres aérés, le fichier des demandeurs d'emploi, les registres des personnes âgées ou handicapées pour les alertes (« fichiers canicule », grands froids…).

Ils concernent également la gestion dématérialisée des marchés publics, la gestion foncière, l'aménagement du territoire, la gestion des taxes et redevances (droits de voirie, droits immobiliers, taxes sur le chauffage et éclairage par électricité, facturation des ordures ménagères…), la vidéo-surveillance des locaux d'une collectivité accessibles[16] ou non au public, les téléservices permettant aux administrés de réaliser certaines démarches en ligne, la gestion administrative des ressources humaines (organisation du travail, rémunération, gestion des carrières et de la formation) et la géolocalisation des véhicules utilisés par les employés.

Souvent, les collectivités territoriales font appel à des entreprises prestataires pour effectuer certaines missions, ponctuelles ou récurrentes, soit pour des raisons financières, soit en raison d'un manque de main-d'œuvre compétente.

[15] Selon l'article 8 2 de la loi « Informatique et libertés » n°78 – 17 du 6 janvier 1978

[16] La mise en place d'une vidéo-surveillance des locaux d'une collectivité accessibles au public nécessite une autorisation préalable auprès de la Préfecture du département, accordée pour une durée de 5 ans renouvelable et l'information du public par voie d'affichage

Ces sous-traitants interviennent pour le compte du responsable du traitement selon les objectifs qui lui ont été assignés, définis dans le contrat de prestation de service.

Lorsqu'un traitement doit être effectué pour le compte d'une collectivité territoriale, celle-ci doit uniquement faire appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles, pour se conformer aux exigences du RGPD et garantir la protection des droits de la personne concernée.

L'article 4.8 du nouveau règlement européen retient que le sous-traitant est « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ».

L'instauration d'un nouveau régime de responsabilité à l'égard des sous-traitants, par le règlement européen, permet d'étendre certaines obligations incombant responsable du traitement au sous-traitant et notamment l'obligation de sécurité.

Ainsi, l'article 32.1 du règlement énonce que « compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant doivent mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté aux risques, y compris entre autres, selon les besoins ».

Avant le RGPD, en cas d'incident et de divulgation des données personnelles, il était difficile d'engager la responsabilité du sous-traitant et la plupart du temps, seul le responsable de traitement était responsable des failles de sécurité.

Depuis le RGPD, l'obligation de sécurité du sous-traitant se trouve ainsi alignée sur celle du responsable de traitement et la collectivité et le sous-traitant peuvent désormais être co-responsables en cas de violation de la confidentialité des données, ce qui est favorable aux communes, aux départements et aux régions.

Ainsi, l'article 82 du règlement dispose désormais que le responsable du traitement peut se dégager entièrement ou partiellement de sa responsabilité vis-à-vis des tiers, lorsqu'il démontre que cette responsabilité incombe à son sous-traitant.

Il convient toutefois être particulièrement vigilant lors de la signature de ces contrats de prestations de services, car les sous-traitants ont tendance à y insérer des clauses qui les dégagent de leurs responsabilités.

Il est donc important de soumettre le contrat à un avocat, avant sa signature, pour s'assurer de la présence des clauses obligatoires du RGPD et de l'équilibre des responsabilités de chacun.

b. Les obligations de la CT en qualité de responsable de traitement

Cinq principes issus de la loi informatique et libertés doivent être respectés par les collectivités territoriales, lors de la création d'un fichier comportant des informations personnelles.

- le principe de finalité :

qui impose que les informations ne peuvent être recueillies et traitées que pour un usage déterminé et légitime, qui doit correspondre aux missions de la collectivité responsable du traitement.

- le principe de proportionnalité :

qui implique que seules doivent être traitées les informations pertinentes et nécessaires pour la gestion des services municipaux.

Par exemple, lors d'une inscription a une cantine scolaire, il n'est pas pertinent de solliciter le numéro de sécurité sociale. Il peut être pertinent en revanche d'enregistrer les préférences alimentaires (ex : absence de sucre) mais pas l'état de santé (ex : diabétique) ni la religion, puisqu'il s'agit de données sensibles.

- le principe d'une durée limitée de conservation des informations :

Les informations personnelles ne peuvent pas être conservées indéfiniment dans un fichier.
Elles ne peuvent être conservées que pendant la durée nécessaire aux finalités pour lesquelles elles ont été collectées (ex : la durée de conservation des données collectées par vidéo-surveillance doivent être conservées pour une durée d'un mois).

- le principe de sécurité et de confidentialité des informations :

Les traitements doivent être sécurisés contre toute divulgation, atteinte à la confidentialité et accès non autorisés, ce qui implique que des habilitations doivent être strictement délivrées aux seuls agents qui ont légitimement le droit d'en prendre connaissance.

