

# VERS L'E-CITOYENNETÉ ET L'E-ADMINISTRATION : QUELS RISQUES POUR LES COLLECTIVITÉS ?



*Intervention de Monsieur Gérard Combe, Président de l'association PRIMO France, et de Monsieur Thomas Graiff, Responsable Secteur Public chez Marsh France, lors du 76<sup>ème</sup> Congrès du Syndicat National des Directeurs Généraux des Collectivités Territoriales.*

# INTRODUCTION

Le 14 octobre dernier, l'association PRIMO France<sup>1</sup> et le courtier en assurances Marsh<sup>2</sup>, étaient présents au 76<sup>ème</sup> Congrès du *Syndicat National des Directeurs Généraux des Collectivités Territoriales* à Antibes. Pendant l'atelier 16 « Vers de nouvelles pratiques : le citoyen, acteur du service public ? », modéré par Madame Fabienne Ihidope, DGS de la commune d'Hasparren, PRIMO et Marsh ont pu exposer aux directeurs présents les différentes manifestations du numérique dans les pratiques citoyennes ainsi que les enjeux des cyber-risques au sein des collectivités locales.

En introduction, M. Combe a rappelé les conclusions du premier rapport d'enquête réalisé par PRIMO France en 2015. Un réel manque de connaissance et de sensibilisation des collectivités et de leurs agents quant aux cyber-risques avait été observé quand bien même elles auraient mis en place une prévention renforcée (SSI, antivirus, firewall, cryptage...). En effet, 15% d'entre elles ont fait concevoir leur site par un agent, 10% ne connaissent pas la paternité de leur site, aucune des collectivités n'a recours au cryptage de données et 5% n'en connaissent pas l'existence. De plus, seulement 10% des sondés organisent des formations de sensibilisation pour leurs agents. Or, ces vigilances sont plus que d'actualité : les collectivités locales ont dû faire face à une augmentation significative des cyberattaques à leur rencontre, notamment lors des suites des attentats de 2015.

Toutefois, tout au long de l'année dernière, les échanges entre PRIMO et les responsables locaux ont été riches de discussions portant sur les cyber-risques des collectivités ; en effet, selon Gérard Combe, 2016 a apporté une vraie prise de conscience de l'importance de ce risque et de ses conséquences pour des collectivités locales.

Aujourd'hui, il apparaît nécessaire à PRIMO France d'approfondir le sujet en procédant bientôt à une seconde enquête auprès des collectivités territoriales. Le nouveau questionnaire permettra d'établir de manière plus précise la nature des données conservées par les collectivités territoriales mais également de déterminer le degré de digitalisation des services publics locaux.

---

<sup>1</sup> Association créée en 2005 dédiée à la gouvernance et à la gestion du risque dans le secteur public ayant pour vocation à informer, sensibiliser et aider les décideurs territoriaux dans le domaine de la gestion de risques.

<sup>2</sup> Leader mondial de la gestion des risques et du courtage en assurance

# LES NOUVELLES PRATIQUES DU CITOYEN : L'E-CITOYENNETE

## LES PLATEFORMES COLLABORATIVES

Ces initiatives mettent quotidiennement le citoyen à contribution puisqu'elles permettent de s'exprimer, échanger et débattre de manière participative, rapide et interactive sur de nombreux sujets (projets, évènements, consultations, votes). La masse d'informations et d'échanges étant importante, les interfaces proposées pour ces dialogues doivent donc subir des contrôles rigoureux et réguliers afin de ne ternir ni l'image de la ville, ni celle de ses élus.

## LES RESEAUX SOCIAUX

Le groupe Ideose, spécialisé dans l'étude et la formation aux réseaux sociaux nous apprend que 55% des villes-préfecture sont présentes sur Facebook et que 50% ont un compte Twitter. 68% des conseils généraux sont présents sur Facebook contre 50% sur Twitter, alors que 89% des conseils régionaux ont un compte Facebook, et 81% ont ouvert un compte Twitter. De plus, le baromètre Epiceum – Harris de la communication locale 2015 indique que quatre personnes sur dix consultent les pages officielles des collectivités.

Les comptes et profils des collectivités sur les réseaux sociaux sont par nature des lieux d'échange où les participants peuvent être nombreux ; de plus, il est aisé pour un hacker de cracker les identifiants et mots de passe et de prendre ainsi le contrôle du contenu de la page concernée.

