

# Sécurité globale

N° 3-4, nouvelle série [N° 29-30 de la série originale]

## DIRECTEUR DE LA PUBLICATION

Serge KEBABTCHIEFF, Editions ESKA, Paris

### CONCEPTION ET RÉALISATION NOUVELLE SÉRIE

Charles-Louis FAVILLIER et Xavier RAUFER

## COMITÉ DE RÉDACTION

Alain BAUER, Professeur de criminologie au CNAM  
Hervé BOULLANGER, Magistrat à la Cour des Comptes  
Eric DANON, Directeur général du Conseil Supérieur de la Formation et de la Recherche Stratégique  
Julien DUFOUR, Commissaire de Police, criminologue  
François FARCY, Directeur judiciaire, Police fédérale belge  
Charles-Louis FAVILLIER, Criminologue, analyste en intelligence économique et stratégique dans l'industrie.  
Rémy FEVRIER, Maître de conférences au CNAM - Lieut.-colonel (réserve) de la Gendarmerie nationale  
Michel GANDILHON, Observatoire français des drogues et toxicomanies  
Jean-François GAYRAUD, Commissaire divisionnaire de la Police nationale  
Sylvain GOUGUENHEIM, Professeur des Universités, historien  
Abdelfettah KABBSSI, Capitaine de Police, Renseignement territorial  
Arnaud KALIKA, Expert et analyste du monde russe et ex-soviétique, Asie centrale, etc.  
Philippe LAVAULT, Ministère de la Défense  
Dominique LEBLEUX, Sociologue, ingénieur d'études à l'EHESS et criminologue  
Doron LEVY, Criminologue, consultant, expert  
Stéphane QUÉRÉ, Ecrivain, expert, dirige le *Bulletin hebdomadaire d'informations criminelles*  
Mickaël ROUDAUT, Administrateur à la direction générale pour les affaires intérieures de la Commission européenne  
Jacques de SAINT-VICTOR, Professeur des Universités, CNAM  
Lauriane SICK, Consultante, lutte contre le blanchiment de capitaux et financement du terrorisme auprès de grandes institutions financières, master en criminologie  
François TRICHET, Capitaine, Gendarmerie nationale, expert ès-sectes  
Christian VALLAR, Doyen de la Faculté de Droit et de Sciences politiques de Nice  
Camille VERLEUW, Expert de l'islam radical, notamment chiite  
Gen. Marc WATIN-AUGOUARD, Directeur du Centre de recherches de l'Ecole des officiers de la Gendarmerie nationale

## Sécurité globale

Editions ESKA  
12, rue du Quatre-Septembre – 75002 Paris  
Tél. : 01 42 86 55 65 – Fax : 01 42 60 45 35  
Site : [www.eska.fr](http://www.eska.fr)

## RECOMMANDATIONS AUX AUTEURS

Le comité de rédaction de la revue est ouvert à toute proposition d'article.

Les auteurs sont priés de respecter les lignes directrices suivantes quand ils préparent leurs tapuscrits :

- ✓ Les articles ne doivent pas dépasser 40 000 signes (notes et espaces comprises).
- ✓ Les articles doivent être inédits. Si justifié par un intérêt éditorial précis, la rédaction accepte néanmoins les versions longues et étayées d'articles préalablement parus.
- ✓ Deux résumés, l'un en français, d'une dizaine de lignes maximum et un autre, en anglais, de la même importance, doivent être fournis avec le manuscrit, accompagnés de la qualité et la liste des dernières publications de l'auteur.
- ✓ Une bibliographie sommaire peut éventuellement être jointe aux articles.
- ✓ Les auteurs feront parvenir leur article par Internet à l'adresse suivante : agpaedit@wanadoo.fr en format MS Word (.doc ou .rtf) ; Times New Roman 11 justifié, interlignes simples.
- ✓ Les auteurs doivent joindre dans un fichier séparé portant mention de l'ensemble de leurs contacts : courriel, adresse postale et le cas échéant numéro de téléphone.
- ✓ L'article doit être présenté de la manière suivante : titre en Times 14, suivi, à chaque fois à la ligne, du prénom et du nom de l'auteur, de sa qualité (notice biographique), du résumé français/anglais et du corps du texte.
- ✓ Les auteurs sont invités à structurer leurs analyses par intertitres afin de faciliter la lecture.
- ✓ Lors de la remise de l'article à la rédaction les fichiers Word doivent être titrés de la façon suivante : NOM (de l'auteur en majuscules) – titre (de l'article en minuscules)
- ✓ Tous les tableaux, graphiques, diagrammes et cartes doivent porter un titre et être numérotés en conséquence et sourcés s'ils ne constituent une œuvre originale. Toutes les figures doivent être transmises séparément en fichiers jpeg ou pdf d'une résolution suffisante (idéal 300 dpi) et leurs emplacements doivent être clairement indiqués dans le texte.
- ✓ Réduire au minimum le nombre de notes, et les placer en notes de fin selon le système de référencement Word.
- ✓ Tous les textes qui ne correspondent pas aux critères linguistiques standards et aux exigences de rigueur critique seront renvoyés aux auteurs pour adaptation.
- ✓ Une attention particulière devra être portée à la ponctuation : guillemets français, majuscules accentuées (État, À partir de, Égypte, etc.) et à un usage modéré des majuscules conformément aux règles typographiques.

Référence : Collectif, *Lexique des règles typographiques en usage à l'imprimerie nationale*, Imprimerie Nationale, Paris, 2002.

*Les articles signés expriment la seule opinion de l'auteur  
et ne sauraient engager la responsabilité de la revue.*

*Tous droits de traduction, d'adaptation et de reproduction par tous procédés réservés pour tous pays.*

La loi du 11 mars 1957, n'autorisant aux termes des alinéas 2 et 3 de l'article 41, d'une part, que des copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective et, d'autre part, que les analyses et courtes citations dans un but d'exemple et d'illustrations, « toute représentation ou reproduction intégrale, ou partielle, faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause, est illicite » (alinéa 1<sup>er</sup> de l'art. 40).

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles 425 et suivants du Code pénal.

Il est interdit de reproduire intégralement ou partiellement le présent ouvrage sans autorisation de l'éditeur ou du Centre Français de Copyright, 6 bis, rue Gabriel Laumain, 75010 PARIS.

**Sécurité Globale | N°3-4, nouvelle série | N°29-30, série originale**  
**Revue trimestrielle | © Editions ESKA**

ISSN : 1959-6782 • ISBN : 978-2-7472-2563-2 • CPPAP : 0916 K 90246

*Imprimé en France*



# Sommaire

## N°3-4, Nouvelle série, 2015

|  |    |
|--|----|
| RÉMY FÉVRIER - <i>Introduction</i>   | 5  |
| RÉMY FÉVRIER - <i>Toujours plus cyber-menacées : les collectivités territoriales</i>   | 11 |
| 1. Spécificités des SI des collectivités territoriales                                 | 11 |
| 2. Les collectivités face aux menaces numériques                                       | 30 |
| 3. Les 3 défis numériques des collectivités territoriales                              | 42 |
| XAVIER RAUFER - « <i>Police prédictive</i> » : les belles histoires de l'Oncle Predpol | 97 |

*Bulletin d'abonnement ou de réabonnement, page 94*





# Introduction

Rémy FÉVRIER

*Docteur en sciences de gestion et Maître de conférences au CNAM ou il dirige les unités d'enseignement « Management et Audit des Systèmes d'Information ». Ancien officier supérieur de Gendarmerie expert en Intelligence Economique et Sécurité des Systèmes d'Information, il est le concepteur du MBA « Management de la Sécurité » de l'Ecole des Officiers de la Gendarmerie Nationale. Intervenant régulièrement auprès de dirigeants publics et privés, il est également Maître de conférences à ESCP Europe et professeur-Affilié à l'EM Normandie en Intelligence Economique et gestion des risques numériques.*

5

Si chaque jour apporte de nouveaux exemples de cyber-menaces pesant désormais sur l'ensemble des organisations publiques ou privées, force est de constater que le traitement médiatiques de ces dernières se milite le plus souvent à la mise en exergue d'affaires emblématiques liées à un piratage d'origine étatique (affaire Snowden...) ou d'attaques numériques touchant des entités particulièrement symboliques (TV5 Monde, Ministère des Finances...). Or, ces quelques cas spécifiques ne doivent pas occulter le fait que de nombreuses autres menaces numériques existent et notamment celles visant des collectivités territoriales peu conscientes des risques numériques qui pèsent dorénavant sur elles.

Notre réflexion sur cette importante perspective provient de notre thèse de doctorat consacrée au management de la Sécurité des Systèmes d'Information (SSI) des collectivités territoriales françaises. Les résultats de cette étude – la seule réalisée à ce jour sur ce sujet spécifique – sont sans appel : la très grande majorité des élus locaux n'ont toujours pas pris la mesure des menaces numériques, alors même qu'à la suite des attentats de janvier 2015, plusieurs centaines de sites Web de collectivités territoriales ont fait l'objet d'un défaçage. Le ciblage de ces dernières s'explique à la fois par leur importance au sein de la communauté nationale, ainsi que du fait des défis numériques auxquels elles sont dorénavant confrontées et qui



## Rémy FÉVRIER

constituent autant d'opportunités pour des cyberpirates cherchant à maximiser l'impact sociétal de leurs attaques.

En effet, parties prenantes des évolutions de la société dans son ensemble et de l'environnement économique. Le fait qu'elles soient constituées d'individus issus de toutes les classes d'âges et de tous les milieux, en font de parfaites vigies des mutations économiques et sociétales. Les élus locaux étant devenus les dépositaires d'attentes souvent divergentes – voire antagonistes – ils demeurent, plus que jamais, les garants de l'intérêt général, ce qui les constraint à une quasi-obligation de résultat, relativement à un impératif de développement harmonieux du territoire dont ils ont la charge. Or, depuis une dizaine d'années, ces territoires sont soumis à des mutations sans précédent sous l'influence conjuguée d'évolutions sociétales majeures et de restrictions budgétaires dont l'impact simultané obligent les élus locaux à revoir en profondeur leurs processus de management ainsi que leur approche de l'environnement extérieur.

La recherche d'une nouvelle rationalité territoriale, illustrée par une gestion plus dynamique et prospective des ressources humaines et financières de la collectivité, ne constitue, néanmoins, qu'une étape dans le processus de prise en compte d'une nouvelle réalité. Les nouvelles technologies ont profondément modifié la définition et le champ de la citoyenneté, tout en induisant des changements majeurs dans l'exer-

cice des responsabilités électives. L'appropriation, par les collectivités territoriales, de l'ensemble des opportunités offertes par les Technologies de l'Information et de la Communication (TIC), s'impose donc aujourd'hui comme un impératif absolu, que ce soit en tant que vecteur communicationnel extérieur ou comme axe organisationnel stratégique.

Cependant, la prise en compte des TIC par les collectivités territoriales ne constitue pas uniquement un choix raisonné, fondé sur la volonté de dialoguer avec l'environnement extérieur et les administrés ou d'améliorer leur gestion interne : plusieurs impératifs s'imposent à elles en termes de mise en place et d'utilisation de nouveaux vecteurs de communication. Sous la pression conjointe d'un continuum gouvernemental soucieux d'améliorer la qualité des prestations rendues aux citoyens et de renforcer les liens entre les acteurs économiques locaux et d'instances européennes privilégiant les TIC pour améliorer la démocratie participative, les collectivités territoriales sont dorénavant amenées à relever trois défis numériques majeurs face auxquels elles paraissent souvent démunies : l'administration électronique, l'e-démocratie et la dématérialisation des appels d'offre.

Le but affiché de l'administration électronique étant de resserrer les liens entre administration et usagers, tout en modernisant le fonctionnement de l'État, celle-ci va de pair avec une certaine simplification



## Introduction

administrative et la mise en place de télé-services et de téléprocédures. Internet se retrouve, de fait, au centre de la construction d'une administration résolument tournée vers les besoins et les attentes des citoyens, que ce soit en matière de diversification de l'offre, de réactivité, de simplicité ou de suppression des files d'attente. Il en résulte que les collectivités territoriales – au nom du vaste ensemble de prestations dont elles ont la charge directe – se retrouvent être concernées, au premier chef, par ce nouveau type de relations virtuelles avec les administrés.

Souvent considéré par ses partisans comme un nouveau vecteur de citoyenneté, de nature à renouer les fils d'un dialogue devenu peu à peu déficient entre les élus et leurs administrés, le concept d'e-démocratie constitue un second défi à relever pour les collectivités territoriales. Le succès d'Internet et des réseaux sociaux, conjugué à une hausse globale du niveau d'instruction des individus, a conduit un certain nombre d'organisations internationales, au premier rang desquelles les instances européennes, à encourager fortement une déclinaison locale de ce nouveau mode de dialogue démocratique. Les collectivités territoriales françaises n'échappent pas à cette tendance. Cela nécessite d'élaborer de nouveaux circuits informationnels dont la mise en place s'avère le plus souvent coûteuse mais également d'avoir recours à des technologies et processus organisationnels encore mal maîtrisés.

Le citoyen ne constitue toutefois pas l'unique cible de ce renouveau territorial : les relations avec le secteur économique privé font également l'objet de toutes les attentions des pouvoirs publics, à travers la volonté de procéder à une dématérialisation de plus en plus poussée des appels d'offre. Bien que les collectivités territoriales soient régulièrement amenées à faire appel au secteur privé, afin de disposer des biens et services adaptés aux missions qui leur sont dévolues, les relations commerciales qui en résultent sont régies par des textes extrêmement précis, dont la complexité décourage de nombreuses PME (Petites et Moyennes Entreprises) qui ne disposent pas nécessairement des ressources indispensables leur permettant de se positionner sur le marché de la commande publique locale. Dans le cadre de la modernisation de l'État et dans un souci global de simplification des procédures, les pouvoirs publics ont décidé d'imposer aux collectivités territoriales un recours accru à des procédures dématérialisées. Ceci afin de réduire les coûts de traitements des propositions commerciales, tout en favorisant la concurrence entre soumissionnaires. Elles sont ainsi confrontées à la nécessité de transformer leurs anciennes procédures internes afin de les faire évoluer vers un traitement exclusivement informatisé des dossiers, ce qui ne manque pas de poser de graves problèmes financiers et d'organisation interne, *a fortiori* pour les collectivités de taille modeste.

Cette utilisation chaque jour plus étendue des Systèmes d'Information (SI) par



## Rémy FÉVRIER

8

les collectivités territoriales conduit assez naturellement à s'interroger sur le niveau de prise en compte du risque numérique par les collectivités territoriales : comment assurent-elles la sécurité des données numériques qui leur sont ainsi confiées et dont le traitement constitue dorénavant une part prépondérante de leur activité quotidienne ? Connaissent-elles vraiment l'ensemble des risques auxquels leurs SI sont confrontés ? Les dirigeants territoriaux ont-ils conscience de leur qualité de responsables de traitements et des implications qui en découlent en matière de SSI ? Eu égard à l'importance des collectivités territoriales dans l'organisation administrative française, de leur poids économique et de leur rôle de plus en plus grand en matière de valorisation économique et d'aménagement du territoire, la question de la sécurisation de leurs SI paraît d'autant plus pertinente.