- le principe du respect des droits des personnes :

La collectivité territoriale, en qualité de responsable de traitement, doit garantir à ses administrés un droit d'accès, de portabilité, de rectification, d'opposition (sauf pour les fichiers fiscaux ou d'état civil), de limitation (gel des données pour une période donnée) et d'effacement des données collectées.

En 2018, 78% des plaintes réceptionnées par la CNIL concernaient une absence de réponse ou un refus, non motivé, d'accéder à ses données collectées. Or, les citoyens sont de plus en plus demandeurs de transparence de la part de leurs administrations.

c. La réalité du terrain

Sur le terrain, on peut relever une grande disparité des moyens et des pratiques de sécurité.

Les Communautés de communes sont généralement accusées d'investir trop peu dans la sécurité de leurs systèmes d'information.

En effet, selon le rapport « Menaces Informatiques et Pratiques de Sécurité en France » publié le 23 Juin 2016 par le CLUSIF[17], les budgets alloués à la sécurité de l'information sont en baisse ou en stagnation et seules 18% des collectivités voient leur budget dédié à la sécurité progresser, alors que pour la grande majorité (67%) la part allouée à la sécurité reste constante.

Par ailleurs, seules 32% des collectivités auraient formalisé une politique de sécurité des systèmes d'information (PSSI) pour maintenir un certain niveau de sécurité.

Pourtant, près de 90% des communautés disposaient, en 2013, de sites Internet et environ 20% développent même des applications spécifiques pour téléphone mobile ou tablette, pour favoriser notamment l'accès aux services publics à distance.

Quant aux réseaux sociaux, plus de la moitié des collectivités possèdent un compte Facebook et utilisent de manière régulière un compte Twitter en 2015, selon le baromètre Ideose.[18]

En revanche, les réseaux extranets-intranets, dont l'objectif est d'assurer une meilleure circulation de l'information et une collaboration efficiente au sein des équipes communautaires pour la gestion des ressources humaines, l'archivage documentaire, la mise en relation des agents) ne connaissent pas la même croissance.

Une enquête réalisée par la Gazette des Communes en 2015 recense environ 6.500 communes françaises qui disposeraient d'un site vulnérable sur 14.000 sites [19]

Chaque année, des centaines de sites Internet de mairies, de conseils généraux et de conseils régionaux sont victimes d'attaques informatiques.

Or, toutes ces attaques ne sont pas détectées et leurs conséquences pourraient potentiellement être graves dans le cadre des villes intelligentes, ce qui pourrait conduire à l'engagement de la responsabilité des collectivités territoriales.

III. Le droit applicable aux collectivités territoriales pour la gestion des données

Les collectivités territoriales doivent répondre des incidents dont elles sont victimes lors de cyber-attaques.

Régions, départements, communes et EPCI ne sont pas encore suffisamment préparés au risque d'une cyber-attaque, alors qu'ils collectent, utilisent et partagent de nombreuses informations privées sur leurs élus et leurs concitoyens.

[17] https://clusif.fr/publications/menaces-informatiques-et-pratiques-de-securite-en-france-edition-2016/?visible=public

[18] Voir http://www.ideose.com/barometre-collectivites-territoriales-reseaux-sociaux/

[19] Voir l'article « Plusieurs milliers de sites Internet de communes mal sécurisés » publié le 25/03/2015 par Julien Kirch et Sabine Blanc consultable à la page https://www.lagazettedescommunes.com/337105/plusieurs-milliers-de-site-de-collectivites-mal-securises/

Plusieurs lois ont renforcé la dépendance des collectivités au numérique comme la loi n°2004-809 du 13 août 2004 relative aux libertés et aux responsabilités locales, définissant le cadre réglementaire applicable aux opérations de télétransmission des données comptables, qui est à l'origine de la dématérialisation obligatoire des marchés publics et la généralisation des moyens de paiement, pour le recouvrement des recettes locales notamment.

Cette dématérialisation concerne aussi les échanges entre les mairies et les préfectures et elle est assurée par des entités telles que l'Agence nationale des titres sécurisés (pour les passeports, permis de conduire et certificats d'immatriculation), la plateforme COMEDEC pour la communication électronique des données de l'état civil et l'Agence nationale de traitement automatisé des infractions pour la dématérialisation de la gestion des amendes (PV électronique, envoi de l'avis de contravention, facilitation des paiements et des contestations).

Depuis la loi NOTRe n° 2015-991 du 7 août 2015**,** les collectivités de plus de 3 500 habitants doivent rendre accessibles, sur Internet, la plupart des informations publiques en leur possession (rapports, études, statistiques, codes sources, permis de construire, correspondances), mais doivent aussi assurer la diffusion des comptes rendus du conseil municipal*,* dans un délai d'une semaine, de manière permanente et gratuite.

La loi pour une République Numérique du 7 octobre 2016, avec l'ouverture des données publiques, oblige les administrations à offrir l'accès libre et gratuit aux données publiques pour permettre de créer de nouveaux services innovants, « au bénéfice des citoyens ».

