Note n°39/20

14 mai 2020

Olivier Kempf
Chercheur associé
Fondation pour la recherche stratégique

Cybersécurité et résilience : les grandes oubliées des territoires

La crise de la Covid-19 frappe durement nos sociétés. Le bilan sanitaire, le confinement ou encore la dépression économique qui s'annonce sont à l'évidence au premier rang des préoccupations. Pourtant, la cybercriminalité a profité de la crise pour augmenter encore son activité. Il y a probablement des attaques menées au niveau national mais force est de constater que les criminels ont visé les plus faibles et les moins protégés.
Si les particuliers et les PME sont évidemment concernés, il convient de regarder les collectivités publiques décentralisées, aussi bien les collectivités territoriales que les établissements hospitaliers : tous ont subi de nombreuses agressions cyber, révélant un phénomène d'ampleur, celui de l'oubli du cyber par ces collectivités de premier niveau. Cette note vise à faire le point de la question.

Les collectivités territoriales ne sont pas épargnées par la cybercriminalité

Une brève histoire des cyberagressions des collectivités territoriales

Les collectivités territoriales (CT) ont subi une première vague d'agressions cyber en 2015, à la suite des attentats terroristes[1]. Il s'agissait d'attaques contre leurs sites internet, principalement par des défacements mais aussi, parfois, par des campagnes de déni de service distribué (DDoS). Il y avait déjà eu quelques exemples de ce type auparavant, comme le défacement du site de la

[1] « Après les attentats, les collectivités locales découvrent la cybersécurité », *Les Echos*, 21 janvier 2015.

ville de Fruges en janvier 2013 ou la suppression d'informations sur le site internet du Sancerrois. À la suite de cette vague, la *Gazette des communes* avait effectué, en mars 2015, un recensement qui montrait que 6 500 communes avaient des sites très vulnérables[2].

Les choses ont poursuivi leur cours et malgré les initiatives des autorités (l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a notamment lancé un certain nombre d'actions sur le sujet, la CNIL s'y intéresse aussi) ou des médias et spécialistes (Cybercercle, *Acteurs Public*, FIC, *SD magazine*, association *Déclic*), la cybercriminalité s'est développée notamment contre les collectivités territoriales. On a ainsi assisté, dès 2018 mais plus visiblement au cours de l'année 2019, au développement d'attaques par rançonnage (*ransomware*), d'abord contre des villes américaines. Baltimore, Atlanta, Las Vegas ou la Nouvelle-Orléans sont les plus connues, mais « *au moins 170 systèmes (informatiques) de comté, de ville ou d'Etat ont subi une attaque de ransomware depuis 2013 et 22 de ces attaques ont eu lieu en 2019 seulement* »[3] selon la conférence des maires (équivalent américain de l'association des maires de France (AMF) pour les villes de plus de 30 000 habitants).

La France a connu un mouvement similaire. La ville de Vannes fut une des premières victimes, dès février 2016[4], avec le virus Locky[5]. Dès juillet 2018, la mairie de la Croix-Valmer dans le Var est agressée par « *une attaque peu banale* », aux dires du journaliste[6]. Mais ce type d'agressions va justement se multiplier en 2019 : Sarrebourg en juin[7], Sequedin dans le Nord en juillet[8], Huez dans l'Oisans en septembre[9], l'agglomération Grand Cognac en octobre[10] comme la Communauté de communes de Trois-Rivières dans l'Aisne[11], Nuits-Saint- Georges et sa communauté de commune en novembre[12] tout comme Aussonne en Haute-Garonne[13]. Ainsi, l'ANSSI a traité 18 incidents liés à des rançongiciels dans la santé en 2019, ce qui en fait le secteur le plus touché devant celui des collectivités territoriales (14 incidents) sur les 69 incidents de rançonnages relevés par l'agence[14].

L'année 2020 a confirmé cette tendance : en janvier, la mairie d'Aimargues dans le Gard est touchée[15] ; en février, la région Grand Est est frappée[16] tout comme la ville de Combloux[17] ou celle de Tullins[18]. En mars, ce sont Charleville-Mézières et, surtout, la métropole Aix-Marseille qui