## LA PARTICIPATION CITOYENNE AU PILOTAGE DU TERRITOIRE

La participation du citoyen au pilotage du territoire se matérialise généralement par la mise en place d'applications permettant de diffuser et recueillir des informations, tout en évaluant les besoins des citoyens en procédant à des tests grandeur nature. Par exemple, la Métropole de Rennes a pu, par le biais d'une application dédiée utilisant la géolocalisation de citoyens volontaires, étudier les pratiques de transports urbains dans un quartier mal desservi. Grâce aux résultats, elle a pu mieux évaluer les besoins et les parcours des usagers et ainsi envisager la création de nouvelles stations.

# LES NOUVELLES PRATIQUES DU CITOYEN : L'E-ADMINISTRATION ?

## L'ADMINISTRATION ELECTRONIQUE

L'administration électronique ou e-administration se veut être un moyen de simplification de l'organisation administrative et des relations avec les citoyens, en favorisant les échanges d'informations et de données. Ces nouveaux enjeux numériques imposés aux collectivités les propulsent dans un monde de données et de menaces auxquelles elles ne sont pas préparées et qui les exposent toujours plus.

La démarche d'administration électronique avait été initiée dès 2000 avec la création du portail [service-public.fr](http://service-public.fr). Cette dématérialisation du service public fut ensuite étoffée avec le lancement du plan ADELE pour aboutir en 2009 au portail [mon.service-public.fr](http://mon.service-public.fr), aujourd'hui fusionné avec [service-public.fr](http://service-public.fr).

La demande de digitalisation sans cesse croissante oblige les collectivités territoriales à créer des interfaces de procédures en ligne faciles d'utilisation et sécurisées lorsqu'elles deviennent transactionnelles, notamment pour les inscriptions ou règlements de factures.

## UNE DEMANDE CROISSANTE DES CITOYENS

Aujourd'hui, les citoyens tendent à se tourner – voire à demander – toujours plus de services en ligne de la part de leur collectivité. Daté de 2010, le *Livre blanc - Téléservices et collectivités* dresse un panorama des demandes les plus fréquentes des citoyens en matière de services en ligne. Les plus demandés concernent l'État civil (demandes de copie ou extrait d'acte), les demandes de certificat d'urbanisme, travaux sans permis de construire, la consultation du cadastre et l'accès au Système d'Information Géographique. On note également une demande forte concernant l'inscription à l'école, à la cantine, à la garderie ou encore quant à la vie culturelle (inscription à une bibliothèque-médiathèque, réservations) avec parfois paiement en ligne.

Cette demande croissante de rapidité et de simplification des démarches administratives concerne toutes les générations. On pense d'abord à la génération Y – qui a maîtrisé très jeune les outils informatiques, puis numériques et qui se tourne aujourd'hui tout naturellement vers les nouveaux objets connectés – puis la génération Z, née après 1995, qui a connu les technologies informatiques de communication depuis sa naissance. Pourtant, les seniors sont également pris dans le tourbillon de la digitalisation : selon le baromètre TNS-Sofres/Cogedim Club 55+ de 2016, 69% des plus de 55 ans possèdent un appareil connecté (ordinateur, tablette, smartphone...) et 33% d'entre eux déclarent faire leurs achats sur Internet.

## LES PERSPECTIVES NUMERIQUES

En février 2010, le rapport Riester, rédigé par le groupe « Experts Numériques » piloté par Franck Riester, exposait dix propositions afin d'améliorer les interactions entre administration publique et usagers. Le rapport préconise la possibilité de se connecter avec un même identifiant et mot de passe à tous les services de l'administration et la proposition d'un support d'authentification et de signature électronique est envisagée. La généralisation des fonctions de paiement dématérialisé et le développement des recours aux factures électroniques sont également recommandés. En outre, le groupe d'experts demande la mise en place d'un « bouquet minimum » pour les mairies, incluant l'inscription à la cantine, aux activités périscolaires, aux écoles et sur les listes électorales, ainsi que les paiements affiliés le cas échéant.