Cette dépendance au numérique et les risques d'attaques informatiques qui l'accompagnent, oblige les autorités administratives à garantir la sécurité de leurs systèmes d'information par la cryptologie, l'utilisation des produits de sécurité et le recours à des prestataires de services de confiance, certifiés par l'État et l'ANSSI, selon le Référentiel Général de Sécurité (RGS).[20] Or, seules 18% des CT se seraient totalement conformées à ce référentiel.[21]

Enfin, le Règlement « eIDAS » n°910/2014 du 23 juillet 2014, applicable depuis le 1er juillet 2016 pour les services de confiance formule des exigences relatives à la reconnaissance mutuelle des moyens d'identification électronique, ainsi qu'à celle des signatures électroniques, pour les échanges entre les organismes du secteur public et les usagers.

A. Sanctions administratives et pénales

A défaut de respecter ses obligations en matière de protection des données, les collectivités s'exposent à des sanctions, qui peuvent être administratives et pénales.

1. Les sanctions administratives prononcées par la CNIL : loi informatique et libertés 1978

[20] Créé depuis le décret n° 2010-112 du 2 février 2010, la version initiale du RGS (v.1.0) a été rendue officielle le 6 mai 2010 et modifiée par une version 2.0 publiée par arrêté du Premier ministre du 13 juin 2014, une refonte de ce référentiel étant actuellement en cours pour le simplifier et l'harmoniser au règlement Le Règlement « eIDAS » n°910/2014 du 23 juillet 2014

[21] Selon le rapport « Menaces Informatiques et Pratiques de Sécurité en France » publié le 23 Juin 2016 par le CLUSIF

Tout incident informatique ou violation de données, présentant un risque pour les droits et libertés des personnes, doit être transmis à la CNIL, dans un délai de 72 heures, à la suite de la constatation de la violation.

L'article 4.12 du RGPD définit une violation de données à caractère personnel comme
une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

En qualité de personnes morales, les collectivités territoriales peuvent être déclarées pénalement responsables sur le fondement des articles 226-24 et suivants du Code pénal puisque selon l'Union européenne, il faut « engager la responsabilité des personnes morales lorsque celles-ci n'ont de toute évidence pas assuré un niveau de protection suffisant contre les cyberattaques ». [22]

Au titre de son pouvoir de sanction, la CNIL peut adresser des avertissements et des mises en demeure de faire cesser un manquement à la loi, et elle peut, en cas d'urgence, décider l'interruption du traitement des données.

Les sanctions administratives sont réparties en deux groupes en fonction de la durée, de la nature et de la gravité de la violation, selon le degré du dysfonctionnement constaté.

Ainsi, peuvent être prononcées :

- une amende correspondant à 2% du chiffre d'affaires mondial ou 10 millions d'euros d'amende en cas de violation des obligations incombant au responsable du traitement et au sous-traitant, à l'organisme de certification et à celui chargé du suivi des codes de conduite.

Exemples : l'absence de tenue d'un registre des traitements ou l'absence d'analyse d'impact préalable aux traitements des données personnelles.

- une amende correspond à 4 % du chiffre d'affaires mondial ou 20 millions d'euros d'amende, pour les infractions plus graves, liées au non-respect des droits des personnes pour le recueil du consentement de la personne concernée avant la collecte, le traitement ou le stockage des données personnelles, refus de suppression malgré son opposition…

Les montants élevés de ces sanctions ont avant tout un rôle dissuasif, car en réalité les peines sont moins élevées.

En effet, la CNIL est saisie fréquemment, mais son pouvoir répressif n'est pas toujours suffisamment dissuasif par manque de personnel et de moyens.

Ces raisons expliquent que les peines prononcées concernent avant tout des entreprises emblématiques du numérique.

Ainsi, une amende de 250.000 € a été prononcée contre la société BOUYGUES TELECOM le 26 décembre 2018 pour manquement à son obligation d'assurer la sécurité des données personnelles des utilisateurs de son site et une autre, de 50 millions d'euros, a été prononcée contre de la société GOOGLE LLC le 21 janvier 2019, pour manque de transparence, information insatisfaisante et absence de consentement valable pour la personnalisation de la publicité.

[22] Cons. 26, Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil.

Il semble peu probable que de telles peines puissent être prononcées à l'encontre des collectivités territoriales actuellement.

2. Les sanctions pénales prévues par la loi Informatiques et Libertés de 1978

Les collectivités territoriales peuvent être également passibles d'une peine de cinq ans d'emprisonnement et d'une amende de 300.000 € sur le fondement des articles 226-16 et suivants du Code Pénal pour défaut de sécurité, collecte illégale de données, refus de suppression malgré la demande de l'administré, lorsqu'elle est fondée sur un motif légitime, conservation au-delà du délai requis, divulgation sans autorisation des données à un tiers non habilité.