Essayant inlassablement d'alerter les pouvoirs publics territoriaux sur les effets induits par des cyberattaques, nous espérons que ce texte sera de nature à susciter l'intérêt de certains élus locaux et fonctionnaires territoriaux ayant à cœur de protéger les données dont leurs collectivités sont dépositaires. Ces dernières sont aujourd'hui essentiellement confrontées à des attaques de niveau 1 (défaçage de site, attaques par déni de services...), mais il nous semble évident qu'à l'avenir, les menaces évolueront vers des vols de données à caractère personnel, la prise de contrôle de faisceaux sans-fil, voire des attaques visant les SI industriels situés sur le territoire de la collectivité cible : signalisation routière, station d'épuration des eaux usées... Il apparaît donc urgent de prendre la mesure réelle de la menace et de protéger les SI des collectivités territoriales, ainsi que de sensibiliser l'ensemble de leurs agents aux nouvelles menaces numériques.



# Dossier | Toujours plus cyber-menacées : les collectivités territoriales

*Rémy FÉVRIER*







# Toujours plus cyber-menacées : les collectivités territoriales

Rémy FÉVRIER

11

Un phénomène totalement nouveau est récemment apparu : l'intrusion dans les systèmes d'information (ci-après SI) des collectivités territoriales. S'il s'avère extrêmement difficile de disposer de données quantitatives à ce sujet, du fait de la prudence compréhensible dont ces dernières font preuve, de plus en plus d'attaques deviennent néanmoins publiques, notamment du fait de l'appétence de journalistes plus sensibilisés à ce genre de menaces. Sans remonter outre mesure dans le temps, force est de constater que les atteintes aux SI n'épargnent plus les collectivités territoriales, que ce soit en France ou à l'étranger. Là encore, le caractère mondialisé des menaces apparaît clairement, non pas né-

cessairement en termes de périmètres d'attaque, mais de ciblage commun.

## 1. Spécificités des SI des collectivités territoriales

À mesure que les collectivités territoriales se sont vues attribuer des compétences et responsabilités supplémentaires, leurs SI ont fait l'objet d'une sollicitation de plus en plus poussée afin de traiter les quantités de données induites par ces nouvelles missions. Si les SI des collectivités territoriales ont à gérer une multiplicité d'informations dans des délais de plus en



## Rémy FÉVRIER

plus restreints, l'importance qui leur est faite dans la stratégie de l'organisation demeure encore trop souvent exclusivement corrélée à une vision strictement utilitariste. En dépit des services rendus et de l'importance toujours croissante prise par les SI, le caractère stratégique de ces derniers peine toujours à émerger dans de nombreuses collectivités territoriales.

### Un champ d'étude inexploré : la SSI des collectivités territoriales

Les études menées dans le domaine des SI montrent que les situations sont extrêmement contrastées et varient fortement d'une entité à l'autre : s'il est aujourd'hui acquis que les SI contribuent à l'efficience des organisations, il existe néanmoins de grandes disparités entre ces dernières relativement à leur prise en compte et cela est encore plus vrai dans le cas des collectivités territoriales. Le rôle stratégique des SI et leur apport en matière de traitement de l'information et de service rendu aux administrés est encore, dans certains cas, sujet à caution ou du moins largement sous-estimé, ce qui n'est pas sans conséquence sur leur sécurisation. Confrontées à de nombreux défis qui s'imposent à elles, les collectivités territoriales doivent prendre en compte la problématique de la SSI mais cette évolution est lente et pose le problème de la protection des données qui leur sont confiées. Afin de mieux cerner cette réalité, il apparaît indispensable de retracer rapidement l'histoire d'une informatisation des collectivités territoriales empreinte de mé-

fiance et qui constitue un champ de recherche encore largement inexploré.

#### • *Un cas exceptionnel de regroupement de données à caractère personnel*

Une des particularités des collectivités territoriales réside dans la large diversité de leurs champs d'intervention respectifs. Les responsabilités qui leur incombent nécessitent de gérer toujours plus de fichiers informatisés comportant des informations personnelles sur les administrés.

Le premier écueil auquel se heurte une collectivité réside dans leur caractère hétérogène et les obligations légales à respecter relativement à ces traitements. L'aspect juridique lié à l'utilisation de ces fichiers fera l'objet d'une partie spécifique. Dans un premier temps, nous chercherons à mettre en évidence deux aspects simultanés des Systèmes de Traitements Automatisés de Données (STAD) mis en place par les collectivités territoriales : leur nombre croissant et la complexité inhérente à leur utilisation et leur sécurité.

Plusieurs catégories de fichiers cohabitent et leur amoncellement nécessite simultanément un compartimentage rigoureux des flux de données ainsi qu'une parfaite étanchéité entre ceux-ci. Cette exigence est rendue d'autant plus indispensable que, dans la plupart des cas, ces traitements contiennent des données à caractère personnel relatifs aux fonctionnaires eux-mêmes (traitements de gestion interne) ou



## *Toujours plus cyber-menacées : les collectivités territoriales*

aux administrés (traitements administratifs et sociaux). L'évolution probable de la société vers toujours plus de dématérialisation des actes administratifs et des services rendus au public n'est pas sans conséquence sur la sécurisation des réseaux informatiques, de par le développement croissant de la cybercriminalité et l'aspect emblématique des collectivités territoriales : assurant à la fois un double rôle administratif et politique, ces dernières deviennent, de plus en plus, des cibles de choix pour les pirates informatiques comme le montrent certaines tentatives récentes.

Face à cette menace, les dirigeants territoriaux se doivent, préalablement à toute action de sécurisation, d'avoir une vision claire de l'ensemble des traitements qui relèvent de leur compétence et, au final, de leur responsabilité.

### Traitements de données à caractère personnel d'origine interne

La notion de donnée à caractère personnel est devenue, au fil du temps, un des concepts clés liés à la législation des TIC.

### Traitements de gestion quotidienne

Suivant en cela l'évolution de la société vers une intégration toujours plus grande des technologies numériques dans la vie courante des individus et, plus largement, des sociétés modernes dans leur ensemble, les possibilités offertes par les SI ont généralement permis d'optimiser les tâches

de collecte, de traitement et de stockage de l'information, jusqu'à être dorénavant considérées, dans le cas d'une entreprise, comme une source d'avantage concurrentiel indirect. Les collectivités territoriales, adoptant de plus en plus des règles de gestion et de management issu du secteur privé ne font pas exception et le phénomène d'informatisation a permis à celles-ci d'acquérir souplesse et réactivité dans le traitement de leurs données d'origine interne et externe.

À l'instar de n'importe quel chef d'entreprise ou directeur d'administration centrale, les responsables d'exécutifs locaux se doivent de disposer d'une structure efficace et apte à assurer les missions qui lui ont été confiées dans les meilleures conditions possible, en termes de service rendu. Encore faut-il, pour ce faire, disposer d'une administration moderne et bénéficiant des dernières évolutions techniques. À ce titre, la plupart des collectivités territoriales ont, par exemple, informatisé leurs traitements internes relatifs à la Gestion des Ressources Humaines et à la gestion de la paie. Une vigilance toute particulière doit néanmoins être apportée à leur sécurisation étant donné le caractère confidentiel des enregistrements.

### Principes fondamentaux à respecter

Ces traitements à vocation interne, en tant que contenant des données à caractère personnel sont, par essence, soumis au respect de cinq principes fondamentaux :



## Rémy FÉVRIER

### Le Principe de finalité

Les données à caractère personnel ne peuvent être recueillies et traitées que pour un usage déterminé et légitime, correspondant aux missions de la collectivité responsable du traitement.

### Le principe de proportionnalité

Seules doivent être enregistrées les informations pertinentes et nécessaires à la gestion des services de la collectivité.

### Le principe de durée de conservation des données

Les informations ne devant être perpétuellement conservées dans les fichiers, une durée de conservation doit être établie en fonction de la finalité du traitement.

### Le principe du respect du droit des personnes

Lorsque des informations sont recueillies, qu'elles soient d'origine interne ou en provenance des administrés, les usagers ou le personnel de l'organisme doivent être informés de la finalité du traitement ainsi que des modalités d'accès à fin de rectification.

### Le droit d'opposition

En cas de motif légitime, toute personne a le droit de s'opposer à ce que des données la concernant soient enregistrées dans un fichier informatique.

14

Parallèlement à ces fichiers internes, la grande majorité des données faisant l'objet d'un traitement de la part d'une collectivité territoriale met en jeu des informations de sources extérieures, au premier rang desquelles les citoyens.

### Traitements de données à caractère personnel d'origine externe

Suivant en cela l'évolution des services proposés aux administrés, le nombre de traitements spécifiques s'accroît régulièrement. Afin d'illustrer ce propos, nous mettrons plus spécifiquement l'accent sur l'échelon communal en tant que constitutif de l'exemple le plus emblématique de cette tendance<sup>1</sup>. Sans prétendre à l'exhaustivité, les exemples de traitements énoncés permettront d'illustrer leur large diversité.

### A finalité administrative

Les fichiers d'informations administratives représentent la première catégorie de traitement que doit gérer une collectivité territoriale.

L'état civil : la tenue des actes d'état-civil constituant une obligation pour les Maires, les services concernés, fortement informatisés, rédigent les actes, assurent le suivi des registres, la copie des actes à destination des administrés, ainsi que la transmission des informations à destination des diverses administrations concernées. L'ensemble des données ainsi



## *Toujours plus cyber-menacées : les collectivités territoriales*

collectées et traitées ne doit être utilisé que dans le cadre des missions spécifiquement dévolues aux Maires en leur qualité d'officier d'état-civil et ne peut, en aucun cas, être communiqué à des tiers non habilités.

Les listes électorales : conformément au code électoral, le Maire est responsable de la tenue, de la gestion et de la révision annuelle de la liste électorale de sa commune. Au-delà de son objectif initial de maintenir à jour la liste des électeurs, ce fichier peut également faire l'objet d'une diffusion, dans des cas prévus par la loi, auprès de tout électeur, candidat potentiel ou parti politique. Des tris spécifiques sont autorisés mais seulement sur des critères précis comme l'âge ou l'adresse des électeurs mais en aucun cas sur des critères susceptibles de faire apparaître les origines raciales, ethniques ou les appartenances religieuses.

Les fichiers fiscaux : les collectivités territoriales et leurs groupements reçoivent chaque année des fichiers concernant les impôts locaux de leurs administrés. Le Maire (ou le Président de l'EPCI) doit prendre toute disposition pour empêcher l'utilisation détournée ou frauduleuse des supports transmis à cet effet. Il doit également mettre en œuvre toute mesure utile afin d'assurer la sécurité et la pérennité de ces enregistrements. Ces fichiers peuvent être légitimement considérés comme faisant partie des plus « sensibles » détenus par une collectivité. À ce titre, il convient d'accorder une attention

particulière en matière de sécurisation des données.

Les Systèmes d'Informations Géographiques (SIG) : le fichier du cadastre recense, en les décrivant, les propriétés foncières de la commune et en donne une évaluation utilisée en matière fiscale. Chaque commune disposant de son propre fichier cadastral, de plus en plus d'EPCI et de conseils généraux centralisent ceux-ci, afin de mettre en place des SIG intercommunaux ou départementaux.

Les fichiers cadastraux demeurent un outil extrêmement précieux de cartographie territoriale et d'urbanisme, leur utilisation doit faire l'objet de précautions particulières puisque, en plus d'informations techniques relatives à la localisation de parcelles, ces SIG regroupent également des données à caractère personnel sur leurs propriétaires. L'aspect intercommunal éventuel de ce système nécessite une identification fine des postes de travail disposant de droits d'accès. Cette problématique de sécurité est rendue d'autant plus indispensable que l'aménagement devient l'un des principaux leviers de valorisation économique territoriale.

Le recensement : les communes et EPCI ayant en charge les enquêtes de recensement, un traitement informatique spécifique doit être mis en place aux fins de collecte et de consolidation des données, sous forme d'un contrôle de l'exhaustivité de la collecte. Afin de mener à bien cette



## Rémy FÉVRIER

mission déléguée par l'État, le plus simple consiste en l'utilisation du fichier de la taxe d'habitation transmis par l'Institut National de la Statistique et des Études Économiques (INSEE) et la Direction Générale des Impôts (DGI). Parallèlement à cette obligation légale de collecte, l'accès des collectivités territoriales à une importante partie des informations recueillies constitue également une opportunité majeure en ce qui concerne la mise en place d'un plan stratégique de valorisation territoriale

16

Le contrôle de légalité : le Code Général des Collectivités Territoriales (CGCT) a récemment évolué et prévoit dorénavant la possibilité de transmission électronique de l'ensemble des actes soumis au contrôle de légalité, depuis la collectivité vers le représentant de l'État<sup>2</sup>. Cette évolution permet de s'affranchir de transferts de documents lourds et fastidieux. Toutefois, cela doit s'accompagner de la mise en place d'une véritable procédure de télétransmission de nature à permettre une sécurité optimale des données transmises.

Les fichiers de communication : si les communes souhaitent connaître, à bon droit, leurs administrés, la mise en place de fichiers de communication nécessite de prendre un certain nombre de précautions particulières car ils peuvent faire, a priori, l'objet d'interrogations quant à la nature de leur utilisation finale (propagande). Ainsi, seules les données relatives à l'identité, la date et année de naissance ainsi

que l'adresse peuvent être renseignées voire l'appartenance à une association subventionnée par exemple. Cependant, dans le cas d'un fichier à des fins de communication municipale, la collecte des données ne revêt en aucun cas un caractère obligatoire et l'administré doit impérativement être informé du traitement et peut, si tel est son désir, demander à ne pas figurer dans ce fichier. Le même principe prévaut en cas d'utilisation d'un fichier de ce type à des fins d'alerte (risques naturels, chimique....) mais la Commission Nationale de l'Informatique et des Libertés (CNIL) recommande alors de constituer ce dernier directement par téléphone auprès des habitants afin de contrôler le caractère valide et actuel des éléments recueillis.

Parallèlement à ces traitements administratifs, une large part de l'action communale étant dédiée à l'action sociale, de nombreux fichiers sociaux ont corrélativement vu le jour, afin de gérer au mieux les mesures à destination des différentes catégories d'administrés.

### A finalité sociale

Au fil du temps, même si l'action sociale à destination des citoyens s'est progressivement étendue aux conseils généraux et régionaux, les communes restent, aujourd'hui encore, des acteurs majeurs en matière de prestations sociales.

Les services aux administrés : parmi les nombreuses prestations assurées par les



## *Toujours plus cyber-menacées : les collectivités territoriales*

municipalités à destinations du public, figurent la gestion des crèches, des garderies, des écoles maternelles et élémentaires ainsi que les activités sportives et de loisirs pour les enfants. Au fil du temps, ces prestations furent parmi les premières à bénéficier de la mise en place de systèmes informatisés de traitement, qui prennent le plus souvent la forme de systèmes de badges individualisés. Le succès remarquable rencontré par cette automatisation nécessite néanmoins une attention toute particulière dans sa mise en place, étant donné l'ensemble des données relatives à chaque famille qui préside au calcul du quotient familial : niveau de rémunération des parents, taux d'imposition etc. Les données ainsi collectées figurant parmi les plus « sensibles » et personnelles dans l'esprit du public, tout dysfonctionnement en termes de sécurisation de celles-ci provoquerait immanquablement, sans préjuger de l'éventuelle mise en cause de la collectivité devant la justice, une suspicion de manquement à l'obligation de sécurité des traitements.