[2] « Plusieurs milliers de sites internet de communes mal sécurisés », *La Gazette des communes*, 25 mars 2015.
[3] « Un groupe de maires américains affirme ne plus vouloir payer de rançons aux pirates informatiques », *ZD net*, juillet 2019, modifié le 3 mars 2020.
[4] « Cybersécurité. 1 200 agents et 45 élus formés contre le piratage », *Le Télégramme de Brest*, 17 juin 2017.
[5] « Virus informatique. Le rançongiciel Locky sévit en France », *Ouest France*, 3 mars 2016.
[6] « Var : La mairie de la Croix-Valmer refuse de payer la rançon après le piratage de son système informatique », *20 minutes*, 31 juillet 2018.
[7] « Comment la ville de Sarrebourg a lutté contre une cyberattaque paralysant sa mairie », *Le Figaro*, 17 juin 2019.
[8] « Drôle de situation à Séquedin, où la mairie a été victime d'une importante cyberattaque cet été », *La Voix du Nord*, 19 septembre 2019.
[9] « La mairie d'Huez victime d'une cyberattaque », *Le Dauphiné*, 10 septembre 2019.
[10] « Cyberattaque : l'agglomération Grand Cognac refuse de payer la rançon », *Le Parisien*, 31 octobre 2019.
[11] « Une cyber-attaque évitée au siège de la Communauté de communes des Trois-Rivières à Buire », *L'union*, 31 octobre 2019.
[12] « La communauté de communes et la mairie de Nuits victimes d'une cyberattaque », *Le bien public*, 20 novembre 2019.
[13] « Haute-Garonne : la mairie d'Aussonne victime d'une cyberattaque », *La Dépêche,* 19 novembre 2019.
[14] « Cybersécurité : 18 incidents liés à des rançongiciels dans la santé traités par l'ANSSI en 2019 », *Ticsanté*, 30 janvier 2020.
[15] « Aimargues, la mairie victime d'une cyberattaque », *Objectif Gard*, 29 janvier 2020.
[16] « Le réseau informatique de la région Grand Est piraté », *L'Est éclair*, 19 février 2020.
[17] « Combloux : la mairie victime d'une cyberattaque », *Radio Mont-Blanc*, 28 février 2020.
[18] « Isère : la mairie de Tullins-Fures victime d'une cyberattaque, une rançon est demandée », France 3, 3 février 2020.

sont durement touchées[19], notamment à la veille des élections municipales (les listes d'émargement sont indisponibles[20]) alors que la crise sanitaire met les services publics sous tension. Martigues ou Vrigne-aux-Bois dans les Ardennes[21] sont également atteintes. La vague ne cesse pas avec la pandémie de coronavirus puisque deux petites communes du Morbihan sont affectées début avril[22].

Le service public hospitalier est lui-même fortement ciblé[23]. Le cas le plus emblématique a été le CHU de Rouen, touché en novembre 2019[24], mais en mars 2020, une agence de santé de l'Illinois[25], un hôpital tchèque[26] ou l'hôpital de Saintes[27] sont également attaqués, ainsi que l'AP-HP parisienne[28], tout ceci au milieu de la crise de la Covid-19, qui semble inciter les cybercriminels à augmenter leurs actions tous azimuts. Les faux messages circulent[29] et même l'OMS s'est fait attaquer[30] de même que l'hôpital de Fleurance[31].

On pourrait poursuivre l'énumération : elle est cependant déjà assez frappante pour constater que les collectivités territoriales, quels que soient leur taille ou leur statut, sont devenues des victimes courantes de cyberagressions. Ces dernières revêtent plusieurs types.

Typologie des agressions

On classe en général les cyberagressions en quatre catégories, selon la règle des « 4 S » : espionnage, sabotage, subversion et escroquerie.

Espionnage

L'espionnage est la plus courante et la moins décelée des cyberagressions. Les affaires en la matière concernent principalement les États ou les grandes entreprises. Il s'agit le plus souvent de vol de brevets ou de renseignements de recherche ou développement. Mais d'autres informations sont également recherchées : contacts avec les clients, positions de négociation, éléments financiers.

Cela concerne évidemment les collectivités territoriales : certes, elles sont soumises à des obligations de données ouvertes (loi NOTRe) et l'on pourrait considérer que la question ne se pose pas. Cependant, elles passent des marchés publics ou détiennent des informations

[19] « Marseille, Martigues, Charleville-Mézières, les villes françaises sous attaque des ransomwares », *ZDNet*, 16 mars 2020.
[20] « Municipales : attaque informatique 'massive' à la mairie de Marseille », *Le Parisien*, 15 mars 2020.
[21] « Les services de la mairie de Vrigne-aux-Bois touchés par la cyberattaque », *L'Ardennais*, 13 mars 2020.
[22] « Cyberattaques : de nouvelles mairies rançonnées à l'heure du coronavirus », *L'Express*, 3 avril 2020.
[23] Les agresseurs avaient déjà frappé le système britannique dès 2017, ce qui avait suscité un rapport du NHS (*National Health Service*), pointant la question de la protection contre les cyberagressions.
[24] « A la suite de la cyberattaque, 7 experts sont arrivés au CHU de Rouen », *Paris-Normandie*, 17 novembre 2019 ; « Collège des DSI/RSI de Normandie, les enseignements de la cyberattaque du CHU de Rouen », *DSIH*, 24 février 2020.
[25] « Une agence de santé a été visée par un rançongiciel en pleine épidémie de coronavirus », *Numerama*, 13 mars 2020.
[26] « Un hôpital tchèque frappé par une cyberattaque en pleine épidémie de COVID-19 », *ZD Net*, 14 mars 2020.
[27] « Coronavirus : l'hôpital de Saintes victime d'une fake news », Hélène FM, 17 mars 2020.
[28] « L'AP-HP victime d'une cyberattaque », *Les Echos*, 23 mars 2020.
[29] « Coronavirus en Occitanie: Le message alarmiste (et viral) d'une infirmière du Samu est une intox », *20 minutes*, 22 mars 2020.
[30] « En pointe sur le coronavirus, l'OMS est visée par des hackers de haut niveau », *Numerama*, 24 mars 2020.
[31] « Fleurance. Le réseau informatique de l'EPSL attaqué », *La Dépêche*, 2 avril 2020.