3. Les sanctions prévues par la loi Godfrain n° 88-19 du 5 janvier 1988

La loi Godfrain, relative à la fraude informatique, réprime les atteintes aux systèmes de traitement automatisé de données (STAD) ce qui concerne les attaques par déni de service et le piratage de données par rançongiciel.

Elles concernent davantage les auteurs des cyber-attaques que leurs victimes, mais en réalité, toute collectivité peut être victime d'un acte malveillant de la part de l'un de ses agents, comme il n'est pas rare que des attaques informatiques soient perpétrées, par le salarié d'une entreprise, par vengeance ou frustration.

Les peines prononcées sont plus importantes lorsqu'il s'agit d'une atteinte portée à un système de traitement automatisé de données mis en œuvre par l'État.

Ainsi, l'article 323-1 du Code Pénal réprime de deux ans de prison et de 60.000 € d'amende, le fait d'accéder ou de se maintenir, frauduleusement, dans un STAD et en cas de suppression ou de modification de données, la peine est portée à 3 ans d'emprisonnement et à 100.000 € d'amende.

Lorsque les infractions ont été commises à l'encontre d'un STAD mis en œuvre par l'Etat, la peine est portée à 5 ans d'emprisonnement et à 150.000 € d'amende.

L'article 323-2 du Code Pénal, réprime quant à lui le déni de service (fait d'entraver ou de fausser le fonctionnement d'un STAD) de cinq ans d'emprisonnement et de 150.000 € d'amende et lorsque cette infraction a été commise à l'encontre d'un STAD mis en œuvre par l'Etat, la peine est portée à 7 ans d'emprisonnement et à 300 000 € d'amende.

Enfin, selon l'article 323-3, le fait d'introduire frauduleusement des données dans un STAD, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de 5 ans d'emprisonnement et de 150.000 € d'amende.

Lorsque cette infraction a été commise à l'encontre d'un STAD mis en œuvre par l'Etat, la peine est portée à 7 ans d'emprisonnement et à 300.000 € d'amende.

Il convient de noter que les peines prévues par la loi Godfrain ont été renforcées par la loi n°2015-912 du 24 juillet 2015 -4 pour être davantage dissuasives.

En réalité, sur le terrain judiciaire, on constate que les peines prononcées sont le plus souvent des peines d'emprisonnement de 3 à 8 mois avec sursis.

Toutefois, si les cyber-attaques visent massivement un jour des collectivités territoriales, dans le cadre de villes intelligentes, l'entrave au fonctionnement des services les plus élémentaires de la vie citoyenne comme les transports, la production d'énergie et les services liées à la distribution d'eau par exemple, les auteurs appréhendés pourraient être sanctionnés plus lourdement.

B. Les failles courantes dans la gestion des données : finalité et consentement

On a pu dénombrer 2.044 notifications de violation de données en France depuis la mise en œuvre du RGPD du 28 mai 2018.

Outre l'absence de sécurisation matérielle suffisante des systèmes d'information, les plaintes déposées concernent principalement la finalité du traitement mis en place par la collectivité et le consentement des administrés.

1. Sécurité et finalité du traitement

Toute collectivité qui traite des données personnelles doit sécuriser l'accès, la consultation et la conservation de ces fichiers, afin de les protéger contre les intrusions et les altérations.

Le responsable de traitement, maire, président de la région ou du département, doit prendre toutes les mesures pour préserver la sécurité des données et notamment empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès.

Cette obligation s'applique aux responsables de traitement et aux sous-traitants.

Ainsi, le responsable du traitement et le sous-traitant ont l'obligation d'assurer sécurité physique et la sécurité logique de tous les traitements qui contiennent des données personnelles des agents et des administrés.

Seules les personnes habilitées en raison de leurs fonctions peuvent avoir accès aux données à caractère personnel. Par exemple, les données relatives à la gestion de la paie ne doivent être accessibles qu'aux personnes habilitées des ressources humaines.

La CNIL recommande d'adopter une politique de gestion des mots de passe, de sécuriser les postes de travail par un verrouillage automatique, ainsi que les comptes utilisateurs, tout en protégeant à la fois le réseau local et les locaux physiques.

Enfin, le responsable de traitement doit mettre en place une politique de sécurité des systèmes d'information et des actions de sensibilisation des utilisateurs par le respect d'une charte informatique et des consignes de sécurité.

La collectivité territoriale détermine les finalités du traitement, c'est-à-dire son objectif et ses modalités.

Il peut s'agir de la tenue et de l'actualisation de la liste électorale, mais aussi de la liste des personnes vulnérables (âgées et handicapées), mais aussi des traitements relatifs à la gestion des déchets, des aires d'accueil pour les gens du voyage…etc.).