Par conséquent, les collectivités locales sont vouées à gérer un grand nombre de données personnelles et confidentielles, dont des données bancaires entraînant des risques qu'il est absolument nécessaire d'anticiper. La centralisation de ces données simplifie leur conservation mais les expose davantage au piratage. La collecte et la bonne gestion de données personnelles est donc au centre des politiques publiques ; les collectivités doivent à présent s'engager dans la sécurisation des réseaux et des *process*, afin d'optimiser leur gestion du cyber-risque.

Face à la multiplication des appareils connectés, l'évolution constante de la technologie et la place de plus en plus importante du numérique dans la vie politique, sociale et économique des collectivités locales, celles-ci se doivent d'offrir des solutions numériques agiles et adaptables pour répondre aux besoins et exigences des citoyens. Les enjeux majeurs des dirigeants sont donc de répondre efficacement à ces demandes, d'adapter les dispositifs en fonction du territoire concerné tout en étant capable d'identifier et d'anticiper l'ensemble des risques.

## LES CYBER-RISQUES

### LES COLLECTIVITES LOCALES : UNE CIBLE DE CHOIX POUR LES HACKERS.

La somme d'informations détenue par les collectivités est conséquente et concerne tous les niveaux de l'administration. Or, le piratage est au cœur des sujets puisque 42% des victimes déclarées à l'ANSSI en 2015 étaient des collectivités territoriales<sup>3</sup>. Ce chiffre alarmant doit être un signal fort pour les dirigeants locaux et le cyber-risque doit devenir une priorité pour les collectivités : lorsqu'une commune est touchée par une attaque ciblée, c'est l'Institution qui est visée.

---

<sup>3</sup> Chiffre donné par l'Agence Nationale de la Sécurité des Systèmes d'Informations (ANSSI)

L'enquête menée par PRIMO France en 2015 révélait les faiblesses des collectivités territoriales dans la bonne gestion et la protection des données personnelles. Pourtant, selon la législation et la documentation fournie par la CNIL, le maire ou le président de l'Établissement Public de Coopération Intercommunale est légalement responsable des fichiers et du traitement des informations de l'ensemble des données personnelles, confidentielles et de gestion collectées par son administration. Selon le décret n° 2010-112 portant Référentiel Général de Sécurité « RGS » (JO du 4 février 2010, p. 2072), lui-même reprenant le Code Pénal (Article 226-17 et Article 226-22), la responsabilité civile et pénale d'un dirigeant territorial ou d'un élu peut être engagée si toutes les mesures de prévention et de protection n'ont pas été prises. Le transfert vers l'assurance est donc un bon moyen d'être certain d'avoir pris toutes les mesures pour se prémunir également contre les conséquences d'une cyberattaque pour la collectivité.

## **LA COUVERTURE ASSURANTIELLE : UNE SOLUTION ADAPTEE AUX ENJEUX DU CYBER-RISQUE ET DES CYBERATTQUES.**

L'augmentation des impératifs numériques et les évolutions techniques présagent une accélération de la fréquence de ces attaques envers les collectivités, pouvant aller du défacement à la prise en otage de données. Ces attaques peuvent avoir une conséquence désastreuse sur la gestion interne des collectivités, le principe de continuité du service public et sur l'image de la collectivité elle-même et de ses élus.

Parce que le risque zéro n'existe pas, une protection visant à prendre en charge les conséquences des cyberattaques est absolument nécessaire. Que cela concerne une perte de données, l'attaque d'un service ou le non-respect de la charte de protection des données, la couverture assurantielle assure une assistance sur mesure avec l'intervention d'experts en sécurité informatique, en communication et gestion de crise ou encore d'un avocat spécialisé en cas de litige. D'autre part, elle propose des garanties d'indemnisations multiples (conséquences pécuniaires suite à des réclamations, des sanctions financières de la part des autorités, des frais de maintien du principe de continuité du service public...) ainsi que le rétablissement d'image et la reconstitution des données.

Ainsi couvertes, les collectivités pourront efficacement faire face aux nombreux impératifs qui leur incombent à la suite d'une cyberattaque, que ceux-ci soient financiers ou relevant de la notification, communication ou de la gestion de crise. Par ailleurs, cette ultime barrière sera le signe que les responsables locaux ont mis en œuvre tous les moyens possibles pour atténuer le cyber-risque et ses conséquences, répondant ainsi à leurs obligations de protection rappelées dans les différents codes et textes de loi.