personnelles, économiques ou fiscales, soit de leurs collaborateurs, soit de leurs administrés ; sans même parler de la question de la protection des données personnelles, devenue une obligation depuis l'adoption du Règlement général de protection des données (RGPD), car elles détiennent des données sensibles qui peuvent intéresser des tiers.

Dans le secteur public, les données de santé sont très recherchées[32]. Aux États-Unis, 176 millions de dossiers de santé ont été piratés entre 2010 et 2017. En France, le ministère de la Santé a recensé en 2016 1 341 déclarations d'attaques subies par des hôpitaux, des cabinets de ville, des EHPAD, etc. Le 20 juillet 2018, les données de santé d'1,5 million d'habitants de l'État de Singapour ont été dérobées[33]. Les données de santé valent trois fois plus cher que des données personnelles classiques (nom, adresse, numéro de téléphone). Elles permettent plus facilement des tentatives d'escroquerie (hameçonnage) ou encore de fraude (à l'assurance maladie, par exemple). Mais il s'agit aussi de donner des bases de référence pour la recherche et développement des grandes sociétés pharmaceutiques[34].

Sabotage

Une collectivité territoriale ou un établissement de santé peuvent être la cible d'attaques de sabotage. Cela peut passer par un défacement de site internet, ou encore par une attaque en déni de service (DoS) ou déni de service distribué (DDoS) qui consiste à saturer de requêtes un serveur informatique pour le faire tomber. Encore s'agit-il là d'agressions « extérieures ». Ainsi, comme indiqué précédemment, le site de l'AP-HP a subi une attaque DDoS au beau milieu de la crise sanitaire.

Mais les attaquants peuvent vouloir entrer dans le système proprement dit : cela passera par des courriels piégés (avec une pièce jointe qui permet d'installer un agent malveillant), plus ou moins profilés par le biais de l'ingénierie sociale, désormais facile à réaliser grâce aux réseaux sociaux. Une fois entré, l'agresseur cherchera à progresser de poste en poste jusqu'à pénétrer un compte d'administrateur de système, ce qui lui donnera les accès privilégiés au système d'information. Ce faisant, il peut détruire de l'intérieur tout ou partie du système. Des informations peuvent être supprimées, ainsi que cela était arrivé au site internet du Sancerrois.

Subversion

La subversion consiste principalement à changer l'état d'esprit du public. Les agresseurs peuvent viser une réputation, par exemple en mettant une nouvelle image sur la page d'accueil d'un site internet (le maire déguisé en Hitler, par exemple) ou en détournant le texte qui y est inscrit. Ils peuvent également se faire passer pour quelqu'un, ce qui peut provoquer des dégâts énormes. Ainsi, une prétendue cyberarmée syrienne avait piraté le compte Twitter de l'agence *Associated Press* et avait annoncé que la Maison-Blanche était attaquée : le Dow Jones avait immédiatement perdu 300 points[35].

Le développement des infox (*fake news*) et de la « post-vérité » est également favorisé par les réseaux sociaux. Des rumeurs informatiques se répandent, se faisant passer pour telle ou telle

[32] « Vol de données, chantage, cyber-espionnage : comment les hackers ciblent les hôpitaux », *Le Quotidien du médecin*, 23 août 2019 ; « Données médicales, pourquoi elles valent de l'or pour les hackers », *Rude baguette*, 17 juin 2019 ; « Sécurité : inquiétudes pour les données de santé des Français », *ZD Net*, 28 octobre 2019.
[33] « Vol massif de données personnelles et médicales à Singapour », *Tic Santé*, 24 juillet 2018.
[34] « Pourquoi les hackers chinois cherchent à dérober des données médicales », *01 net*, 27 août 2019.
[35] Olivier Kempf, « Le cyberterrorisme : un discours plus qu'une réalité », *Hérodote*, 2014/1-2, n° 152-153, pp. 82-87.

personne. Ce peut être anodin, comme cette (fausse) infirmière du Samu de Toulouse[36] ou plus grave, comme cette prétendue information de l'hôpital de Bourgoin-Jallieu annonçant une infection maximale[37]. Mais les maires eux-mêmes peuvent être victimes d'infox, avec de nombreux exemples, comme ceux des maires de Metz[38] et de Castres[39].