Les centres communaux d'action sociale : le Centre Communal d'Action Sociale (CCAS) constitue l'organisme de gestion de nombreuses prestations à caractère social et supervise l'attribution des diverses aides spécifiques en direction des populations les plus fragiles. Ce rôle s'accompagne d'une obligation de vérifier l'identité et la situation des demandeurs au regard des critères d'éligibilité de ces participations financières. À ce titre, les

CCAS sont fondés, entre autres, à collationner des informations correspondant à la situation familiale, professionnelle, voire financière des demandeurs. La nature des informations recueillies engage les municipalités à une grande prudence dans la manipulation des données et leur transmission à des organismes extérieurs, dont la liste exhaustive figure précisément dans les différents textes encadrant les dispositifs de distribution.

Les demandeurs d'emplois : les collectivités territoriales s'étant depuis longtemps engagées dans la lutte contre le chômage, ces dernières peuvent recevoir des offres d'emploi à destination de leurs administrés respectifs et contribuer à leur diffusion auprès de ces derniers. À ce titre, les Maires peuvent demander à être destinataires de la liste des demandeurs d'emploi domiciliés dans leur commune. Par extension, il est admis qu'en cas de plan social ou de liquidation d'une entreprise située sur le territoire communal, les Maires puissent être destinataires de la liste des administrés potentiellement concernés, sous réserve de l'acceptation préalable de ces derniers. Les collectivités font généralement preuve d'un réel volontarisme en matière d'accompagnement des demandeurs d'emploi ce qui est tout à fait admirable et contribue fortement à la préservation du lien social. Pour autant, il convient de demeurer extrêmement vigilant sur la qualité et la sécurité du traitement des informations personnelles relatives à une population le plus souvent





## Rémy FÉVRIER

18

fragilisée, a fortiori dans le cas d'un chômage de longue durée.

Les logements vacants : le manque de logements disponibles rentre également dans le champ d'action des collectivités : la loi prévoit que l'administration fiscale puisse fournir aux communes, départements et EPCI à fiscalité propre, les fichiers dont elles disposent aux fins d'établissement de la taxe d'habitation, pour leur permettre d'établir la liste des logements vacants dépendant de leur responsabilité respective. Ce fichier ayant pour but de contacter les propriétaires de logements disponibles, ceux-ci peuvent faire l'objet de mailings ciblés visant à les informer sur les aides octroyées pour la réhabilitation de leurs biens et leur remise sur le marché locatif.

Les associations subventionnées : le tissu associatif français étant d'une grande richesse, de nombreuses associations reçoivent des subventions des pouvoirs publics locaux au titre de leur activité sociale, sportive ou culturelle. Du fait du caractère public des aides octroyées, ces dernières sont tenues de transmettre aux collectivités qui les soutiennent l'ensemble des documents disponibles relatifs à leur gestion et plus largement à leurs activités. Des statistiques de provenance géographique des adhérents ainsi que leur nombre peuvent faire l'objet d'une transmission, mais celles-ci doivent obligatoirement exclure toute information nominative sur leur identité. Dans de grandes

collectivités territoriales, l'agrégation des fichiers des associations subventionnées peut atteindre des proportions très conséquentes au fil des exercices budgétaires.

### De nouveaux types de traitements

Parallèlement à la mise en place des fichiers administratifs et sociaux, de nouveaux types de traitements sont apparus dans certains domaines spécifiques. Etant donné leur caractère extrêmement sensible, ces fichiers doivent faire l'objet d'un soin tout particulier de la part de la collectivité détentrice. Eu égard à leur finalité ainsi qu'aux informations conservées, leur mise en place fait l'objet d'une vigilance particulière de la part de la CNIL.

Les fichiers de suivi de l'assiduité scolaire : la loi du 5 mars 2007<sup>3</sup> a octroyé au Maire de nouvelles prérogatives en matière d'identification et d'accompagnement des familles en difficulté. À ce titre, il est devenu destinataire de nombreuses informations à caractère confidentiel en provenance des Ministères de l'Intérieur et la Justice ainsi que des institutions à caractère éducatif et social. Le Maire anime désormais, sur le territoire communal « la politique de prévention de la délinquance et en coordonne la mise en œuvre ». Une des mesures phare de ce texte revient à permettre au Maire de disposer d'informations lui permettant d'assurer le suivi de l'obligation d'assiduité scolaire des enfants domiciliés dans sa commune. Il doit ainsi procéder au recensement des enfants rési-



## *Toujours plus cyber-menacées : les collectivités territoriales*

dant sur sa commune et soumis à l'obligation scolaire. La loi prévoit qu'il puisse, pour ce faire, disposer d'un traitement automatisé de données en provenance de diverses sources, à l'image des organismes en charge du versement des prestations familiales, des chefs d'établissements et des inspecteurs d'académies. Ce traitement peut également contenir des informations sur le manque d'assiduité éventuel des élèves.

Les demandes d'attestations d'accueil : conformément à la loi, tout étranger non ressortissant de l'Union Européenne qui souhaite venir en France dans un cadre familial ou privé, pour une durée n'excédant pas trois mois, se doit de présenter un justificatif d'hébergement (attestation d'accueil signée par la personne hébergeant l'étranger) ainsi qu'un engagement de prise en charge du visiteur par son hôte en cas d'impossibilité de celui-ci de subvenir à ses besoins durant la durée de son séjour. Dans ce cas précis, le Maire doit valider l'attestation d'accueil et un fichier spécial relatif à ces demandes d'attestation peut être mis en place afin de lutter contre les détournements de procédures<sup>4</sup> à la condition expresse de respecter un certain nombre de critères précis en matière de sécurité des informations et de non croisement des fichiers.

La vidéoprotection : un nombre croissant de communes s'équipe de matériels de vidéoprotection afin de lutter contre la délinquance de voie publique. Bien que

n'apparaissant pas comme un fichier d'information nominative stricto sensu, les images issues de ces dispositifs constituent, de fait, des données à caractère personnel, puisqu'il s'agit du visage et par conséquent de l'identité de la personne filmée. De solides garanties sont exigées de la part des communes relativement à la mise en place d'un dispositif de vidéoprotection :

Le respect de la vie privée (pas de visualisation de l'intérieur d'une résidence ni d'un appartement privés) ;

Une durée de conservation limitée (fixée par l'autorité préfectorale, elle ne peut excéder un mois) ;

L'information des personnes (la présence de caméras doit faire l'objet d'un affichage clair et dépourvu d'ambiguïté sur l'ensemble de la zone couverte) ;

Le droit d'accès (toute personne peut demander à visualiser les enregistrements la concernant et vérifier la bonne destruction des données à l'issue de la période de conservation fixée) ;

Les destinataires des images (ils doivent être nominativement identifiés).

La biométrie : cet exemple est issu des dernières méthodes d'identification individuelles. Il s'agit des dispositifs de reconnaissance biométriques utilisés notamment dans le cas de contrôle d'accès



## Rémy FÉVRIER

20

cès. Étant donné le caractère extrêmement inquisiteur des techniques utilisées (reconnaissance faciale, oculaire, digitale ou veineuse), il s'agit là d'un domaine extrêmement sensible, dont la mise en place éventuelle nécessite des précautions toutes particulières de la part de la collectivité intéressée et ce, aussi bien sur le plan juridique (conservation des données) qu'humain (explications des objectifs de sécurité poursuivis auprès de l'ensemble des agents concernés). L'ensemble de ces traitements, en tant que constitués d'enregistrements à caractère personnel, est sous l'entièvre responsabilité des Maires et des présidents d'EPCI. Ces derniers, considérés comme responsables de ces traitements informatiques, peuvent voir leur responsabilité, civile et pénale, engagée en cas de non-respect des dispositions de la loi.

À l'issue de l'étude des multiples traitements évoqués ci-dessus, se pose formellement la question corolaire de leur archivage.

- *L'archivage des données*

Le succès grandissant de la notion d'administration électronique, commencé avec le transfert des actes soumis au contrôle de légalité (plus de 8 millions d'actes chaque année), a fortement catalysé la prise en compte de la notion d'archivage des documents immatériels, jusqu'à devenir un enjeu majeur de crédibilité de ce nouveau type de rapport en passe d'être instauré entre les administrations et les ci-

toyens. Responsables de l'archivage des documents et flux produits dans le cadre de leur fonctionnement, les collectivités se voient donc contraintes de gérer cette problématique dans le cadre d'un objectif de dématérialisation optimale des procédures visant à un abandon progressif d'un maximum de documents papiers.

En matière d'archivage des données, une des principales tâches préalables consiste à établir une différentiation entre les différents types de documents à conserver.

Une erreur relativement courante revient à confondre la notion d'archivage avec celle de stockage. Alors que le stockage consiste simplement à conserver un ensemble de données brutes, sans autre souci que celui de ne pas perdre l'information, le but de l'archivage est de pouvoir accéder le plus simplement possible à des données certifiées. Cela nécessite la mise en place d'un système d'indexation, fondé le plus souvent sur une architecture de type Système de Gestion de Bases de Données Relationnelles (SGBDR), dont les tables d'enregistrements sont interrogables par le biais de requêtes plus ou moins complexes, selon le langage utilisé et la puissance de calcul disponible.

### La notion de valeur probante

Si toute donnée peut faire l'objet d'un archivage, celui-ci est rendu d'autant plus nécessaire dans le cas de documents nu-



## *Toujours plus cyber-menacées : les collectivités territoriales*

mériques à valeur probante, ce qui constitue l'essentiel des données recueillies et traitées par les collectivités. Un document à valeur probante désigne la faculté qu'a ce dernier à être utilisé par un individu dans le cadre d'une obligation légale. Depuis la Loi du 13 mars 2000<sup>5</sup>, la qualité de document probatoire a été étendue à l'écrit électronique au travers de la modification de l'article 1316 du Code civil qui stipule désormais que « la preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission » et précise clairement que « l'écrit sur support électronique a la même force probante que l'écrit sur support papier »<sup>6</sup>.

### Les différents types d'archives

Il existe trois types d'archives, dont la hiérarchisation – entièrement indépendante du support utilisé – s'établit en fonction de la nature du document concerné :

Les archives courantes : de même que les entreprises, les collectivités territoriales produisent des fichiers indispensables à leur gestion courante. Ces données sont indispensables au bon fonctionnement du service public, leur utilisation est permanente et nécessite des sauvegardes très régulières.

Les archives intermédiaires : certains fichiers n'ayant plus une utilité immé-

diate doivent néanmoins être conservés afin de satisfaire à des obligations d'ordre légal ou administratif. La durée de conservation de ces derniers varie en fonction de règles spécifiques à chaque nature de document.

Les archives définitives : elles concernent exclusivement les documents présentant, comme le souligne la CNIL, un intérêt historique, scientifique ou statistique manifeste. Les collectivités territoriales n'échappent pas à cette règle et leurs archives définitives doivent faire l'objet d'un versement aux archives départementales géographiquement compétentes.

### Obligations légales

À la différence des entités privées, l'archivage des collectivités territoriales est soumis au respect de contraintes issues de nombreux textes d'origines diverses. Le régime général est donné par le Code du patrimoine<sup>7</sup>, mais des dispositions issues du CGCT<sup>8</sup> sont également applicables, ainsi que certaines directives du Code de commerce. Ces dispositions de ce cadre général sont précisées par trois décrets spécifiques<sup>9</sup>. En ce qui concerne les documents numériques, le texte de référence demeure la loi Informatique et Liberté (LIL)<sup>10</sup>, précisée par un décret relatif à la liberté d'accès aux documents administratifs<sup>11</sup>. L'ensemble de la législation concernant les obligations des collectivités territoriales est disponible sur le site des Archives de France<sup>12</sup>.



## Rémy FÉVRIER

### Intégrité des données

Au travers de l'article 1316-3 du Code civil, le Législateur a directement subordonné ce type de document à son authenticité intrinsèque : « l'écrit sur support électronique est admis en preuve au même titre que l'écrit sur support papier sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité ». Il s'avère donc indispensable, non seulement d'établir sans aucune ambiguïté l'origine du document considéré, mais également d'assurer sa parfaite conservation.

22

### Droit à l'oubli

Les données archivées sont soumises, du moins en ce qui concerne les archives courantes et intermédiaires, au respect de la Durée d'Utilité Administrative (DUA). Cette DUA représente la durée légale pendant laquelle un document est susceptible d'être utilisé par le service producteur ou son successeur, au terme de laquelle est appliquée la décision concernant son traitement final, le document ne pouvant être détruit avant cette période qui constitue sa durée minimale de conservation. À l'issue de leur phase de conservation respective, les documents doivent faire l'objet d'une suppression, a fortiori lorsque ceux-ci contiennent des données à caractère personnel afin de respecter le désormais célèbre « droit à l'oubli ». En cas de manquement à cette obligation, la CNIL peut prendre des sanctions à l'encontre de la Collectivité concernée.

### Collectivités Territoriales et archivage électronique

L'archivage électronique est soumis à plusieurs exigences fondamentales, que l'on peut regrouper en deux grandes catégories : la conservation et la sécurité.

#### Conservation optimale des données

La conservation des données peut se décliner, elle-même, en deux impératifs distincts que sont la pérennité et la traçabilité.

**La pérennité :** les documents doivent être disponibles et consultables par les personnes habilitées pendant une durée au moins égale, dans le cas d'archives courantes et intermédiaires, à leur DUA.

**La traçabilité :** chaque document doit pouvoir faire l'objet d'un suivi, depuis sa création et jusqu'à sa destruction éventuelle à l'issue de sa DUA, ou à sa date de transmission à un service d'archive.

#### Sécurité des données

L'ensemble des documents archivés doit être protégé de toute atteinte à son intégrité, qu'elle soit volontaire ou accidentelle.

La mise en place d'un système d'archivage nécessite une réflexion préalable extrêmement poussée afin de répondre aux contraintes exprimées. Que cette tâche soit assumée en interne par la collectivité, ou



## *Toujours plus cyber-menacées : les collectivités territoriales*

au travers d'un contrat avec une société spécialisée, la DSI de la collectivité doit étudier avec le plus grand soin les implications techniques inhérentes aux objectifs à atteindre. À chaque étape du processus d'archivage, des procédures déclinées en modes opératoires détaillés doivent être définies afin de mieux évaluer les contraintes techniques et humaines dont va dépendre l'efficacité du système final. Il convient de définir notamment le format numérique, les marqueurs qui vont accompagner chaque document au cours de sa vie et les moyens de contrôle à mettre en place pour vérifier le droit des agents à les consulter.

La combinaison de ces actions nécessite un minutieux travail d'évaluation et de synthèse de la part de la DSI et rares sont celles qui peuvent mener à bien l'intégralité du processus. En effet, de nombreux paramètres sont à prendre en compte, allant de la définition des éléments constitutifs de la fiche signalétique du document à l'indexation de ce dernier dans une base de données. Afin d'aider les collectivités confrontées à ces exigences légales, la Direction Générale de la Modernisation de l'État (DGME) a élaboré des référentiels normatifs en matière d'interopérabilité et de sécurité<sup>13</sup>. Les DSI pourront utilement s'inspirer du travail effectué, sachant qu'il ne constitue qu'une assistance technique et ne dispense en aucune façon de disposer des compétences nécessaires afin de mener le projet à son terme. Devant une telle complexité de mise en œuvre, le re-

cours à une prestation extérieure d'accompagnement s'avère souvent nécessaire.