La région, le département ou la commune doivent veiller à respecter strictement les finalités du fichier et ne doivent pas réutiliser les données collectées auprès des administrés pour la mise en œuvre d'autres fichiers, sans que ce nouvel usage ai été porté à la connaissance de ses administrés.

Dans la pratique, il est fréquent que les données collectées soient employées pour d'autres usages que ceux prévus initialement, par facilité et par souci de rapidité, pour éviter d'avoir à procéder à une nouvelle et fastidieuse collecte auprès des administrés.

Or, ce détournement de finalité du fichier est interdit et toute collectivité doit veiller à respecter strictement les raisons pour lesquelles les données ont été collectées, sous peine d'être lourdement sanctionnées d'une peine de cinq ans d'emprisonnement et d'une amende de 300.000 €, sur le fondement des articles 226-16 et suivants du Code Pénal.

2. Le consentement préalable de l'administré

L'administré a en théorie le pouvoir d'accepter ou de refuser l'utilisation de ses données par la collectivité territoriale.

En réalité, pour le traitement des données personnelles, ce consentement peut être implicite.
Il ne doit être explicite que pour la collecte des données sensibles.

Selon l'article 7 du RGPD, le consentement est une manifestation de volonté, libre et informée et la validité du consentement est logiquement liée à la qualité de l'information reçue, qui doit être rédigée en des termes simples et compréhensibles pour tout agent ou administré.

De plus, le consentement n'est valide que si la personne exerce un choix réel, ce qui implique qu'elle soit parfaitement informée de la nature des données collectées, la finalité du traitement, la durée de conservation, du transfert des données…

Enfin, la personne qui refuse de donner son consentement doit pouvoir continuer à bénéficier du service mis en œuvre par la collectivité.

Si pour les données personnelles, la collecte des données peut être implicite, le consentement doit nécessairement être explicite et positif pour les données sensibles.

Il ne saurait dès lors y avoir de consentement en cas de silence, de cases cochées par défaut ou d'inactivité. L'adage « Qui ne dit mot consent » n'est pas applicable dans le cadre de la protection des données personnelles et de manière générale il n'est pas reconnu en droit français.

Le consentement de la personne concernée doit être recueilli préalablement au traitement des données à caractère personnel.

L'administré garde tout au long du traitement des données la pleine maîtrise sur ses données personnelles. Le retrait du consentement doit être aussi simple que le fait de donner son consentement.

C'est au responsable du traitement, donc à la Mairie, au Département et à la Région de prouver qu'il sollicité et obtenu le consentement de la personne concernée par le traitement de ses données.

Mais en réalité, dans certains cas, les collectivités territoriales n'ont pas à recueillir le consentement des administrés puisque les traitements mis en œuvre sont imposés légalement ou nécessaires à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique.

C'est le cas pour la tenue du registre de l'état civil, sauf pour la diffusion d'événements familiaux (naissance, mariage, décès) dans les lettres de communication des collectivités à leurs administrés car dans ce cas, le consentement des personnes concernées doit être expressément sollicité.

S'agissant du compteur intelligent LINKY, par sa décision n° MED 2019-035 du 10 février 2020, la CNIL a mis en demeure les sociétés EDF et ENGIE en raison du non-respect des exigences relatives au recueil du consentement à la collecte des données de consommation, ainsi que pour une durée de conservation excessive des données de consommation.

En effet, recueillir le consentement est fondamental car les données de consommation (heures de lever et de coucher, périodes d'absence, nombre de personnes présentes dans le logement) sont de nature à porter atteinte à la vie privée et une pétition en ligne a déjà recueilli 166.344 signatures de citoyens pour s'opposer à son installation. [23]

Ainsi, des communes ont voté contre l'installation des compteurs Linky sur leur territoire et une action collective est prévue, alors que le compteur communiquant a été installé dans 24 des 35 millions de foyers français[24]

Déjà, par décision n° 2018- 007 du 5 mars 2018, la CNIL avait mis en demeure la société DIRECT ENERGIE au motif que le consentement au traitement de données personnelles n'étant pas libre, éclairé et spécifique, conformément à l'exigence posée par la loi Informatique et libertés du 6 janvier 1978.

A l'avenir, les collectivités territoriales pourraient de plus en plus souvent se trouver confrontées à une opposition de leurs administrés quant à la mise en place de services intelligents car que la susceptibilité des citoyens sur le traitement de leurs données est désormais plus importante et ils souhaitent davantage que soit garanti le respect de leur vie privée.

Bien évidemment, il n'est pas souhaitable que la responsabilité des collectivités territoriales puisse être engagée en raison des cyber-attaques dont elles sont avant tout les victimes.

C'est la raison pour laquelle mettre en place des solutions pour prévenir les cyber-attaques est fondamental.