D'autres maires peuvent être victimes indirectes d'infox ou devoir lutter contre ces rumeurs, comme le maire de Pieux (Manche), qui dément l'installation d'une vidéosurveillance sur la plage[40], celui de Crozon – une levée précoce de confinement[41], ou la mairie de Saint-Maur, qui crée une page internet pour démonter des fausses informations[42].

On le voit, l'information publique est désormais au centre des préoccupations, même au niveau local – et non seulement national.

Escroquerie

L'escroquerie est aujourd'hui le phénomène le plus rapide et le plus handicapant pour les maires. En premier lieu, la technique de l'hameçonnage ne cesse d'augmenter et de viser des collectivités territoriales de plus en plus réduites, comme nous l'avons vu.
Mais d'autres techniques existent, comme celle du faux changement de coordonnées, mésaventure survenue à la mairie de Sens : la méthode du pirate « *consiste à se renseigner sur les activités d'entreprises du BTP avant de contacter leurs clients, en l'occurrence la mairie de Sens et d'autres structures moins emblématiques en Île-de-France. L'escroc se fait passer pour l'entreprise du bâtiment avant d'expliquer que la société a changé de coordonnées bancaires et qu'il convient de virer l'argent sur un autre compte* »[43]. Une technique proche est celle du faux ordre de virement (connue aussi sous le nom d'arnaque au président), ce qu'a bien compris la municipalité de Mondragon, qui a averti ses administrés du danger[44].

L'escroquerie affecte également le secteur sanitaire et hospitalier, comme le rappelle *Le Monde*[45] : « *Au nombre des nouvelles victimes de cette escroquerie devenue monnaie courante depuis une dizaine d'années – depuis 2010, 3 000 sociétés en ont été victimes pour un montant global de 752 millions d'euros, selon la police judiciaire –, figurent des hôpitaux publics, des établissements d'hébergement pour personnes âgées dépendantes (Ehpad), des pharmacies, des grossistes ou encore des collectivités locales* ».

Fragilité des collectivités territoriales

Les collectivités territoriales présentent de nombreuses fragilités numériques. Cela est dû principalement à deux facteurs.

---

[36] Cf. note 29.
[37] « Hôpital de Bourgoin-Jallieu, alerte à la fake news », *L'essor 38*, 27 mars 2020.
[38] « Non, Dominique Gros, maire de Metz, n'a pas refusé d'enlever le porc des cantines », *Rue89 Strasbourg*, 20 décembre 2018.
[39] « Le maire sortant de Castres victime d'une fake news relayée par le candidat RN », *La Dépêche*, 21 février 2020.
[40] « Vidéosurveillance sur une plage de la Manche, le maire dénonce 'des fake news' », Actu.fr, 20 février 2019.
[41] Cf. Tifenn Clinkemaillié, « Facebook s'attaque aux fake news sur le coronavirus », *Les Echos*, 31 janvier 2020.
[42] « Saint-Maur s'attaque aux fake news », *Le Parisien*, 20 juin 2019.
[43] « Île de France : le spécialiste de l'escroquerie aux virements cueilli à sa descente d'avion », *Le Parisien*, 21 octobre 2019.
[44] « Attention, escroqueries aux faux ordres de virement ! », mairie-mondragon84.fr.
[45] « Le secteur de la santé visé massivement par les escroqueries aux faux virements », *Le Monde*, 2 avril 2020.

Tout d'abord, la complexité de l'organisation territoriale rend les choses difficiles : régions, départements, communautés de communes et agglomérations, sans compter les syndicats mixtes soit de niveau départemental soit de la commune (établissements publics intercommunaux, EPCI) : le millefeuille territorial rend les choses malaisées, surtout pour un domaine émergent.

Ensuite, la plupart des collectivités territoriales, particulièrement celles de petite taille, n'ont pas les moyens d'une action en la matière. Pour la plupart, elles utilisent des prestataires informatiques extérieurs pour assurer la mise en place et le suivi de leurs systèmes informatiques. Autant dire qu'elles n'ont pas de directeurs des systèmes d'information (DSI) et encore moins de responsable de la sécurité des systèmes d'information (RSSI) : d'une part parce que la ressource disponible sur le marché est rare, d'autre part parce que ces talents sont généralement chers, donc hors de portée de bourse de la plupart des collectivités territoriales. Elles font donc face à la même difficulté que les PME et les ETI dans le secteur privé : elles constituent une cible évidente, détiennent des données nombreuses mais ne sont pas capables de se saisir de la question.