### L'externalisation de l'archivage

Le choix de certaines collectivités d'externaliser leur archivage impose une grande prudence, à la fois dans le choix du prestataire et dans la rédaction du contrat de délégation : des clauses trop floues ou des objectifs insuffisamment précis sont de nature à causer de graves dysfonctionnements en termes de sécurité et d'intégrité des données. Pour éviter cet écueil, il apparaît impératif de procéder à une rédaction minutieuse du contrat, y compris en ayant recours, dans le cas où le service juridique de la collectivité ne disposera pas, en interne, de l'expertise nécessaire, à un cabinet d'avocats spécialisés. En l'absence de telles précautions, la collectivité et ses dirigeants pourraient être directement mis en cause en cas d'atteinte à l'intégrité des données, surtout si ces dernières contiennent des données à caractère personnel.

Certaines collectivités particulièrement dynamiques ont imaginé des solutions novatrices en matière d'archivage, comme la mise en place d'une architecture mutualisée<sup>14</sup>. C'est notamment le cas du Conseil général de l'Aube qui a procédé à l'élaboration de services de dématérialisation et d'archivage mutualisés à destination des 433 communes du département. Chacune d'entre elles a désormais la possibilité de bénéficier d'outils et de services de gestion



## Rémy FÉVRIER

24

des archives électroniques. Le Conseil général de Seine-Saint-Denis a choisi, quant à lui, de procéder à une dématérialisation de l'ensemble de ses procédures. Dans ce cadre, des efforts ont été entrepris afin de parvenir, dans les années à venir, à un archivage numérique complet de l'ensemble des documents administratifs.

Des actions de ce type vers la dématérialisation totale des actes administratifs sont appelées à se multiplier avec la mise en place de l'administration électronique. Néanmoins, certaines collectivités ne disposant pas des ressources nécessaires hésitent encore à franchir le pas car elles sont le plus souvent confrontées à la nécessité de procéder à la numérisation de l'ensemble de leurs fonds documentaires. Selon toute vraisemblance, cette étape indispensable vers l'administration électronique devra faire l'objet d'une attention particulière des pouvoirs publics, sous peine de freiner les efforts gouvernementaux dans ce domaine.

- *Un manque de légitimité paradoxal de la DSI*

La première chose que l'on observe, en matière d'informatisation des collectivités territoriales, réside dans son caractère éminemment progressif et l'impérieuse nécessité d'établir des interactions avec leur environnement extérieur. Les rapports établis avec les administrations et le secteur privé contraignirent mairies, conseils généraux et conseils régionaux à une adaptation de leurs procédures de gestion interne.

### Une évolution laborieuse

Peu à peu, comme dans beaucoup d'autres institutions et de structures économiques privées, la nécessité d'adapter la gestion de l'information et sa dématérialisation s'imposa aux Élus locaux et services territoriaux.

La diffusion de l'informatique émergea surtout au travers de fonctionnaires territoriaux à l'esprit « pionnier » qui, s'intéressant naturellement à l'émergence de ces Nouvelles Technologies de l'Information et de la Communication (NTIC), acceptèrent de prendre en charge la diffusion de celles-ci au sein de leurs collectivités respectives. De profils divers, souvent à dominante scientifique, mais disposant avant tout d'une sensibilité naturelle qui les portaient vers l'innovation technologique, ces novateurs avaient en commun le goût du défi et une grande capacité de travail. C'est en grande partie grâce à leur action obstinée que les collectivités territoriales sont entrées dans l'ère de l'informatique.

À l'origine, l'informatisation des collectivités, à l'image de ce qui s'est généralement passé pour la grande majorité des entreprises, a pris la forme de postes bureaucratiques individuels, l'objectif étant de substituer modestement éditeurs de texte et tableurs aux machines à écrire et calculatrices. La notion de réseau n'étant pas encore à l'ordre du jour, on vit apparaître des équipements hétérogènes constitués des « frères ennemis » qu'étaient, à l'époque les ordinateurs personnels fonc-



## *Toujours plus cyber-menacées : les collectivités territoriales*

tionnant sous MS-DOS<sup>®15</sup> (PC) et les Macintoshs<sup>®</sup> d'Apple. Chaque utilisateur devenant souvent un irréductible inconditionnel de l'un ou de l'autre système, au grand désespoir du responsable en charge de la cohérence du parc informatique.

### L'avènement de la bureautique

Peu à peu, la bureautique évolua autour de la notion de client-serveur : cette architecture permettant à la fois d'établir une certaine cohérence technique et de mettre en place des disponibilités de calcul, de stockage et d'archivage sans commune mesure avec ce qui existait précédemment. Simultanément, le concept de réseau local s'imposa dans les grandes entreprises et les administrations, structuré autour d'un serveur dédié aux tâches les plus courantes. Le développement de nouvelles applications spécifiques à chaque activité (DAO, PAO, logiciels ordo-comptables...) justifia l'émergence d'une véritable direction informatique au sein des collectivités avec le recours à des contrac-tuels extérieurs, souvent plus à même de gérer la mise en place de véritables SI, susceptibles d'apporter confort et efficacité dans la gestion de l'activité quotidienne.

### L'impact d'Internet

Cette évolution prometteuse connaît une nouvelle accélération, à partir du milieu des années 1990, avec la diffusion d'Internet. Cette innovation majeure constitua

une véritable révolution qui est encore loin d'être achevée à l'heure actuelle. Face à des évolutions de plus en plus rapides, la notion de Direction des Systèmes d'Information (DSI) s'imposa bientôt, en lieu et place de l'ancienne appellation de Direction Informatique. L'apparition de ce vocable souligne le caractère éminemment stratégique qu'ont acquis, au fil du temps, les réseaux internes jusqu'à constituer, aujourd'hui, l'épine dorsale technique de l'activité des collectivités.

### Des facteurs déterminants

Comme dans beaucoup d'autre type d'organisations, la diffusion des TIC au sein des collectivités a également varié en fonction de l'appétence technologique de certains de ses membres ou de la taille intrinsèque de la structure.

### Le facteur humain

Pour autant, cette évolution s'est faite de manière extrêmement diverse selon les collectivités et le facteur humain a une nouvelle fois présidé à son évolution plus ou moins rapide au travers non plus de la personnalité d'un responsable technique mais bien plutôt en fonction du niveau d'appropriation de la problématique par les Élus : les communes, puis les conseils généraux et régionaux, ont accompagné la mise en place d'un portefeuille portant spécifiquement sur les nouvelles technologies. Selon le parcours professionnel, la curiosité d'esprit et la conscience



Rémy FÉVRIER

26

qu'avaient ces Élus de l'importance des TIC, de grands progrès furent accomplis en matière de structuration des SI internes, puis de mise en place de véritables infrastructures informatiques à l'usage des administrés.

### La taille de la structure

La mise en place d'un SI dans une collectivité est étroitement liée à la taille de celle-ci. Au cours de missions réalisées à la demande de collectivités territoriales, nous avons pu constater des différences d'approches assez conséquentes quant à la prise en compte des problématiques liées aux systèmes d'informations et à leur suivi quotidien. Les collectivités de taille modeste apparaissent souvent assez mesurées quant à la gestion d'un SI. Beaucoup d'Élus locaux de communes ou d'EPCI de taille modeste, conservent une vue excessivement complexe et essentiellement technique d'une infrastructure informatique. Cette représentation, qui devrait s'estomper au fil du temps du fait de la diffusion toujours plus grande des TIC sur l'ensemble du territoire, demeure à l'origine de certaines difficultés de mise en place d'applicatifs spécialisés, sans parler des intranets ou des portails Internet.

### Repenser le management des SI

Les SI des collectivités connaissent une mutation rapide, en grande partie catalysée par la mise en place de nouveaux services à destination des administrés.

### Un caractère stratégique à reconnaître

Cette évolution est paradoxale car, en dépit d'un caractère stratégique des SI le plus souvent reconnu, le positionnement organisationnel des DSI traduit encore les efforts qui sont à fournir afin que celles-ci gagnent, définitivement, leurs lettres de noblesse. Ces services doivent devenir des partenaires à la fois opérationnels et stratégiques, aptes à assurer un rôle reconnu en termes d'assistance interne tout en assumant pleinement une fonction de conseil en matière d'aide à la définition et à la réalisation de projets stratégiques.

### Un positionnement inadéquat

Afin de mieux appréhender cet état de fait, nous complèterons notre expérience de ces situations par l'analyse de deux enquêtes récentes consacrées à ces évolutions, menées respectivement par le cabinet Mazars<sup>16</sup> en partenariat avec l'Association des Maires des Grandes Villes de France et Sopra Group<sup>17</sup> en collaboration avec le Forum pour la Gestion des Villes et des Collectivités Territoriales. Au-delà de proportions et de pourcentages toujours délicats à interpréter globalement, la pertinence de ce rapprochement réside dans la remarquable corrélation de nombreuses tendances relatives, non seulement à la perception de la notion de SI par les décideurs territoriaux (Élus et fonctionnaires), mais également aux perspectives d'évolution liées à celle-ci.



## *Toujours plus cyber-menacées : les collectivités territoriales*

### Une légitimité réduite à la dimension technique

Ces études établissent le caractère récent de la dénomination « Direction des Systèmes d'Information », y compris dans les grandes collectivités puisque dans 75% des cas, le vocable DSU n'est employé que depuis moins d'une dizaine d'années. Savant que leur taille respective constitue l'un des facteurs majeurs d'appropriation par les collectivités des principales méthodes de management et d'organisation contemporaines, il semble légitime d'envisager que la diffusion de ce terme connaisse un cheminement encore plus long dans les communes et EPCI de taille réduite.

Au-delà du signifiant, le vocable de DSU suggère en lui-même le caractère éminemment stratégique du SI. Or, alors même que régions et départements ont convenablement intégré cet aspect prévisionnel, de nombreuses communes et EPCI considèrent encore ces directions au travers d'un prisme structurant, mais essentiellement lié à la notion de technicité sous-jacente : Direction de l'Organisation et des Moyens Techniques, Direction des Technologies de l'Information, Direction Informatique et Télécoms... Souvent tributaires d'un archétype de fonction support et d'un rattachement aux Services Généraux, les SI peinent à émerger en tant qu'entités distinctes à forte valeur ajoutée prospective. Cette situation est d'autant plus paradoxale que les résultats des enquêtes laissent apparaître une large prise de

conscience, par les Élus et hauts fonctionnaires territoriaux, du caractère éminemment positif des SI en tant que vecteurs de modernité et d'adaptation aux nouveaux enjeux socio-économiques.

Cependant, contrairement à ce que l'on observe dans la quasi-totalité des grandes entreprises, cette reconnaissance affichée ne se traduit pas nécessairement par un rattachement hiérarchique adéquat ou une participation aux instances décisionnaires : les DSU ne dépendent encore que rarement de la direction générale et, dans plus de la moitié des grandes collectivités, ces dernières ne sont pas même associées aux comités de direction. Néanmoins, ces obstacles n'empêchent pas complètement les DSU de contribuer utilement à la définition et à la mise en œuvre de la stratégie définie par la collectivité car souvent, le lien de confiance existant entre les DSU et leurs Élus de tutelle apparaît de nature à permettre à ce service d'expliciter son point de vue et ses apports potentiels.

### Une certaine hétérogénéité

Dans leur activité quotidienne, les DSU sont soumises à des enjeux variés et directement liés à la nature de la collectivité. En conséquence, les villes orientent plus volontiers l'activité de leur DSU vers la mise en place des diverses réformes qui les impactent, et les EPCI vers les moyens de maîtriser leurs obligations juridiques. Les DSU des Régions et Départements se préoccupent avant tout d'accompagner, du



## Rémy FÉVRIER

mieux possible, les nouveaux transferts de compétences issus de la loi du 13 Août 2004 des domaines aussi variés que la formation professionnelle sanitaire et sociale, la voirie ou encore l'enseignement.

### Impact des évolutions législatives sur l'activité SI

D'autres paramètres influent directement sur l'activité des DSIs, comme le montre le taux, encore faible mais en pleine progression, de mutualisation des Systèmes d'Informations entre communes membres d'un même EPCI. Certes, des rapprochements se font jour, mais ceux-ci sont encore trop souvent limités à la mise en place de groupements de commandes, la mutualisation des fonctions s'avérant plus délicate à mettre en place, notamment du fait de l'asymétrie de moyens et d'infrastructures pouvant exister entre des villes de tailles par trop différentes. Une évolution est néanmoins perceptible, la mutualisation des Systèmes d'Information apparaissant de plus en plus comme un des moyens susceptibles de permettre d'atteindre une efficacité nouvelle dans les services apportés aux administrés.

La question du degré direct d'implication de l'exécutif varie également assez fortement selon la taille de la collectivité, les plus modestes ne disposant généralement pas des ressources humaines nécessaires pour assurer une tutelle directe sur la DSIs au travers d'un Élu spécifiquement dédié aux TIC. Inversement, si on en croit

le panel de l'étude Sopra group, dans 25% des grandes collectivités hors départements, plusieurs Elus se partagent l'ensemble des problématiques liées aux SI, ce qui nécessite une vigilance accrue afin d'éviter des luttes d'influence toujours possibles et susceptibles d'amoindrir l'impulsion initiale.

### Des défis managériaux

Au-delà de ces contingences, force est de constater que les DSIs sont aujourd'hui en pleine expansion et bénéficient indubitablement d'un remarquable consensus quant à la nécessité de favoriser l'émergence d'une véritable administration électronique, dont le but est de faciliter les démarches et formalités administratives et d'assurer une qualité de service optimale pour le citoyen connecté. Pourtant, en dépit de cette unanimité, il s'avère que la plupart des DSIs sont quotidiennement confrontées à des difficultés organisationnelles résultantes de l'insuffisante prise en compte par les autres services et strates de direction, de l'aspect transversal des SI et de la nécessité d'intégrer la DSIs en amont de chaque projet d'envergure. Les deux études présentent conjointement cette sous-estimation de leur rôle comme la principale préoccupation des responsables interrogés, loin devant les aspects budgétaires ou les contraintes techniques.

Les collectivités territoriales sont parties prenantes d'un environnement public



## *Toujours plus cyber-menacées : les collectivités territoriales*

dans lequel la mise en place d'une Gestion moderne et dynamique des Ressources Humaines (GRH) est encore assez récente (Chanut & Chavas, 2008). Or, Si la montée en puissance des collectivités territoriales s'est accompagnée d'une décentralisation parallèle de la GRH (De Fabrègues, 1992), ce mouvement se heurte, dans le cas de la DSi, à des difficultés récurrentes en matière de recrutement. Une quasi-unanimité se dégage, parmi les DSi, pour réclamer plus de souplesse dans le recrutement de leurs collaborateurs, dans la mesure où tout délai relatif à l'embauche d'un agent peut retarder considérablement, voire mettre en péril, certains projets nécessitant une expertise technique de haut niveau. Les DSi figurant parmi les services les plus consommateurs de contractuels, une solution pourrait être de mettre définitivement en place un concours adapté aux exigences des métiers de gestion des réseaux, afin de fidéliser des collaborateurs attirés par le service public mais tributaires de renouvellements de contrats à durée déterminée et qui partent le plus souvent dans le secteur privé au bout de quelques années d'activité en collectivité.

Eu égard à la spécificité des traitements informatiques quotidiennement réalisés par les collectivités territoriales et dont la plupart concernent des données à caractère personnel, on pourrait penser que la sécurité figure parmi les principales préoccupations des DSi. Or, force est de constater qu'elle ne représente globalement

qu'une faible partie de leur activité. Il s'agit pourtant d'une nécessité incontestable, dont l'absence de prise en compte peut s'avérer infiniment dommageable, à la fois pour la collectivité en elle-même, mais également pour l'ensemble des Élus et des services. Le fait de bénéficier de la confiance des administrés implique, pour les Élus et responsables administratifs, de faire preuve d'une grande prudence dans le traitement et le stockage des données et d'assurer une sécurité optimale de ces dernières.