IV – <u>La gestion des risques pour assurer une meilleure cybersécurité des collectivités territoriales</u>

[23] https://www.mesopinions.com/petition/politique/petition-nationale-mettre-compteur-linky-etat/39642 consulté le 04/03/2020

[24] Article de Béatrice Colin publié le 24/02/20 consultable sur https://www.20minutes.fr/societe/2725819-20200224-opposants-compteur-linky-vont-bientot-lancer-action-collective-justice

Le développement des villes intelligentes va nécessiter de recourir à des objets connectés, qui devront être sécurisés et à un délégué à la protection des données, qui assurera la conformité des traitements mis en œuvre avec la loi.

De plus, la faille étant avant toute humaine, lorsqu'une collectivité est victime d'une attaque informatique, puisque l'ouverture d'une pièce jointe vérolée ou l'utilisation d'un lien qui renvoie à un site malveillant, est fréquent, il convient de sensibiliser les élus et les agents par la diffusion d'une charte informatique et par des manifestations.

A. Recourir à des objets connectés qui offrent des garanties importantes

Souvent, les objets connectés ne sont pas suffisamment sécurisés, ce qui pose un problème pour le développement des villes intelligentes.

Pour minimiser les risques d'un non-respect du traitement des données, le RGPD oblige les entreprises à intégrer la protection des données personnelles dès leur conception.

Ainsi, l'application de ce principe « Privacy by design » permet de mettre en œuvre des mesures préventives pour empêcher la collecte de données personnelles sans raison légitime et la suppression des données s'il n'y a pas ou plus de raisons de les stocker, mais aussi de limiter les risques de violation des données personnelles.

Concrètement, pour y parvenir, il est possible de recourir à la pseudonymisation des données, c'est-à-dire par le remplacement de certaines données à caractère personnel par un pseudonyme, ce qui rend la personne concernée par les données inidentifiable, puisque les données sont ainsi « séparées » de l'identité de la personne.

Mais aussi à la minimisation de la collecte des données, ce qui signifie que seules les données, nécessaires à la finalité recherchée par l'entreprise, seront collectées.

Le principe du « Privacy by design » est étroitement lié au « Privacy By default » selon lequel chaque entreprise traitant des données applique par défaut la protection maximale pour chaque nouvelle application, produit ou service traitant des données personnelles.

B. L'élaboration d'une charte informatique

Parmi les mesures de protection, le facteur humain est un élément central à prendre en compte, car une grande partie des incidents informatiques trouvent leur origine dans les agissements des agents, employés par les collectivités territoriales.

Un nombre important d'agents font courir des risques inconsidérés à leur collectivité en envoyant de simples courriels contenant des informations sensibles vers l'extérieur ou en utilisant des services en lignes gratuits de stockage et de partage de données en ligne via le nuage informatique.

Par ailleurs, les agents sont susceptibles de publier des informations sensibles sur les réseaux sociaux, sans même en avoir conscience.

Clefs USB et disques durs externes sont, quant à eux, tout aussi exposés car ces objets ne nécessitent généralement pas de mot de passe pour accéder à leur contenu. Ils peuvent être volés, perdus ou les

données qu'ils contiennent peuvent être récupérées *via*, par exemple, l'infection de l'ordinateur familial.

Enfin, l'usage massif des technologies mobiles, l'essor du *« bring your own device »* (BOYD) qui consiste à utiliser ou à apporter des appareils personnels dans un cadre professionnel, est également risqué.

Ces terminaux personnels, généralement peu ou pas protégés, comportent souvent des vulnérabilités et constituent pour les hackers de véritables portes d'entrée, pour s'introduire dans les systèmes d'information professionnels.

De plus, le développement de services de stockage et de partage en ligne, placent les données hors du contrôle des élus des collectivités territoriales, alors même que leur responsabilité peut être engagée.

Ainsi, établir une charte, clarifiant les rôles et responsabilités de chacun, en informant tous les services du plan de gestion de crise, en cas de cyber-attaques, est primordial.

Cette charte devra rappeler les règles de sécurité informatique élémentaires (ex : le choix d'un mot de passe robuste) les droits et les obligations des agents concernant l'utilisation du matériel informatique de l'entreprise (ex : l'interdiction d'ouvrir les pièces jointes provenant d'expéditeurs inconnus, l'utilisation abusive des réseaux sociaux, la navigation sur des sites Internet non sécurisés…).

Pour être réellement efficace, une charte informatique doit toujours assortir un comportement inapproprié de sanctions, qui peuvent aller du simple avertissement au licenciement.

C. Désignation d'un délégué à la protection des données (DPO)

Les collectivités territoriales traitent un volume croissant de données dans le cadre de leurs missions et sont soumises à des réglementations importantes en matière de protection des données.

Depuis le RGPD entré en vigueur le 28 mai 2018, elles doivent désigner un délégué à la protection des données collectées par elles.

1. DPO interne ou externe

Le rôle du délégué à la protection des données est d'informer et de conseiller la collectivité territoriale, ses élus et ses agents.