Des acteurs (presque) oubliés

Constatons enfin que ces acteurs sont presque oubliés, tout d'abord parce que l'État n'a pas vraiment les moyens de s'en occuper. Il y a pourtant une prise de conscience nationale des enjeux de la cybersécurité : débutée avec le Livre blanc sur la défense et la sécurité nationale de 2008, la mobilisation s'est depuis poursuivie au niveau du pays avec notamment la création de l'ANSSI en 2009 puis la définition d'opérateurs d'importance vitale (OIV) astreints à des règles numériques de protection renforcées dès 2013. De même, le Forum international de la Cybersécurité (FIC) de Lille a été fondé au milieu des années 2000 par le général de gendarmerie Watin-Augouard et la gendarmerie nationale, dont la mission est d'être proche des territoires, est très sensible à cette question. Il a depuis pris une importante européenne, avec 15 000 visiteurs en janvier 2020. En 2018, la Revue stratégique de cyberdéfense[46] consacre quelques paragraphes aux collectivités territoriales.

Il reste que les moyens sont encore peu utilisés au niveau local. L'ANSSI a bien créé, en 2015, un dispositif de délégués régionaux de SSI et nommé, en 2019, un chargé de mission à la cybersécurité des territoires[47]. Pourtant, en 2018, un sondage montrait que « *pour 66 % des fonctionnaires en collectivités interrogés, leur administration ne possède pas de programme de sécurité, et seulement 49 % d'entre eux estiment que leur organisation a correctement évalué l'importance des enjeux de cybersécurité. Pour ces employés des services publics, leurs organisations sont en retard* »[48]. Il en est de même quand on les interroge sur la capacité de réaction : « *Au total, 53 % des personnes interrogées estiment leur organisation en mesure d'identifier une cyberattaque. Mais ce nombre chute pour les fonctionnaires territoriaux : ils ne sont plus que 37 % à se montrer confiants* ».

Des initiatives commencent à se faire jour, comme la publication régulière d'articles sur le sujet par le magazine *Acteurs publics*[49] ou la tenue d'un colloque consacré à la question en février 2020, organisé par la chaire Saint-Cyr de cyberdéfense[50]. L'ANSSI a publié en janvier 2020 un

[46] Revue stratégique de cyberdéfense, SGDSN, février 2018.
[47] Voir le site de l'ANSSI : https://www.ssi.gouv.fr/agence/cybersecurite/action-territoriale/
[48] « Les collectivités territoriales : maillon faible de la cybersécurité du secteur public ? », *Numerama*, 7 mars 2018.
[49] « La cybersécurité s'invite dans les collectivités », *Acteurs publics*, 19 février 2020.
[50] Chaire de cyberdéfense et cybersécurité Saint-Cyr Thalès SOGETI : programme du colloque, février 2020.

guide consacré à l'essentiel de la réglementation de cybersécurité à destination des collectivités territoriales[51]. Pourtant, la montée des rançonnages attaquant le secteur public ou le secteur hospitalier appellent à une mobilisation plus importante de la part des acteurs concernés, au premier rang desquels il faut compter les élus.

Quelle réponse des responsables de collectivités territoriales ?

La responsabilité des élus

Les élus sont responsables de la cybersécurité des systèmes informatiques employés par leurs collectivités territoriales mais aussi des EPCI (établissements publics de coopération intercommunale) qui en dépendent.

En effet, les élus sont soumis à plusieurs obligations.

La première est celle du Référentiel général de sécurité (RGS[52]) complété des recommandations de l'ANSSI, émises dans le guide susmentionné. La version 2.0 de ce référentiel date de 2014. Une troisième version doit prendre en compte la réglementation européenne. Il « *s'impose spécifiquement aux systèmes d'information mis en œuvre par les autorités administratives dans leurs relations entre elles et dans leurs relations avec les usagers* » et indirectement « *il s'adresse à l'ensemble des prestataires de services qui assistent les autorités administratives dans la sécurisation des échanges électroniques qu'elles mettent en œuvre* ». Il recommande d'une part une méthodologie de mise en conformité, d'autre part des règles et bonnes pratiques à mettre en place (certification et horodatage électroniques, audit de sécurité).

Par ailleurs, comme le remarquent D. Mullenex et G. Morat, « à *l'instar des personnes morales de droit privé, il n'est pas à exclure que les collectivités territoriales puissent voir leur* ***responsabilité pénale*** *engagée devant les juridictions répressives sur le fondement de l'article 121-2, alinéa 2 du Code pénal*[53]*, par exemple, pour les dommages causés à autrui par l'intermédiaire d'un système d'information non sécurisé* »[54].