Les collectivités territoriales se distinguent par la grande diversité de leurs traitements informatiques : entités institutionnelles, elles sont également au cœur des rapports entre l'administration et les citoyens, comme avec le tissu économique local. À ces différents titres, elles ont à traiter de grandes quantités d'informations allant de la gestion interne courante au traitement de grandes quantités de données à caractère personnel. L'informatisation des collectivités ne s'est pas effectuée de manière rapide et uniforme, mais au contraire très progressivement, jusqu'à occuper, aujourd'hui, une place prépondérante. Néanmoins, à l'heure où l'administration électronique se met en place à grande échelle, un certain nombre d'indices montrent que le rôle stratégique des SI, bien que reconnu, a souvent du mal à émerger structurellement en termes de rattachement hiérarchique ou de participation à l'évolution stratégique de ces collectivités.



Rémy FÉVRIER

## 2. Les Collectivités face aux menaces numériques

Pour parler simplement, relativement aux menaces numériques touchant les SI des collectivités territoriales françaises, on peut considérer que nous en sommes encore, pour le moment du moins, à un niveau non encore complètement préoccupant. Toutefois, il est quasiment certain que, dans un avenir proche, le niveau de danger augmentera fortement au point de menacer directement, non seulement l'intégrité des données dont les collectivités sont dépositaires, mais également les Élus locaux en termes de mise en cause personnelle.

30

- *Exemples concrets*

Pour donner corps à ce constat qui induit la nécessité, pour les collectivités territoriales, de protéger convenablement leurs systèmes d'information, nous prendrons plusieurs exemples d'attaques récentes contre les SI des collectivités territoriales afin d'illustrer explicitement la typologie des menaces mais également de montrer la nature protéiforme de ces dernières selon le but recherché.

### Pénétration du SI

Le premier type d'attaque informatique revient à la pénétration d'un SI d'une collectivité depuis l'extérieur. Nous relèverons, à ce propos, trois exemples particulièrement symptomatiques de com-

promission de systèmes mettant en cause des grandes villes : La ville de Reims (51) a subi dans les premiers jours de mars 2011, une attaque de type pénétration directe via un flux RSS<sup>18</sup>. Révélé par la presse locale, il semble que les pirates aient profité d'une faille de sécurité spécifique.

Le rédacteur de l'article, que l'on sent surpris par le fait qu'une mairie puisse faire l'objet d'une attaque informatique directe, précise qu'en dépit de ses demandes, il ne dispose d'aucune information sur les conséquences de l'attaque, notamment en termes de perte ou de détérioration d'informations. Néanmoins, ce dernier s'interroge avant tout sur les raisons de la pénétration : « Ce qui pose désormais question, c'est le pourquoi de l'attaque » ainsi que sur l'émergence de nouvelles cibles jusque là épargnées : « Un avertissement [...] mais bel et bien symptomatique d'une nouvelle forme de délinquance qui émerge »<sup>19</sup>. On ne saurait mieux mettre en évidence le fait selon lequel, alors même que la possibilité d'attaques contre des institutions étatiques semble désormais établie, il n'en va pas du tout de même avec des collectivités territoriales dont on ne réalise pas encore véritablement le potentiel en matière de gestion de données sensibles et par voie de conséquence, la vulnérabilité à des tentatives de compromission, voire de sabotage.

Pourtant, le même type de cyberattaque s'était déjà produit auparavant, tout en



## *Toujours plus cyber-menacées : les collectivités territoriales*

étant passé largement inaperçu, notamment en 2005, lorsque le SI de la mairie de Clichy-sous-Bois (93) fut l'objet d'une pénétration ayant entraîné la mise en ligne d'une fausse information, annonçant la démission du Maire, sur le site municipal ainsi qu'àuprès de l'ensemble des abonnés à la lettre numérique d'information municipale. Cet article, ajouté illégalement a nécessité un démenti de la part de la mairie sous la forme d'un communiqué de presse publié sur son site : « Un article a été publié illégalement sur le site Internet de la ville de Clichy-sous-Bois mercredi 3 novembre de 20 heures à 21 h et un mail envoyé aux abonnés de la newsletter. Les informations qu'il relate sont bien évidemment mensongères et n'engagent en rien la Ville de Clichy sous Bois »<sup>20</sup>.

Cependant, le cas le plus emblématique de pénétration de système – avant tout de par la qualité du premier édile municipal – demeure celui qui a frappé la ville de Longjumeau (91), au mois d'octobre 2009, le Maire n'étant autre que Mme Nathalie Kosciusko-Morizet, à l'époque Secrétaire d'État auprès du Premier ministre, chargée de la Prospective et du développement de l'économie numérique. Le SI de la ville a ainsi fait l'objet d'une pénétration directe visant une prise de contrôle de plusieurs ordinateurs municipaux : « Certaines machines ont commencé à avoir un comportement étrange, à s'allumer toutes seules, à faire défiler des pages et des menus, d'autres ne répondaient plus... raconte Nathalie Kosciusko-Morizet. Nous ne

connaissions pas l'état d'infection des ordinateurs et du serveur, mais par sécurité tous ont été déconnectés pour être vérifiés. » « C'est un acte de malveillance, ça ne fait aucun doute »<sup>21</sup>. Cette dernière a d'ailleurs publié, en toute transparence, le compte-rendu de la découverte de l'attaque et des mesures de sauvegardes prises sur son blog personnel<sup>22</sup>.

### Dénaturation de site

Si les sites des grandes entreprises constituent des cibles de choix pour des pirates ou certains activistes opposés à l'activité de celles-ci (expérimentation animale, exploitation pétrolière...), de plus en plus de portails publics font également l'objet d'une dénaturation. Ainsi, l'aéroport de Montpellier (34) a t-il fait l'objet, durant le week-end du 15 août 2010, d'une pénétration informatique visant à remplacer la page d'accueil de son site web par un message politique visant directement le président de la République et signé du patronyme pirate « Ma3sTr0-Dz »<sup>23</sup>.

31

Mais ce genre de désagrément n'est pas réservé aux sites consulaires : des mairies en font également les frais. Nous prendrons, à ce propos, deux exemples de communes dont les sites web ont été dénaturés, alors même que leurs tailles modestes ne les désignent pas intuitivement comme de potentielles victimes.

Le premier exemple est celui de la ville de Gaillac (81) (11.000 habitants) qui a fait



## Rémy FÉVRIER

l'objet, le 20 mars 2010, d'une pénétration de son site web conduisant à sa dénaturation et l'apparition du message « Hacked by WaZo & eyMz »<sup>24</sup>, ces deux pirates n'en étant pas à leur coup d'essai puisqu'on estime qu'avant leur arrestation par la police, ils avaient réussi à pénétrer plus de 300 sites institutionnels sur l'ensemble du territoire<sup>25</sup>.

Pareillement, le village de Croisilles (62) (1300 habitants) a connu une mésaventure similaire le 2 août 2010 : le site Internet municipal a été piraté alors même qu'une nouvelle version plus ergonomique et réactive devait être lancée quelques jours plus tard. La page d'accueil du site avait été remplacée par un visage inconnu et entouré par les mentions « hacked » (piraté) et « 1923Turk Grup »<sup>26</sup>, en référence, semble-t-il à la date de proclamation de la république de Turquie. Néanmoins, à l'instar de l'origine initiale d'une attaque informatique, ce genre de message doit être pris avec beaucoup de prudence et n'est pas toujours révélateur de la personnalité ou des motivations de son auteur. Cette agression numérique montre qu'un village de petite taille peut dorénavant être autant la cible d'un piratage informatique qu'une grande ville.

### Contrefaçon de site

Le dernier exemple que nous retiendrons relève de la possibilité, pour un « hacker » habile, de contrefaire le site d'une collectivité au travers de l'utilisation d'une adresse de site très proche de celle de la

cible et qui peut se substituer à elle en cas d'utilisation d'un moteur de recherche. Ainsi, à plusieurs années d'écart, la ville de Toulouse (31) a fait l'objet de deux attaques indirectes visant à aiguiller les internautes sur des noms de domaines se faisant passer pour le site municipal officiel.

Si aujourd'hui l'adresse du portail Internet de la ville de Toulouse a été simplifiée pour devenir « [www.toulouse.fr](http://www.toulouse.fr) », elle est longtemps demeurée « [www.mairie-toulouse.fr](http://www.mairie-toulouse.fr) ». Or, en 2003, suite à certaines affaires judiciaires mettant en scène de supposées soirées libertines mêlant certains notables toulousains – et dont la justice montrera plus tard l'absence de fondement – le site « [www.mairie-de-toulouse.fr](http://www.mairie-de-toulouse.fr) » proposait une contrefaçon du site municipal agencé à l'identique du site officiel mais proposant une rubrique « libertinage à Toulouse » qui renvoyait à des photos explicites censées représenter les personnalités précitées.<sup>27</sup> Puis, en mai 2009, l'infortuné site municipal sera de nouveau contrefait mais cette fois au travers du site « [www.mairietoulouse.fr](http://www.mairietoulouse.fr) » qui jouera, de manière nettement moins dramatique, sur le surnom de « ville rose » pour annoncer aux internautes la mise en place d'un nouveau projet d'aménagement urbain visant à permettre de « batifoler à tous les coins de rue »<sup>28</sup>.

### Un phénomène global

En plus d'être nouveau, le phénomène semble devoir s'établir de manière globale



## *Toujours plus cyber-menacées : les collectivités territoriales*

– suite logique de la diffusion des TIC – comme le montrent certains exemples récents.

En mai 2010, cinq pirates ont été inculpés pour avoir porté préjudice, trois années auparavant, à la ville de Carson (Californie)<sup>29</sup>. En réussissant à infecter le logiciel d'identification présent sur l'ordinateur portable de la comptable municipale, les auteurs ont volé 450.000 dollars depuis l'un des comptes bancaires de la municipalité. Suite à cette affaire, la mairie de Carson a réagi en mettant en place un nouveau processus de sécurisation des transferts financiers : désormais, trois responsables de cette collectivité reçoivent des notifications de toute transaction par e-mail, sms et fax. Cet exemple illustre très bien le fait selon lequel les collectivités territoriales deviennent reconnues comme des entités économiques et, dès lors, susceptibles d'être victimes d'attaques d'essence crapuleuse.

En Europe également, certaines collectivités font les frais de ce nouveau genre de menaces : le site Internet de la ville belge de Rochefort a fait l'objet, le 19 Août 1987 d'une défiguration particulièrement malséante : en lieu et place de la page d'accueil figurait un postérieur masculin... et la ville n'en a été avertie que par un appel extérieur. L'enquête a montré que la ligne téléphonique ayant servi à l'attaque provenait d'Allemagne et que le méfait était lié à la volonté de disposer d'espace de stockage pour des contenus pornogra-

phiques<sup>30</sup>. Cet exemple s'est avéré au final sans réelle gravité mais qu'en aurait-il été si, en lieu et place d'images pornographiques, les pirates avaient dissimulé, de manière un peu plus habile et surtout moins voyante, des images à caractère pédophile ?

Le 5 février 2011, le portail web de l'Union de la ville et des communes de la Région Bruxelloise a été piraté par le « Mouvement Offensive Hackers » (MOH) qui, selon la Radio Télévision Belge Francophone (RTBF), semble apparenté à « la mouvance des cyber-activistes de WikiLeaks »<sup>31</sup>. Le MOH avait déjà fait parler de lui auparavant en publiant des données supposées confidentielles en provenance, entre autres, de ministères de la Région wallonne.

33

On peut sans grand risque émettre l'hypothèse selon laquelle les attaques numériques contre les collectivités territoriales s'amplifieront à mesure que ces dernières verront leurs responsabilités et leurs prérogatives s'étendront, ce qui semble devoir être une tendance globale, a fortiori au sein de l'UE.

### • *Les principales failles*

A mesure que se développaient les SI des collectivités territoriales, leur exposition aux risques numériques s'est accrue et de nombreuses failles potentielles sont apparues. Le fait de chercher à mesurer leur vulnérabilité réelle implique de passer



## Rémy FÉVRIER

en revue les principaux vecteurs de menaces utilisés par les cybercriminels pour attenter à l'intégrité des données et des systèmes.

### Les portails web

Les sites Internet constituent une des cibles les plus exploitées en matière de pénétration des SI institutionnels. Pour comprendre cette problématique, il est indispensable de connaître les mécanismes qui entrent en jeu dans la consultation d'un portail web.

### Pénétration d'un site

34

Internet constitue un gigantesque enchevêtrement de réseaux entrecroisés couvrant l'intégralité de la planète. Les informations transitant sur ce "réseau des réseaux" sont de différentes natures (messages électroniques, pages web, chat, flux rss...) et plusieurs protocoles de transferts sont utilisés selon la nature du flux acheminé : Hyper Text Transfert Protocol (HTTP) pour la consultation des sites, Simple Mail Transfert Protocol (SMTP) pour les mails, File Transfert Protocol (FTP) pour l'échange direct de grandes quantités de données etc. Or, chacune de ces architectures logiques de transfert est vulnérable. Afin de mieux comprendre les enjeux de la sécurité, relativement à l'utilisation du vecteur Internet par une collectivité, il est indispensable de présenter brièvement la notion de page web, ainsi que l'architecture des transferts de flux de données

s'établissant lors de la consultation de celle-ci. Nous reprendrons en cela la nomenclature des chercheurs de l'université de Valenciennes, à l'origine de la création de la première licence française d' « Ethical Hacking<sup>32</sup> », (Crocfer, Ebel, Hennecart, 2010).

### Architecture globale

De nombreux portails ont été conçus avec comme objectif principal de séduire l'internaute, au travers d'une ergonomie et d'une fonctionnalité optimales. Si ces considérations constituent des prérequis indispensables pour assurer une utilisation régulière desdits sites, cela ne doit pas s'effectuer au détriment de la sécurité. On observe pourtant que ce dernier aspect est souvent ignoré ou du moins largement minoré lors de la conception des sites. Il s'agit là d'une véritable erreur stratégique : cela revient à rendre vulnérable l'ensemble du SI de la collectivité ainsi qu'à faire fuir le citoyen internaute soucieux de ne pas voir ses informations personnelles faire l'objet d'une interception.

Une grande partie des sites Internet ne disposent toujours pas d'un verrouillage de leur arborescence interne : il suffit la plupart du temps à l'internaute connaissant les règles standards d'arborescence interne, d'effectuer une simple manipulation au niveau de l'adresse Internet figurant dans son navigateur (lien URL<sup>33</sup>) pour rentrer tout simplement dans l'architecture interne du serveur.



## *Toujours plus cyber-menacées : les collectivités territoriales*

Nous avons malheureusement pu constater que de nombreux serveurs sont accessibles par ce moyen et qu'avec un minimum de connaissances en matière d'arborescence des systèmes UNIX (Uniplexed Information and Computer Service), il était extrêmement aisément d'accéder aux fichiers de l'ensemble des mots de passe ! Cette faille excessivement simple à utiliser ne constitue néanmoins qu'une des attaques possibles à l'encontre d'un site web : la pénétration volontaire relève le plus souvent de la mise en place d'un mode opératoire extrêmement méticuleux. Sans rentrer dans des détails d'ordre technique par trop repoussant, nous allons dérouler le schéma type d'une attaque à l'encontre d'un portail Internet.