Il doit contrôler le respect du règlement et du droit national en matière de protection des données, conseiller la collectivité sur la réalisation d'une analyse d'impact relative à la protection des données et en vérifier l'exécution, coopérer avec la CNIL et être son point de contact en cas de demande d'information ou de notification d'incident.

Il doit aussi organiser une veille juridique et technique sur les sujets touchant aux données personnelles, élaborer un plan de communication interne pour informer l'ensemble des agents de ses missions au sein de la collectivité, cartographier les traitements, réaliser une étude d'impact, prioriser les actions à mener, gérer les risques et organiser la procédure interne à suivre en cas d'incident.

Désigner un délégué est fondamental pour assurer une meilleure protection des données.

Or, seul 38% des collectivités territoriales auraient désigné un DPO et 46% s'y refuseraient. [25]

[25] Rapport sur les « Menaces Informatiques et Pratiques de Sécurité en France » publié par le CLUSIF le 23/06/2016

La réticence des élus est souvent principalement liée à des raisons financières, surtout dans les communes de petites tailles, raison pour laquelle elles sont tentées de désigner leurs secrétaires de Mairie en qualité de DPO.

Ce choix n'est pas toujours pertinent car ils manquent souvent de temps pour assurer ces missions et il peut y avoir un risque de conflit d'intérêts.

Cela explique d'ailleurs que les conseillers municipaux et le maire ne peuvent jamais être désignés pour exercer ces fonctions de DPO, car ils prennent directement part aux décisions lors de l'assemblée délibérante de la commune.

Désigner un agent titulaire ou contractuel de la collectivité peut être judicieux si cet agent a des compétences juridiques et informatiques avérées, car sa proximité permet une réactivité immédiate.

A défaut, il est nécessaire de recourir, partiellement ou totalement, à un délégué externe compétent et sur ce point, la CNIL recommande de recourir à un avocat, qui connaît parfaitement la réglementation relative au RGPD.[26]

2. Mutualisation

Face à l'exigence coûteuse de nomination d'un Délégué à la Protection des données introduite par le RGPD, il est possible de mutualiser cette fonction entre différentes structures à l'échelle d'un service intercommunal, départemental ou régional.

Pour les petites et moyennes communes, la meilleure option est effectivement de désigner un DPO mutualisé pour réaliser des économies et c'est le choix qui a été effectué dans certains départements ou certaines régions comme en Hauts-de-France où depuis 2018, 1200 collectivités ont délibéré pour faire de l'Adicoleur un DPO mutualisé.

Cette mutualisation a été rapidement étendue à d'autres communes et départements (Beauvais, Creil, Compiègne et elle est même envisagé au Havre.

Dans ce cas, les collectivités territoriales ont l'obligation de conclure une convention de mutualisation pour définir les outils, les moyens alloués au DPO et la répartition des responsabilités en cas d'incident.

Dans la mesure du possible, il est souhaitable de contracter avec des prestataires français ou européens, dont les serveurs sont situés sur le territoire national, afin de conserver la maîtrise de ses données.

Il est important également de s'assurer du non-transfert des données hébergées vers d'autres pays tiers et des conditions générales de vente et d'utilisation.

Des audits réguliers peuvent également être réalisés pour s'assurer de la sécurité des systèmes d'information.

D. Sensibiliser et former les élus et les agents

La collectivité territoriale doit également sensibiliser les élus, agents et usagers aux bonnes pratiques en matière de cybersécurité.

Les collectivités ne sont pas seules et de nombreux acteur, publics et privés, peuvent très concrètement les aider à gérer les nouveaux risques liés au numérique et à s'organiser pour lutter contre les cyber-attaques.

[26] Selon le guide de la CNIL dédié aux collectivités territoriales pour la sensibilisation au RGPD publié en 2019

Ainsi, pour les acteurs publics, un référent territorial de l'ANSSI est présent dans chaque région du territoire[27] pour sensibiliser et diffuser les bonnes pratiques, au plus proche des territoires et la CNIL publie régulièrement des guides pour rendre la réglementation plus accessible et favoriser le respect des lois, en matière de protection des systèmes d'information et des données.

La CNIL[28] et l'ANSSI[29] ont aussi élaboré des guides pratiques de bonne qualité dédiés à la cybersécurité des collectivités territoriales en 2019 et 2020.

Certains acteurs privés sont résolument tournés vers les collectivités territoriales et se sont donnés pour mission de leur offrir des solutions technologiques et de les sensibiliser.

Parmi eux, la mission ECOTER, est une association ayant pour but le développement des systèmes de communication et d'information dans les collectivités, mais elle assure également les fonctions de veille, conseils et échanges en organisant différents colloques avec le fournisseur de solutions Engie ou encore le réseau Soluris qui offrent des solutions numériques territoriales.

Les experts informatiques de l'AMF délivrent également leurs conseils à l'égard des collectivités locales, sur le site Internet de l'association.