La loi *NOTRe* de 2015 impose aux collectivités territoriales de plus de 3 500 habitants de rendre accessibles, sur internet, la plupart des informations publiques en leur possession. La loi de 2016 pour une République numérique oblige les administrations à offrir l'accès libre et gratuit aux données publiques. Rappelons également le règlement européen *eIDAS*, en vigueur depuis 2016, qui formule des exigences sur les moyens d'identification électronique ainsi que la signature électronique.

Enfin, les responsables de collectivités territoriales sont considérés comme des responsables de traitement. A cet égard, ils encourent la responsabilité pénale associée au traitement des données personnelles, selon les instructions données par la CNIL puis par le règlement européen de protection des données personnelles (RGPD). Cette responsabilité pourrait être mise en cause à la suite de divulgation de données qui ferait suite à une cyberattaque résultant d'un système d'information non sécurisé.

---

[51] ANSSI, « Sécurité numérique des collectivités territoriales : l'essentiel de la réglementation ».
[52] ANSSI, *Référentiel général de sécurité*.
[53] « *les collectivités territoriales et leurs groupements ne sont responsables pénalement que des infractions commises dans l'exercice d'activités susceptibles de faire l'objet de conventions de délégation de service public* ».
[54] « Cybersécurité, les obligations des collectivités ? », Weka.fr, 20 février 2015.

Selon le baromètre Databreach rendu public au FIC 2020, 3,7 % des plaintes déposées à la CNIL en 2019 concernent les libertés publiques et les collectivités. Il reste que de nombreuses attaques contre les collectivités territoriales n'ont probablement pas suscité de déclaration d'incident… Notons que la plupart des plaintes concernent aujourd'hui les dispositifs de vidéoprotection de la voie publique ou la collecte de données excessives lors de démarches administratives. La CNIL peut prononcer des sanctions administratives mais aussi des sanctions pénales.

Quant au RGPD, entré en vigueur en mai 2018, il encadre la gestion des données personnelles : cela concerne le nom et l'adresse (données nominatives) mais aussi les données indirectes (numéro de téléphone, numéro de plaque minéralogique, empreinte digitale, inscription cadastrale, demande de permis de construire, impôts, retraits à la médiathèque) ou rattachées, comme le nombre de repas de cantine facturés ou encore l'adresse IP utilisée pour se connecter au site de la commune[55]. La collectivité doit respecter cinq principes : finalité, proportionnalité, durée limitée de conservation des informations, sécurité et confidentialité des informations, respect des droits des personnes. Théoriquement, tout organisme traitant des données personnelles (et donc toutes les collectivités territoriales) doit désigner un délégué à la protection des données (DPO). La CNIL a publié en 2019 un guide sur le sujet à l'attention des différentes collectivités territoriales[56]. Il rappelle la démarche de mise en conformité, complémentaire (mais distincte) de celle proposée par l'ANSSI pour la sécurisation des systèmes informatiques.

Une faible prise de conscience

Les collectivités territoriales sont, sauf exception, peu sensibilisées à ces questions. Bien sûr, le niveau régional est présent et quasiment toutes les régions ont pris des initiatives en la matière : Occitanie[57], Hauts de France[58], Normandie[59], Ile de France[60], Bretagne[61], Nouvelle-Aquitaine[62], pour ne prendre que quelques exemples, ont engagé des actions en faveur de la cybersécurité.

Les départements peuvent également agir en la matière, même si ces actions paraissent plus isolées : ainsi de la Gironde[63] ou du Morbihan[64], seuls exemples que nous avons relevés.

Enfin, les agglomérations sont également intéressées : Rennes, où est implanté le Pôle d'excellence cyber et qui accueille la *European Cyber Week*, ou Lille, qui accueille chaque année le Forum international de Cybersécurité (FIC), sont évidemment sensibilisées. Mais des agglomérations comme Brest[65], Limoges[66] ou Lyon[67] ont pris des initiatives. Vannes se