### La phase de recueil d'informations (« fingerprinting »)

La pénétration d'un site web implique généralement – hormis le cas évoqué précédemment – le recueil d'un maximum d'informations concernant la structuration et les caractéristiques techniques internes de ce dernier : langage de programmation utilisé, arborescence, cookies, systèmes d'identification... La plupart du temps, le recours à quelques logiciels spécialisés librement disponibles sur le Net permettra de connaître ses principales fonctionnalités (technique dite de fingerprinting ou prise d'empreinte) et d'en déduire son comportement face à telle ou telle attaque. Une fois cette action réalisée, il devient nécessaire d'utiliser d'autres outils pour

cartographier (mapping) plus précisément la « face cachée » du site (ensemble des paramètres de structuration).

Dans la plupart des cas, le concepteur du site se polarise sur l'aspect fonctionnel de celui-ci et ne prend pas le temps de tester convenablement le site en cas de sollicitation anormale, ou d'erreur de comportement aberrant de la requête client vers le serveur. Cette accumulation d'informations va permettre aux pirates de déterminer un vecteur optimal de pénétration du site et de choisir un type d'attaque particulier, en fonction du but recherché et de la nature des failles découvertes.

### Les principaux types d'attaques

Selon l'association ACSSI<sup>34</sup>, les attaques à l'encontre d'un site Internet peuvent globalement être classées en quatre principales familles, selon le procédé utilisé.

#### L'attaque par DDoS

Elle vise à rendre le site inaccessible durant le maximum de temps. Dans le cadre d'une collectivité territoriale, les dégâts sont directement proportionnels au nombre de services accessibles en ligne par le public et peuvent donner lieu, entre autres, à des mouvements d'humeurs de citoyens, a fortiori si l'incident se produit lors d'une campagne d'inscription en ligne à un service public précis : crèches, écoles des sports, centres aérés, programmes culturels etc.



## Rémy FÉVRIER

### La modification du contenu

Le but recherché est de dénaturer un site en y incluant des informations extérieures. Cette intrusion vise généralement à décrédibiliser la collectivité ou l'entreprise propriétaire du portail web et peut impacter durablement les esprits des internautes, selon la violence des propos tenus et leur apparence de véracité. Ce type d'attaque redoutable peut considérablement nuire à l'image de l'institution concernée ainsi qu'à celle de ses dirigeants (e-réputation).

### La récupération illicite d'informations

Étant donné la grande diversité des données traitées par les collectivités territoriales (données à caractère personnel ou économique), il s'agit là d'un danger majeur de nature à induire des répercussions civiles et pénales pour les Élus locaux, selon la qualité de la politique SSI suivie et la rigueur de sa mise en place.

36

### La prise de contrôle du serveur

Cette technique consiste à agir de manière indirecte en se servant de la puissance du SI pénétré pour attaquer un autre serveur de manière anonyme, l'offensive étant alors identifiée comme provenant du SI de la collectivité piratée.

### Les postes de travail

Les postes de travail individuels représentent potentiellement une autre source

de vulnérabilité majeure du fait de leur utilisation quotidienne et du peu de précautions prises par des agents qui n'ont, dans l'immense majorité des cas, pas été sensibilisés aux risques encourus relativement à l'utilisation quotidienne d'un ordinateur connecté à Internet.

### L'utilisation d'Internet

Dans le cadre de l'utilisation d'Internet, les risques encourus sont principalement de deux ordres. Ceux-ci sont liés, d'une part, à la notion d'intégrité du SI et d'autre part, à la consultation de portails web prohibés. Dans un cas, c'est le chef de l'exécutif local qui est directement sous la menace de poursuites judiciaires, alors que dans l'autre, c'est l'intégrité du SI qui est menacée avec, au final, le risque de voir se diffuser vers l'extérieur des données à caractère personnel, ce qui mettra également en cause directement la responsabilité pénale de l'Élu.

Si la mise à disposition des fonctionnaires territoriaux d'un accès personnel à Internet constitue globalement la règle, il s'avère indispensable de prendre un certain nombre de précautions de bon sens afin d'éviter, le cas échéant, une éventuelle mise en cause pénale. Faute de charte opposable d'utilisation ou de restriction d'utilisation, les agents peuvent accéder à n'importe quel site Internet, même prohibés par la loi, ainsi qu'à tous types de forum de discussion. Cette situation pose le problème de la nécessité,



## *Toujours plus cyber-menacées : les collectivités territoriales*

pour l'Élu local, de prendre des mesures conservatoires relativement aux agissements de ses collaborateurs ainsi que des personnes extérieures transitant sur son réseau.

Pas plus qu'une entreprise, une collectivité ne peut aujourd'hui interdire l'utilisation, à des fins personnelles, de l'ordinateur de travail utilisé par le collaborateur mais ce dernier doit toutefois veiller à une utilisation raisonnable de son poste. Les impératifs de la collectivité et le nécessaire respect de la vie privée des agents doivent être conciliés, grâce à la discussion collective et à la formation des utilisateurs à la sécurité informatique.

Bien que le collaborateur ait le droit d'utiliser, depuis son poste de travail, Internet à des fins personnelles, cette utilisation doit impérativement respecter la législation en vigueur relative à la licéité des sites consultés et des opérations effectuées. Ainsi, un certain nombre d'items de consultation sont purement et simplement interdits au collaborateur dans le cadre de son travail. On peut citer à ce propos les sites à caractères pédophile, raciste ou encore négationniste. Toutefois, la consultation de certains sites ne constitue pas la seule interdiction faite au collaborateur : le téléchargement de musique ou de film (via P2P<sup>35</sup>) est également prohibé, ainsi que le développement d'un portail web personnel ou encore la participation à des forums sans rapport avec son activité professionnelle.

Ce qui apparaît le plus préoccupant aujourd'hui, devient sans conteste le fort tropisme des salariés internautes à utiliser des réseaux sociaux : ceux-ci constituent de véritables aubaines pour des pirates souhaitant pénétrer le SI d'une entreprise ou d'une collectivité. En effet, les réseaux sociaux figurent parmi les applications les moins sécurisées et les plus enclines à être pénétrées au travers de l'exploitation de failles de sécurité ou plus simplement encore la crédulité de l'internaute par la technique dite du « social engineering<sup>36</sup> ».

### L'utilisation d'une messagerie électronique

L'utilisation de la messagerie électronique a révolutionné le monde de la communication professionnelle et personnelle. L'ensemble des entités publiques et privées ont, peu à peu, appris à maîtriser ce nouvel outil synonyme de meilleure efficience opérationnelle. Pour autant, la messagerie électronique demeure, comme on a pu le voir dans les exemples précédents, l'un des moyens les plus efficaces de pénétrer à distance dans le poste de travail d'un agent ou d'un collaborateur.

Le vecteur le plus couramment utilisé pour pénétrer un poste de travail à distance en vue d'y soustraire des informations confidentielles demeure le mail, que ce soit par l'intermédiaire d'un pourriel ou par un mail en provenance d'une adresse électronique connue mais usurpée. Dans les deux cas, le principe est le même : on





Rémy FÉVRIER

envoie un mail avec un fichier joint et tout va être fait, au travers du message constituant le corps du texte, pour inciter l'utilisateur à ouvrir cette pièce jointe contenant un trojan<sup>37</sup> qui va ouvrir une backdoor<sup>38</sup> et installer un keylogger<sup>39</sup>. Ainsi, à intervalles réguliers, l'ensemble des données entrées en mémoire vont faire l'objet d'un enregistrement à l'insu du propriétaire du poste de travail et d'un envoi vers une adresse IP<sup>40</sup> (Internet Protocol) déterminée à l'avance.

De surcroît, il est un autre danger, très largement négligé relativement à l'utilisation de la messagerie : le caractère juridique du document électronique et du document envoyé par voie électronique. En effet, seul un document signé de façon électronique sûre, permet de donner une réalité juridique à la correspondance.

### Les postes nomades et Tablettes

Le vol d'informations et l'espionnage industriel sont une réalité à laquelle toutes les entreprises sont confrontées. Le risque est encore mal évalué, trop souvent sous-estimé. Ce risque augmente pourtant avec le succès des technologies mobiles : périphériques qui transportent de plus en plus de données stratégiques et qui restent le talon d'Achille des politiques de sécurité. En effet, peu de personnes savent que 15% des ordinateurs volés le sont pour leurs données confidentielles et que les pertes financières dues aux vols d'ordinateurs portables sont les deuxièmes plus impor-

tantes derrière celles dues aux virus. À titre d'exemple, plusieurs centaines d'ordinateurs portables sont perdus chaque semaine dans les grands aéroports mondiaux.

Face au vol ou à la perte d'un ordinateur portable contenant les fichiers clients, la comptabilité, les présentations stratégiques, les données financières de l'entreprise ou encore les bases de contact et les commandes du jour, les protections traditionnelles que sont les antivirus et les pare-feux ne sont d'aucune utilité.

Si les réseaux internes d'entreprises demeurent extrêmement vulnérables et doivent faire l'objet d'une attention de tous les instants de la part du service informatique, leur pénétration nécessite la plupart du temps des ressources conséquentes en matériels et logiciels, sans compter les complicités internes éventuelles. Pour autant, l'étanchéité indispensable à la préservation des données stratégiques de l'entreprise est de plus en plus mise à mal par un phénomène d'ampleur croissante : le vol d'ordinateurs portables. En effet, avec la mobilité accrue des acteurs constituant l'entreprise ou la collectivité territoriale, les risques se sont considérablement accrus. Quelle organisation moderne, qu'elle soit publique ou privée, pourrait dorénavant se passer d'ordinateurs portables ? Ces derniers rendent des services inestimables et tout porte à considérer que ce phénomène s'accentuera encore à l'avenir. Néanmoins, le succès rencontré par les



## *Toujours plus cyber-menacées : les collectivités territoriales*

portables et autres tablettes a induit de nouvelles vulnérabilités en matière de captation de données.

En effet, les ordinateurs portables contiennent souvent des informations de première importance dont la divulgation est de nature à nuire grandement à l'entreprise et demain à la collectivité. Face à cela, bien peu de DSI font preuve de lucidité. La plupart continuent de se contenter de sécuriser le réseau interne, laissant le soin aux possesseurs d'assumer la responsabilité de leur perte éventuelle : le plus souvent, les formalités de mise à disposition d'un portable ou d'une tablette auprès d'un collaborateur se limitent à la signature d'une « décharge » qui libère le service informatique de toute responsabilité ultérieure et au choix d'un mot de passe personnel.

Cet état de fait n'est pas satisfaisant car il n'implique aucune véritablement de prise de conscience, par le collaborateur, de l'ensemble des enjeux relatifs à la préservation des données. Le récipiendaire devrait se voir signifier les précautions élémentaires à respecter relativement à son ordinateur, ainsi que les éléments de base de sécurité, qu'elle soit physique (toujours veiller à garder le portable à portée de vue en cas de déplacement) ou logique (proscrire le mot de passe « date de naissance » ou « prénom des enfants »). À ce titre, on peut noter que 31% des managers français déclarent noter leur mot de passe sur un document (post-it...) afin de

pouvoir s'en souvenir et 25% admettent le partager avec d'autres personnes<sup>41</sup> !

### Les réseaux sans-fil (« Wireless »)

Le vocable WiFi (contraction de Wireless Fidelity), devenu synonyme de connexion sans fil, correspond, à l'origine, au nom donné à la certification délivrée par la Wi-Fi Alliance, autrefois WECA (Wireless Ethernet Compatibility Alliance), l'organisme chargé de maintenir l'interopérabilité entre les matériels répondant à la norme 802.11<sup>42</sup>. Le succès rencontré par le WiFi provient de la possibilité de créer des réseaux locaux sans fil à haut débit pour des ordinateurs situés à proximité d'une borne d'accès. Dans la pratique, le WiFi permet de relier des ordinateurs portables, des ordinateurs de bureau, des tablettes tactiles ou tout type de périphérique à une liaison haut débit sur un rayon allant de plusieurs dizaines de mètres à plusieurs centaines de mètres en environnement extérieur. Si le WiFi présente plusieurs avantages incontestables, au premier rang desquels on trouve une mobilité accrue pour les utilisateurs, ainsi qu'une interopérabilité des équipements. Il convient néanmoins de connaître les risques inhérents à son utilisation.

De par sa nature intrinsèque (la transmission radio électrique sur une plage de fréquence de 2,4 GHz) tout individu équipé du matériel adéquat peut détecter la présence d'un réseau, à l'aide de logi-





## Rémy FÉVRIER

ciels intégrés de pénétration, le plus souvent disponibles librement sur Internet (par exemple la suite Backtrack fonctionnant sous Linux<sup>43</sup>). La pénétration des systèmes WiFi est devenue, depuis quelques années – suivant en cela le succès croissant rencontré par ce type de réseau – le « sport » favori d'un nombre toujours croissant de hackers et de nombreuses entreprises en ont déjà fait les frais : la captation d'un réseau WiFi est relativement aisée et demeure à la portée de n'importe quel amateur – même non éclairé – suffisamment opiniâtre.

Sans rentrer dans les détails techniques relatifs au cryptage des données transitant sur un réseau WiFi, on ne peut que constater la vulnérabilité de ce type de vecteur : il existe des outils gratuits qui permettent de découvrir la clé de chiffrement en quelques minutes. On trouve très facilement ces outils en effectuant une simple recherche sur Internet : de nombreux logiciels sont ainsi mis à la disposition des hackers, que ce soit en termes de détection des réseaux sans fil ou de pénétration du système. On peut même trouver un mode d'emploi de conception d'une antenne WiFi surpuissante à partir d'une boîte de conserve de grande taille ! Il nous est arrivé, dans le cadre de nos fonctions, d'utiliser sur un réseau de test des outils de hacking directement accessibles sur le web. Nous avons réussi à casser le cryptage dans la plupart des cas en un temps compris entre une dizaine de minutes à un peu plus d'une heure en fonction du cryptage

utilisé. Une sécurisation optimale d'un système WiFi nécessite donc de prendre de nombreuses précautions d'ordre technique.

### La gestion des mots de passe

Les services de la collectivité doivent obligatoirement disposer d'une visibilité complète sur l'attribution et le suivi des mots de passe des serveurs (mots de passe super-utilisateur ou « root ») et des progiciels spécialisés, y compris en cas de délégation de service et d'infogérance. Même dans le cas d'une supervision de réseau par un prestataire, la collectivité doit conserver, en permanence, une certaine maîtrise de l'attribution ou du moins du recensement de ces mots de passe, a fortiori lorsque certains d'entre eux donnent accès à d'importantes bases de données d'informations à caractère personnel.

En cas de consultation de sites ou de forums illégaux, la responsabilité de l'Elu pourra être engagée si ce dernier n'a pas explicitement pris un minimum de mesures indispensables à la saine utilisation de l'Internet au sein de ses services. Certaines collectivités territoriales mettant gracieusement à disposition de leurs administrés des bornes WiFi en libre service, il est pareillement impératif de procéder à un verrouillage fin des sites consultables, sous peine de graves surprises du fait du caractère anonyme de la consultation publique et par conséquent de l'impossibilité de remonter jusqu'à l'utilisateur occasionnel du service.



## Toujours plus cyber-menacées : les collectivités territoriales

### • Une supervision insuffisante de l'architecture

La gestion, par les collectivités territoriales, de la sécurité de leurs réseaux recoupe des situations très diverses, selon la taille de ces organisations, le budget consacré à la SSI et surtout l'implication des strates de direction en matière de SSI. Alors même que l'administration quotidienne d'un SI répond à un ensemble de normes et de procédures extrêmement précises, il arrive néanmoins que certaines règles de base soient oubliées, ce qui ne peut que concourir à la vulnérabilité de l'infrastructure globale.