Afin de lutter efficacement contre la cybercriminalité, certains territoires mettent en place des solutions innovantes afin de protéger leurs systèmes d'information et les données personnelles de leurs citoyens. Le projet « Safegouv » mis en place par la ville de Marseille en juin 2017,[30] introduit la première plate-forme éducative nationale de sécurité informatique dédiée aux institutions publiques.

L'idée est de tenter de détecter les failles des sites de la ville, du conseil régional Provence-Alpes-Côte d'Azur et de la Région Provence-Alpes-Côte d'Azur, mais également les failles possibles des objets connectés et applications qui pourraient être utilisés par la ville intelligente.

Si les métropoles sont nombreuses à avoir déployé différents dispositifs pour lutter contre la cybercriminalité, les petites et moyennes communes manquent encore de moyens financiers et logistiques.

Conclusion :

Les collectivités territoriales, devenues massivement dépendantes au numérique, sont désormais la ciblé privilégiée des cyber-attaques.

Leur vulnérabilité pourrait devenir encore plus importante avec l'avènement des villes intelligentes, le recours à l'intelligence artificielle et aux objets connectés.

Les citoyens et administrés exigent une plus grande transparence et la protection de leur vie privée, ce qui pourrait les conduire à déposer plus facilement plainte contre la collectivité, qui n'aurait pas suffisamment sécurisé ses systèmes d'information pour éviter la divulgation de leurs données.

Assurer la cybersécurité des traitements instaurés par les Régions, les Départements et les Communes est par conséquent primordial.

Pourtant, selon un sondage IFOP, réalisé en 2018, 66 % des fonctionnaires estiment que leur administration ne possède pas de programme de cybersécurité, seulement 49% estiment que leur

[27] Toutes les régions sont dotées d'un référent de l'ANSSI à ce jour, à l'exception d'Orléans, Toulouse et Lyon.
[28] https://www.cnil.fr/sites/default/files/atoms/files/cnil-guide-collectivite-territoriale.pdf
[29] https://www.ssi.gouv.fr/uploads/2020/01/anssi-guide-securite_numerique_collectivites_territoriales-reglementation.pdf
[30] http://prevention.marseille.fr/actualites/safegouv-un-projet-pour-securiser-le-systeme-d-information-de-la-ville

organisation a correctement évalué l'importance des enjeux de la cybersécurité et leur faculté d'identifier une cyber-attaque ne dépasse pas 37 %.[31]

En effet, la cybersécurité des SI n'est pas toujours une priorité pour certaines collectivités et pour 40 % des fonctionnaires**,** la restriction budgétaire explique l'absence ou le développement partiel d'une véritable politique de cybersécurité.

Les petites communes sont généralement celles qui manquent le plus d'informaticiens ou de personnel pour prendre en considération le risque cyber.

Respecter les droits des personnes : accès, portabilité, rectification, suppression et d'opposition est également fondamental puisqu'en 2018, 78% des plaintes réceptionnées par la CNIL concernait une absence de réponse ou un refus non motivé d'accéder à ses données collectées.

Des solutions existent pour garantir la cybersécurité des collectivités territoriales !

Tant au niveau technique avec le développement par les entreprises françaises innovantes de produits de sécurité certifiés**,** qu'au niveau juridique avec l'élaboration d'une charte informatique pour sensibiliser les agents, la désignation d'un DPO externe et mutualisé et la sensibilisation des élus et des agents.

Pour atteindre une cybersécurité efficace et opérationnelle, les collectivités peuvent bénéficier de l'accompagnement de nombreux acteurs publics : l'ANSSI, la CNIL et privés : l'AMF, la mission ECOTER et le réseau Soluris.

En réalité, la principale difficulté, notamment pour les petites et moyennes communes est le financement, en raison des réductions de dotation globale de fonctionnement depuis la loi NOTRe.

L'absence de lisibilité sur la répartition des compétences et des responsabilités de chacun, selon une étude d'impact remis à l'assemblée nationale 18 décembre 2019[32] est également un facteur aggravant.

Au final, la nouvelle répartition des compétences est source de nombreuses difficultés pour les collectivités territoriales, en raison de l'impossibilité de délimiter clairement des champs de compétences exclusifs de chacune des collectivités.

Ces difficultés devront être réglées si l'on souhaite garantir la cybersécurité et le bon fonctionnement des services offerts par les collectivités territoriales à leurs administrés.

[31] https://www.ey.com/Publication/vwLUAssets/ey-sondage-acteurs-publics-cybersecuritee-et-esecteure-public/%24FILE/ey-sondage-acteurs-publics-cybersecuritee-et-esecteure-public.pdf

[32] https://www.vie-publique.fr/rapport/272406-evaluation-de-limpact-de-la-loi-du-7-aout-2015-notre par Bruno Questel - Raphaël Schellenberger