[55] Voir C. Doutriaux, *Gestion du risque numérique et des données par les collectivités territoriales*, Chaire Saint-Cyr de cyberdéfense, février 2020, p. 6.
[56] CNIL, *Guide de sensibilisation au RGPD pour les collectivités territoriales*.
[57] « Occitanie, place forte de la cybersécurité », laregion.fr, 13 novembre 2019.
[58] « Un plan régional pour la cybersécurité », hautsdefrance.fr.
[59] https://www.normandie.fr/cybersecurite
[60] « Assises régionales de la cybersécurité », iledefrance.fr, 26 novembre 2018.
[61] « La Bretagne, terre de cybersécurité », bdi.fr.
[62] « Les Assises Régionales de la Cyber Sécurité », nouvelle-aquitaine.fr.
[63] « Cybersécurité, la Gironde contre-attaque ! », gironde.fr, 16 janvier 2020.
[64] « Le Morbihan, terre d'accueil des start-ups de cybersécurité », *Le Monde informatique*, 29 janvier 2020.
[65] « Brest bientôt centre national de cybersécurité maritime ? », brest.fr, 30 août 2019.
[66] « Limoges, pionnière de la cybersécurité en matière de santé », *Le populaire du Centre*, 29 novembre 2019.
[67] « Lyon crée le premier collectif en Europe dédié à la cybersécurité des systèmes industriels et urbains », economie.grandlyon.com, 9 février 2017.

distingue[68] avec le lancement d'un Cyberwest challenge[69] ou encore la création d'une chaire de cybersécurité des grands événements publics[70]. Pour la plupart, il s'agit de grandes villes même si une petite ville comme Malestroit (aire urbaine de 16 000 habitants), en Bretagne, publie un appel au renforcement des mesures de cybersécurité le 18 mars 2020[71].

Logiquement, ce tableau suggère que les villes moyennes ou petites, sans même parler du monde rural, sont les grandes absentes de ce paysage, sauf exceptions.

Des défis nouveaux

La révolution informatique dure depuis maintenant quatre décennies. Elle a connu plusieurs vagues : ordinateur personnel, accès à l'internet, écriture 2.0 (blogs), smartphone… Ces outils numériques ont profondément transformé nos vies, dans le champ personnel comme professionnel. L'adaptation (individuelle ou organique) est plus ou moins rapide et, surtout, synchronisée avec les évolutions techniques. Si toutes les collectivités territoriales disposent désormais de systèmes informatiques, beaucoup restent à la traîne sur les nouvelles évolutions à l'œuvre.

Aussi, la prise de conscience des enjeux de la cybersécurité doit s'inscrire dans un phénomène plus général : de même que nous ne vivons plus sans électricité ou voiture[72], nous ne vivrons plus sans internet et ses services associés. Là aussi, l'augmentation et la diversification des usages imposent des standards et des réglementations de plus en plus exigeants. On a ainsi imposé un permis de conduire qui s'est durci au fil du temps. On a de même mis en place un contrôle technique des véhicules ayant dépassé un certain âge. Ces mesures sont bien sûr contraignantes mais elles assurent une plus grande sécurité pour tous, sachant que simultanément, la circulation automobile n'a cessé d'augmenter. Il doit en être de même pour la cybersécurité.

Or, tout comme dans le cas du secteur automobile, de nouveaux changements sont déjà présents.

La crise de la Covid-19 a imposé à beaucoup de Français l'usage du télétravail ou de la communication à distance. Chacun se sert désormais de quatre ou cinq applications de vidéo conférence, connaissant les avantages et les inconvénients de chacune. Or, ce télétravail n'a la plupart du temps pas été préparé. Chacun a dû improviser – beaucoup de fonctionnaires territoriaux n'ayant pas d'accès sécurisé à leurs dossiers professionnels, l'immense majorité n'ayant même pas d'outil informatique portable… On a donc assisté à l'utilisation de moyens personnels (ce qu'on désigne par BYOD : *bring your own device*), ce qui a logiquement entraîné d'énormes failles dans la sécurité des communications professionnelles.
D'autres révolutions sont à l'œuvre : celle du stockage des données ; celle de l'utilisation à distance d'applications, appelée à passer de plus en plus par des systèmes d'infonuagique (*cloud*), qui permettront ultérieurement de travailler sur ces données en masse afin d'en tirer de

[68] « La région de Vannes en pointe dans le domaine de la cybersécurité », *Global Security Mag*, mars 2020.
[69] http://www.cyberwestchallenge.bzh/
[70] Chaire CGEP Cybersécurité des Grands Evènements Publics.
[71] « [Coronavirus/COVID-19] Appel au renforcement des mesures de vigilance cybersécurité », villedemalestroit.bzh, 18 mars 2020.
[72] Hors le cas des citadins qui peuvent se passer de voiture personnelle mais qui utilisent tout de même des transports en commun, dont certains fonctionnent avec des moteurs thermiques : l'usage se distingue alors de la propriété.

nouvelles informations (*datavisualition)*, puis de valoriser des données massives (*Big Data*), qui pourront, au-delà, être analysées par des intelligences artificielles à base d'apprentissage machine.