### Structure des réseaux

Le premier document que l'on doit pouvoir consulter dans le cadre d'un SI de taille conséquente demeure invariablement le Schéma Directeur Informatique (SDI).

### Le Schéma Directeur Informatique

Ce SDI, qui a pour but de récapituler l'ensemble des structures constituant l'intégralité du SI jusqu'à dans les plus infimes détails inclut simultanément un inventaire exhaustif des matériels et technologies employés, ainsi qu'une présentation précise de la logique globale ayant présidé à l'élaboration du SI.

L'absence de SDI structuré peut porter indirectement atteinte à la collectivité car il demeure une référence indispensable, à

la fois en termes de compréhension globale et de suivi du SI, mais également par le fait qu'il constitue intrinsèquement une mesure objective de la rigueur avec laquelle a été menée l'installation du réseau ainsi que de la pertinence de ses évolutions ultérieures.

### Du plan de câblage au Plan de Continuité Informatique

Parallèlement au SDI, la tenue scrupuleuse d'un plan de câblage retracant l'ensemble des goulottes et chemins de câbles existant au sein des bâtiments est rendue indispensable par la nécessité de disposer d'une vision immédiate de la cohérence de l'infrastructure, qui sera de nature à permettre des interventions rapides et ciblées en cas de rupture de continuité du signal. Un plan d'adressage récapitulant l'ensemble des adresses physiques et logiques des postes de travail doit conjointement permettre de suivre les modifications successives apportées au fil du temps. De surcroît, le service en charge de la supervision du réseau informatique doit posséder un Plan de Continuité Informatique (PCI), décomposé en procédures distinctes et successives, permettant de procéder – en un temps minimal – à la remise en service de l'ensemble du SI en cas de « down » accidentel. Si l'élaboration de ce PCI demeure une tâche complexe et fastidieuse, elle apparaît néanmoins indispensable à la pérennité du SI dans la mesure où l'activité d'une collectivité territoriale ne peut plus se



## Rémy FÉVRIER

concevoir sans flux informatiques et un simple dysfonctionnement de ceux-ci prend immédiatement des proportions fâcheuses, voire catastrophiques.

### La gestion des risques

La culture du risque demeure encore peu développée au sein des collectivités territoriales, que ce soit en interne ou vis-à-vis de prestataires extérieurs à qui l'on confie encore trop souvent la responsabilité de la gestion quotidienne du SI sans en exiger le minimum de précautions indispensables à la sécurisation des données.

### Maîtrise de l'infogérance

Les organisations modernes ayant tendance à rationaliser leur gestion en se rentrant sur leurs processus métiers fondamentaux (Chabrol, Feniès et al., 2006), il en résulte un recours de plus en plus important à des prestataires extérieurs en ce qui concerne les fonctions de support. À ce titre, de nombreuses collectivités territoriales qui ne disposent pas, en interne, des ressources indispensables au bon fonctionnement de leur SI, font appel à des sociétés d'infogérance. Or, le fait de confier à un prestataire extérieur la gestion de son réseau informatique constitue une décision lourde de la part de la collectivité en raison du caractère éminemment sensible des données échangées et stockées. Le choix d'un infogérant nécessite de prendre un certain nombre de précautions allant de la rédaction d'une clause de confidentialité

sévère à la vérification de la qualité des services proposés.

### Une insuffisante culture du risque

Le seul risque informatique réellement appréhendé par les agents correspond, la plupart du temps, aux attaques virales d'origine externe : bien que n'ayant qu'une vision parcellaire des modes opératoires et des dégâts potentiellement engendrés, ces derniers les considèrent néanmoins comme les principales menaces encourues par un SI. L'approche des agents des collectivités territoriales diffère assez peu de celle de leurs homologues du secteur privé : la vision qu'ils ont des vulnérabilités du SI tourne beaucoup plus autour de la notion d'attaque d'origine extérieure que de maladresses ou dysfonctionnements liés à de mauvaises pratiques internes.

Cette inconscience des impératifs minimaux de sécurisation des SI ne peut qu'induire de graves dysfonctionnements futurs, dans la mesure où la sécurité d'un SI n'est, sinon parfaite, du moins optimale, que lorsque l'ensemble des utilisateurs du réseau ont une vision claire des différentes menaces pouvant affecter celui-ci.

## 3. Les 3 défis numériques des Collectivités Territoriales

La mise en place de l'administration électronique constitue l'un des principaux



## *Toujours plus cyber-menacées : les collectivités territoriales*

défis numériques auxquels sont aujourd’hui confrontées les collectivités territoriales. Au contact direct des administrés, elles sont soumises à une volonté gouvernementale récurrente de profiter d’une diffusion sans cesse croissante des TIC afin de proposer aux citoyens une meilleure efficience administrative.

### *• L’administration électronique*

Si l’on se réfère à la définition de l’Organisation de Coopération et de Développement Economiques (OCDE), l’administration électronique représente « l’usage des technologies de l’information et de la communication et en particulier de l’Internet en tant qu’outils visant à mettre en place une administration de meilleure qualité ». Même si certains États sont plus avancés que d’autres en ce domaine, on observe aisément que la réflexion sur l’utilisation administrative des TIC n’est pas nouvelle et constitue une constante source d’intérêt depuis la diffusion d’Internet auprès du grand public.

### Une évolution des processus de gestion

La première approche relative à l’Internet fut essentiellement constituée autour des infrastructures de transport numérique : la notion « d’autoroute de l’information » émerge rapidement et le gouvernement français a pris relativement tôt conscience des futurs bouleversements que ne manquerait pas de provoquer une large diffusion des nouvelles technologies de l’information au sein de l’ensemble de la société.

### Historique

La première impulsion est venue du Premier Ministre Alain Juppé, qui a insisté sur le rôle déterminant de l’Internet en tant que passerelle vers la modernité. La circulaire du 15 Mai 1996<sup>44</sup> pose clairement la nécessité, pour une France « pionnière de la télématique » de relever les nouveaux défis liés à l’impact grandissant des TIC. Les administrations deviennent, à ce titre, des acteurs majeurs de diffusion et les initiatives menées doivent dorénavant se placer dans un cadre structurant, afin d’éviter redondances et incohérences.

### L’apport d’Internet : du PAGSI au RE/SO

Rapidement, les nouvelles possibilités offertes par le réseau Internet deviennent des thèmes de débats médiatiques et les TIC émergent sur l’agenda politique en tant que vecteurs d’évolutions économiques et sociétales. Dès lors, les choses vont s’accélérer et le Premier Ministre Lionel Jospin poursuivra l’œuvre de son prédécesseur, preuve que l’émergence de la société de l’information constitue un sujet de préoccupation essentiel qui transcende les clivages. Le Programme d’Action Gouvernemental pour la Société de l’Information (PAGSI), créé en 1998, constituera ainsi le fer de lance de la volonté gouvernementale de faire pénétrer la France dans un XXI<sup>e</sup> siècle numérique. Plusieurs axes de développement sont définis, allant de l’équipement des établissements d’enseignements en matériel informatique à une meilleure efficacité des administrations



## Rémy FÉVRIER

publiques, en passant par la diffusion de la culture française à l'étranger ou l'incitation à l'investissement privé dans les TIC.

Ce programme se révèlera au final comme une remarquable réussite qui constituera le socle de multiples actions ultérieures à l'image du portail de l'administration française (2000), au travers duquel les contribuables se voient proposer, pour la première fois, la possibilité de remplir leurs déclarations de revenus en ligne. Pour autant, ce premier pas vers l'administration électronique est souvent freiné par des résistances internes<sup>45</sup>, contrecoups inévitables à toute remise en cause des habitudes de travail au sein de grandes structures, paradigme majeur de la socio-logie des organisations<sup>46</sup>.

44

Surmontant ces résistances, une deuxième étape est franchie, en 2002, au travers de la mise en place du plan RE/SO 2007 (pour une REPUBLIQUE numérique dans la Société de l'information). Ce plan s'oriente plus spécifiquement vers la dématérialisation des procédures administratives et une nouvelle structure est créée afin de rapprocher les SI des différentes administrations et mener des projets concrets de modernisation en interministériel : l'Agence pour l'Administration Electronique (ADAE). Un objectif quantitatif est même fixé à chaque ministère : la dématérialisation de deux procédures par an avant l'année 2005. La poursuite de ces objectifs sera encore encouragée par le

rapport « Hyper-République : bâtir l'administration en réseau autour du citoyen » (De La Coste, 2003)<sup>47</sup> qui préconisera que l'ADAE ait pour objectif de « favoriser la standardisation et l'interopérabilité, de coordonner et de mutualiser les initiatives des services publics en matière d'administration électronique ».

### Le programme ADELE

Toutefois, c'est au travers de l'engagement du Président de la République Jacques Chirac, à l'occasion de la présentation de ses vœux aux corps constitués le 7 janvier 2004, que l'impulsion définitive est donnée. En effet, peu de temps après, le Premier Ministre Jean-Pierre Raffarin présentera un plan ambitieux de développement de l'administration électronique. D'après lui « les technologies de l'information et de la communication sont un outil particulièrement efficace pour la modernisation de l'administration. Les usagers, personnes physiques ou entreprises, doivent en être les premiers bénéficiaires. Ces technologies permettent, en effet, non seulement de faciliter l'accomplissement matériel des formalités, notamment par la mise à disposition de téléprocédures, mais aussi de proposer de véritables services personnalisés, utilisables pour un ensemble de démarches »<sup>48</sup>. Le programme gouvernemental ADELE (ADministration ELEctronique 2004/2007) doté d'une ligne budgétaire de près de 2 milliards d'euros, doit permettre à la France de rattraper son retard, notamment en matière d'informatisation des administrations.



## *Toujours plus cyber-menacées : les collectivités territoriales*

Un Plan Stratégique de l'Administration Electronique (PSAE) sur 4 ans (2004-2007) est adopté avec pour objectif de constituer un véritable schéma directeur interministériel entièrement dédié à la mise en place et la diffusion de l'administration électronique ; le Plan d'Action de l'Administration Electronique (P2AE), en coordonnera la mise en place au travers de projets innovants : dématérialisation de l'état civil, création de la carte d'identité électronique, mise en place d'un portail unique des services publics... C'est à cette période que les premiers rapprochements avec les collectivités territoriales verront le jour.

Depuis 2005, l'ADAE est devenue une sous-direction de la Direction Générale de la DGME, qui regroupe plusieurs services interministériels auparavant indépendants. La DGME a pour mission de moderniser les modes de fonctionnement de l'État au travers de la définition de règles applicables à l'ensemble des services publics en matière de gestion électronique. La mise en place, en 2007, de la Révision Générale des Politiques Publiques (RGPP) ayant érigé le développement de l'administration électronique au rang de priorité, de nombreuses initiatives sont en cours en matière de dématérialisation des procédures en direction de l'usager. Ainsi, de plus en plus de services sont dorénavant proposés en ligne : paiement de la TVA, déclarations de revenus<sup>49</sup>, plans cadastraux, annonces de marchés publics, formalités de création d'entreprises...), le point d'orgue de ce bouquet étant sans conteste le site

mon.service-public.fr mis en ligne en janvier 2009.

L'administration électronique est aujourd'hui une réalité qui représente un enjeu d'avenir pour les collectivités territoriales : leur proximité avec les citoyens, ainsi que leur rôle de gestionnaires des services publics locaux, imposent de prendre la mesure des améliorations à attendre, ainsi que des incontournables contraintes sous-jacentes.

### Enjeux et objectifs

Au-delà des attentes fortes exprimées par les citoyens internautes, l'administration électronique répond conjointement à plusieurs enjeux politico-sociétaux, à l'instar de la lutte contre la fracture numérique. La réalisation de ces objectifs est intimement liée à une forte implication conjointe des administrations de l'État et des collectivités territoriales.

### Une demande croissante

Avant d'évoquer les attentes des français en matière d'administration électronique, il convient de s'interroger préalablement sur le succès que rencontrent les TIC au sein de la société française. Selon un sondage réalisé en 2008 par la société IPSOS<sup>50</sup> et consacré aux habitudes des français en matière d'utilisation d'Internet, il apparaît que plus des 3/5<sup>e</sup> des français sont internautes et en matière d'usage d'Internet, force est de constater que la réalisation de



Rémy FÉVRIER

démarches administratives arrive dorénavant au 4<sup>e</sup> rang en termes d'utilisation d'Internet, ce qui indique que les efforts consentis en matière d'administration électronique rencontrent un écho favorable de la part du public connecté.

Cette impression est renforcée par les résultats d'une enquête réalisée la même année par l'institut TNS Sofres, pour le compte de la société Capgemini Consulting<sup>51</sup> : depuis 2006, la France se stabilise à un taux élevé de connexion aux services publics (76%), ce qui correspond à une progression de 11 points en 5 ans. On constate également un incontestable phénomène de fidélisation des « internautes publics » avec un taux de 23% en 2008, ce qui représente un gain de 4 points par rapport à 2003. La satisfaction des utilisateurs des sites publics est manifeste dans la mesure où, globalement, le taux de satisfaction des internautes français s'établit autour de 80% en 2008 et ce, indépendamment du critère de qualité retenu (fonctionnement des sites, étendue des services disponibles, qualité des informations...), à l'exception de celui de rapidité de la réponse à une demande en ligne, ce dernier demeurant néanmoins aux alentours de 70%. En terme quantitatif, l'enquête annuelle du CREDOC intitulée « Conditions de vie et aspirations des Français » fait apparaître que plus de 21 millions de français ont eu recours à Internet pour mener à bien des démarches administratives ou fiscales en 2008<sup>52</sup>.

46

Les internautes se connectent plus volontiers sur des sites offrant des services pratiques à l'utilisateur (site impots.gouv.fr, sites des mairies et organismes publics locaux, sites des services sociaux...) que sur de simples portails informatifs et l'administration électronique apparaît de plus en plus comme une sorte de guichet électronique où les usages interactifs prédominent. En procédant à une analyse comparative des résultats entre 2003 et 2008, il apparaît que les motivations des internautes sont avant tout d'ordre pratique : éviter de se déplacer (+20 pts), ne pas être tributaire des horaires d'ouverture administrative (+14 pts), gagner du temps par rapport à une correspondance épistolaire (+10% pts), etc.

Au vu des résultats présentés, il est indéniable que l'administration électronique, en plus de représenter une formidable opportunité, se situe également au cœur d'une dynamique plus large conjuguant disponibilité et interactivité des services publics.

#### La recherche d'une nouvelle efficience administrative

L'enjeu majeur de l'administration électronique revient à permettre une mutation des relations traditionnelles entre l'administration et des usagers. Toutefois, au-delà du consensus existant à ce propos, les obstacles à la réalisation de cet objectif sont encore nombreux et la mise en place de services électroniques adaptés nécessite, avant tout, une solide connaissance des rouages administratifs et une refonte



## *Toujours plus cyber-menacées : les collectivités territoriales*

des circuits et processus en vigueur. Si l'informatique a depuis longtemps intégré le champ administratif, c'était surtout en tant qu'outil de production essentiellement tourné vers la recherche d'une nouvelle efficacité interne et non en direction du public. Progressivement, on va assister, notamment au travers du projet ADELE, à une évolution des priorités vers une meilleure prise en compte des attentes de l'usager : ce que les sciences de gestion qualifient de « front office ».