Une autre révolution touchera beaucoup plus directement les collectivités territoriales : celle des réseaux télécom de cinquième génération (5G), qui permettra le développement massif de l'internet des objets (*internet of things, IOT*). Déjà, ces objets connectés envahissent l'espace public – si l'on pense aux caméras publiques de surveillance. La plupart ont des protections numériques très faibles[73]. A titre d'exemple, en 2016, une gigantesque attaque par déni de service a causé d'énormes problèmes. Elle reposait sur des robots (botnet Mirai) qui utilisaient des caméras de vidéosurveillance à travers le monde pour qu'elles envoient des requêtes vers les serveurs ciblés, qui tombaient (sous la surcharge des demandes) les uns après les autres[74].

Or, la 5G, associée à l'internet des objets, est à la base des développements futurs de la ville intelligente (*smart city*). On imagine par exemple que demain, les véhicules seront tous connectés aux services de la ville et que les feux de signalisation réguleront automatiquement la circulation, au regard des données reçues et analysées. Imaginez qu'un pirate s'introduise dans le système et mette tous les feux au rouge : il s'ensuivrait un gigantesque embouteillage qui bloquerait même les services d'urgence (pompiers et ambulances) avec des morts à la clef. Or, il risque d'y avoir un creusement entre les collectivités territoriales, les plus grandes agglomérations pouvant passer à la « ville intelligente » et accroître ainsi leur compétitivité au niveau national, au détriment de la région environnante, qui sera numériquement handicapée.

Un investissement, plutôt qu'une assurance

Les collectivités territoriales doivent donc considérer la cybersécurité comme une priorité. Il s'agit, à court terme, d'éviter des sabotages et escroqueries qui entraveraient leur fonctionnement normal (rançonnage). Il faut également se mettre en conformité avec le RGPD et prendre conscience que les données manipulées constituent un trésor qu'il faut protéger mais aussi valoriser. Les collectivités territoriales doivent empêcher les escroqueries qui les ciblent, protéger leur réputation, garantir la confidentialité des informations de leurs collaborateurs et de leurs administrés : cette mission de sécurité du service public est première.

De même, il s'agit d'organiser la résilience de son administration par la mise en place régulière de plans de continuité d'activité mais aussi de dispositifs récurrents de télétravail. Au fond, les collectivités territoriales doivent organiser une résilience générale qui va au-delà des plans communaux de sauvegarde (PCS) : ceux-ci ne sont pas toujours dressés, pas toujours mis à jour ni testés, et ils s'intéressent le plus souvent à des catastrophes naturelles. La cybersécurité doit s'intégrer dans une démarche plus générale de résilience territoriale.

À terme, il s'agit d'envisager les risques qu'apportera la ville intelligente. Les collectivités territoriales peuvent ici se saisir des avancées futures pour renforcer leur développement économique et réduire la fracture territoriale et numérique qui existe aujourd'hui en France. Bien sûr, l'édile peut considérer cette dimension comme une contrainte ou une dépense. Autrement dit, un système d'assurance et de simple couverture du risque. Ce serait une erreur.

[73] Voir Eric Hazane, « Sécurité numérique des objets connectés, l'heure des choix », *Notes de la FRS*, n° 15/2018, 3 septembre 2018.
[74] « Bilan des attaques IOT en 2016 », *Digital Security*, 16 janvier 2017.

Il doit au contraire prendre le parti que c'est un investissement sur lequel il aura un retour, non seulement en fiabilisation de son administration et du service rendu aux administrés, mais aussi en termes de développement.

Tout d'abord, la cybersécurité fait partie, avec la connectivité, des demandes récurrentes des entreprises qui veulent s'installer sur un territoire : pas de développement économique aujourd'hui sans cybersécurité. Ensuite, la cybersécurité entraîne les administrations à porter un regard nouveau sur leur outil informatique et donc à conduire une transformation digitale qui permettra une plus grande efficacité et une plus grande satisfaction des employés et des administrés. Enfin, cela permet de prendre à bras le corps la transformation profonde occasionnée par la révolution informatique que nous connaissons. S'en saisir parmi les premiers permet d'influer sur la définition des règles et des standards plutôt que de les subir quand ils sont définis par d'autres.

Il ne s'agit bien sûr pas de faire cela tout seul, et chaque collectivité territoriale veillera à se rapprocher de ses voisines afin de « chasser en meute » : la mutualisation paraît à l'évidence une des premières réponses au défi posé. De même, réfléchir ensemble afin de trouver des réponses collectives, à chaque niveau adapté, paraît de bonne méthode. On peut espérer que dans ces conditions, la fracture numérique qui existe aujourd'hui entre les grandes métropoles et le reste du territoire sera progressivement réduite.

Les opinions exprimées ici n'engagent que la responsabilité de leur auteur.

W W W . F R S T R A T E G I E . O R G

4 BIS RUE DES PÂTURES 75016 PARIS TÉL : 01 43 13 77 77 FAX 01 43 13 77 78

ISSN : 2273-4643