Cette révolution copernicienne ne s'est pas réalisée aussi facilement que l'on aurait pu l'espérer car il est rapidement apparu illusoire de vouloir mettre en place une nouvelle approche orientée « client » sans procéder à une véritable réingénierie des procédures administratives. Il s'agit là d'une tâche difficile, rendue d'autant plus indispensable que les critères de stabilité budgétaire auxquels la France a souscrit impliquent un impératif de réduction des coûts et la recherche d'une meilleure productivité globale.

Or, si l'utilisation des nouvelles technologies en matière de flux sortants a été plutôt bien acceptée par les administrations, en tant que vitrine de leur activité quotidienne (portail web essentiellement explicatifs, podcasts...), il n'en fut pas toujours de même en ce qui concerne la consolidation d'informations en provenance de l'extérieur et les nouveaux impératifs de traitements qui en résultaien. Peu à peu, la logique a prévalu et au-

jourd'hui, de plus en plus d'administrations disposent de site web résolument interactifs et directement orientés vers la satisfaction finale de l'usager. L'internaute dispose dorénavant d'un ensemble de services accessibles 24h sur 24h à l'ergonomie satisfaisante. Néanmoins, au-delà de la simple mise à disposition de formulaires et de textes administratifs le web administratif doit permettre à l'usager de dépasser la simple notion de téléchargement de documents ou de consultation informationnelle, pour investir également le champ de l'applicatif interactif lui permettant d'engager un véritable dialogue avec l'administration, à propos de tel ou tel sujet sur lequel il souhaite obtenir des informations précises et officielles.

47

Il semble qu'une dynamique se soit enclenchée, qui devrait logiquement contribuer à offrir au citoyen-internaute des services administratifs plus efficaces et plus soucieux de ses besoins et interrogations. Cependant, des efforts sont encore à fournir en matière d'interopérabilité entre les différents services et les différentes strates administratives. En effet, la contrepartie du développement relativement rapide des TIC au sein des administrations est l'extrême hétérogénéité des plateformes matérielles utilisées et des protocoles techniques choisis.

### Réduction de la « fracture numérique »

En dépit de la forte diffusion des TIC et de l'Internet chez les ménages français, il



## Rémy FÉVRIER

48

apparaît que la notion de « fracture numérique » n'est pas une vue de l'esprit : l'ancienne dichotomie existante entre ceux qui avaient accès à l'information et ceux qui en étaient exclus – au sens figuré du terme – se retrouve aujourd'hui entre les adeptes d'Internet et ceux qui n'en font pas usage. Plusieurs facteurs discriminant apparaissent nettement, aux premiers rangs desquels le niveau de diplôme et l'âge de l'utilisateur.

L'étude précédente montre que le recours à Internet découle souvent du niveau des diplômes dont dispose l'individu. On relève, à ce propos, un écart de 58 points entre les diplômés de l'enseignement supérieur et ceux qui sont dépourvus de tout diplôme. Ceci se double par une forte corrélation entre l'âge et l'utilisation d'Internet, les plus jeunes constituant la grande majorité des internautes. Il est vrai que les plus jeunes générations sont littéralement nées avec Internet : on peut approximativement dater le début de la démocratisation de l'accès à Internet (via des modems externes à faibles débits disponibles pour une connexion personnelle) aux années 1994-1995, ce qui est extrêmement récent et constitue une deuxième évolution technologique et sociétale majeure dans la droite ligne de la diffusion de l'informatique personnelle du milieu des années 1980, avec l'apparition du Personal Computer® d'IBM et du Macintosh® Apple II.

À cela s'ajoute l'impact des Catégories Socio-Professionnelles (CSP) : la profes-

sion du chef de ménage apparaît déterminante puisque l'écart est de plus de 30 points entre les cadres et les ouvriers : les individus les plus élevés socialement ont une tendance naturelle à utiliser Internet, vraisemblablement du fait d'une capacité à mieux appréhender l'outil et surtout à le maîtriser plus aisément. Les personnes défavorisées sont, elles aussi, exclues de l'accès à l'Internet sans qu'il s'agisse là d'un choix volontaire, c'est l'absence de ressources suffisantes qui leur interdit l'usage des nouvelles technologies et cette situation est rendue d'autant plus dommageable pour ces personnes, qu'elles ont souvent des rapports extrêmement fréquents avec l'administration et gagnaient, par conséquent, à disposer de moyens efficaces de liaison avec cette dernière.

Le niveau de diplôme, l'âge et la profession du chef de ménage modèlent pareillement le recours à l'administration électronique. Sachant qu'il convient également de prendre en considération l'accessibilité des sites aux personnes handicapées, ce qui nécessite une prise en compte d'un fort aspect ergonomique lors de la conception des portails web afin de ne pas pénaliser ces personnes dans leur légitimes aspirations à bénéficier, comme tout un chacun, des avantages d'une nouvelle proximité avec les services publics. À ce titre, la question de la diffusion du haut débit apparaît cruciale, a fortiori lorsque l'on sait que les nouveaux sites et portails administratifs cherchent de plus



## *Toujours plus cyber-menacées : les collectivités territoriales*

en plus à tirer partie de l'ensemble des opportunités offertes par l'évolution des technologies, nécessitant de fait des disponibilités toujours plus élevées en matière de bandes passantes. À ce titre, le Président Nicolas Sarkozy a spécifié qu'il considérait comme primordial d'atteindre en 2010 l'objectif des 70% de ménages français équipés d'un ordinateur et permettre à chacun de disposer d'un accès au haut débit fixe et mobile avant 2012<sup>53</sup>.

Les enjeux liés à l'administration électronique sont multiples, allant de la recherche d'économies budgétaires – recherche d'une meilleure efficience –, au renforcement de la confiance entre les usagers et leurs administrations. Face à cela, les collectivités territoriales se retrouvent en première ligne, de par leur proximité immédiate avec les citoyens. À ce titre, elles sont le meilleur relais des administrations centrales, en même temps qu'un échelon indispensable et représentent la possibilité, pour les administrés, de disposer de bouquets de services administratifs conjuguant proximité, réactivité et connaissance de l'environnement social.

### Implication des collectivités territoriales

Au-delà d'un simple rôle d'accompagnement des efforts nationaux de mise en place d'une administration électronique performante, les collectivités territoriales, en tant que « prestataires » de services administratifs, tout autant que par leur rôle de structuration et de développement ter-

ritorial, doivent s'approprier intimement les enjeux et opportunités liés au développement de l'E-administration, afin d'en faire un outil de gestion quotidienne et d'optimisation de la relation avec l'administré-citoyen, dans une véritable approche partenariale avec l'ensemble des administrations de l'État.

### Des collectivités au contact

Les internautes français ont parfaitement compris les divers avantages découlant de l'appropriation, par l'administration, des hautes technologies, mais contrairement à ce que l'on pourrait intuitivement supposer, la mise en place de l'administration électronique ne représente pas, pour ces derniers, le bannissement de tous rapports « *intuitu personae* » avec les fonctionnaires, mais bien plutôt une indispensable contribution à l'émergence d'un nouvel « espace-temps » administratif.

### Des attentes fortes

Parallèlement aux nouvelles opportunités offertes par la mise en place de téléprocédures à l'échelon national (déclaration de revenus en ligne...), les usagers de l'administration électronique n'en oublient pas pour autant les e-services de proximité. À ce titre, les attentes demeurent fortes en direction des collectivités territoriales, puisque 76% des internautes interrogés considèrent la disponibilité en ligne des services administratifs locaux (carte d'identité, permis de conduire, état civil...)





Rémy FÉVRIER

comme prioritaires. Les portails administratifs locaux ont donc vocation à devenir de plus en plus des guichets en ligne accessibles 24h sur 24 et permettant d'éviter au requérant actif de perdre une partie de son week-end dans une file d'attente.

Pourtant et peut-être doit-on considérer cela comme un symptôme de l'attachement au « service public à la française », les internautes demeurent très attachés à la persistance de ces mêmes guichets administratifs, puisque 45% d'entre eux considèrent que le guichet électronique et l'accueil physique des personnes ont vocation à coexister, voire que l'accueil physique des personnes restera le mode de contact privilégié entre les citoyens et les administrations. Ce tropisme, non dénué d'une légère schizophrénie, conduit néanmoins à rassurer les tenants de l'utilisation des nouvelles technologies en tant que vecteurs d'optimisation du service rendu et non comme vecteur unique, à moyen terme, de la relation directe entre le citoyen et l'administration.

La notion de proximité, qu'elle soit humaine ou géographique demeure un archétype constant de « l'inconscient administratif » national et, à ce titre, les collectivités territoriales se trouvent confortées dans leur rôle d'intermédiation de premier niveau entre l'usager et l'administration. Il leur incombe donc de mettre en place des portails et services performants à destination de leurs administrés tout en cherchant à inciter au maximum

ces derniers à utiliser ces nouveaux types de services en répondant à leurs interrogations, en matière d'ergonomie ou de confidentialité des données échangées.

### Une structuration difficile

Si les collectivités territoriales ne sont pas restées inactives, relativement à l'émergence de l'administration électronique, l'exemple est incontestablement venu de l'État et les actions menées en local ont directement résulté de cette impulsion nationale. De nombreuses collectivités ont fait preuve de volontarisme, le plus souvent sous l'impulsion directe et récurrente d'un exécutif convaincu de l'intérêt de faire profiter le citoyen des bienfaits des nouvelles technologies dans ses rapports avec l'administration territoriale. Pour autant, toutes n'ont pas montré le même dynamisme et la situation demeure aujourd'hui contrastée entre celles qui agissent résolument en faveur de la diffusion de l'administration électronique et celles qui se contentent de suivre ce mouvement avec une certaine appréhension devant l'ampleur de la tâche.

Si 85% des collectivités de plus de 100.000 habitants déclaraient mener des projets liés à la mise en place de l'administration électronique en 2008<sup>54</sup>, ces derniers sont conduits sans véritable concertation et cette multitude d'initiatives se révèle souvent décevante en termes de résultats, eu égard au temps et aux efforts consentis.



## *Toujours plus cyber-menacées : les collectivités territoriales*

Pour tenter de rationaliser l'ensemble de ces initiatives, il convient de définir le plus précisément possible l'objectif à atteindre, afin de faire coïncider au mieux les projets en cours avec les attentes des citoyens, mais aussi des collectivités. À ce titre, le concept de guichet unique représente une piste intéressante en tant que portail regroupant l'ensemble des services administratifs électroniquement disponibles selon le principe de subsidiarité. Les collectivités territoriales, fortes de leur proximité immédiate avec les citoyens, pourraient devenir le point de passage obligé vers une administration électronique dynamique et performante et bénéficier, de fait, d'aides substantielles au titre d'une contribution majeure à la modernisation de l'État.

### Une diversification des services

La quantité des services « proposables » aux citoyens est théoriquement aussi étendue que les tâches administratives assignées aux collectivités. Ces dernières ne pourront toutefois assumer une réelle maîtrise de l'administration électronique qu'à la condition de conduire celle-ci progressivement, tout en respectant des priorités préalablement définies. L'appropriation progressive et la gestion, par les collectivités, de la complexité des impératifs consubstantiels à l'E-administration s'effectuera d'autant plus facilement que l'accent sera mis sur des items combinant, à la fois, maîtrise technique des dossiers traités, intérêt pour l'État d'un traitement décentralisé de l'information et désidératas des administrés.

À ce sujet, les résultats d'une étude réalisée en 2008 à la demande de la Direction Générale de la Modernisation de l'État<sup>55</sup>, offre quelques pistes de réflexion : il apparaît que les préoccupations prioritaires des collectivités territoriales s'articulent autour de la fréquence des démarches effectuées, du savoir-faire de la collectivité, ainsi que du nombre d'usagers concernés. Afin d'optimiser les chances de réussite d'une telle démarche, on peut envisager de regrouper les démarches en trois types : l'inscription à des prestations et services, les demandes de renseignements administratifs et les formalités à caractère personnel.

Les prestations de services : les collectivités territoriales, au premier rang desquelles les communes, assurent la majeure partie des services publics de proximité proposés aux citoyens, spécialement en ce qui concerne les prestations liées à l'environnement familial et éducatif. Les démarches relatives à ces services sont le plus souvent répétitives, selon une périodicité propre : annuelle pour les inscriptions en crèches, bimestrielle pour les centres de loisirs... La majeure partie des demandes d'inscription aux services municipaux pourraient s'effectuer en ligne : inscription en crèches, à la cantine, aux centres aérés, aux bibliothèques, aux activités sportives... Trop souvent encore, les parents de jeunes enfants consacrent, en début de rentrée scolaire, une ou plusieurs demi-journées à patienter dans des files d'attentes interminables qui, en plus de





## Rémy FÉVRIER

nécessiter une présence physique de leur part (traitement des dossiers selon la logique du « premier arrivé-premier servi»), induit un coût conséquent pour les municipalités en termes de paiement d'heures supplémentaires à des agents spécialement requis à cet effet.

Un dispositif de traitement en ligne de ces inscriptions ne peut, toutefois, légitimement s'envisager sans mise à disposition de bornes dédiées à destination de ceux qui ne disposent pas de connexion à Internet sous peine de provoquer une distorsion inconcevable en termes d'accès aux services publics. Et pour permettre à ce genre de dispositif une efficacité optimale, il convient d'envisager simultanément la détermination et l'application automatique du quotient familial (sous réserve de vérification ultérieure), ainsi que le paiement en ligne des prestations souhaitées. Ce traitement numérique pourrait également s'envisager en matière de demandes d'aides sociales.

Les demandes de renseignements administratifs : une autre spécificité des collectivités territoriales réside dans le nombre croissant de renseignements devant être mis à disposition des administrés en cas de demande expresse. Le traitement informatisé de ces demandes constituerait un gain de temps et de disponibilité conséquent pour les fonctionnaires territoriaux, a fortiori pour tout ce qui relève du domaine de l'urbanisme et de la fiscalité locale : demande de permis de construire,

consultation du Plan Local d'Urbanisme ou simulation de calcul des taxes et im- pôts locaux... Le coût d'un tel système se- rait vraisemblablement amorti en quelques années pour autant qu'il s'accompagne d'un véritable effort de formation et de ré- organisation des procédures internes et du redéploiement des personnel concernés vers des activités plus valorisantes.

Les formalités à caractère personnel : les demandes d'actes administratifs font également partie des sollicitations quoti- diennes adressées aux collectivités et l'as- pect récurrent de leur gestion en font un domaine particulièrement approprié à un traitement dématérialisé initial. Il en va ainsi des fiches personnelles et familiales d'état civil, des certificats de mariage ou de décès, des extraits d'actes de naiss- ance... À l'image du casier judicaire na- tional qui dispose, depuis plusieurs années, d'un serveur dédié à la délivrance épistolaire des bulletins personnels n°3, un nombre croissant de communes s'appro- prient un tel procédé afin d'optimiser l'ef- ficacité des réponses apportées tout en évitant aux usagers de consacrer une par- tie de leur temps libre à ces demandes.

### Des expérimentations réussies

De nombreuses collectivités ont lancé d'ambitieux programmes d'administration électronique. Si beaucoup d'entre elles éprouvent des difficultés à maîtriser cor- rectement les impératifs liés aux coûts ainsi qu'aux contraintes intrinsèquement



## *Toujours plus cyber-menacées : les collectivités territoriales*

liées à la gestion de tels projets, il n'en demeure pas moins que certaines réussites remarquables émergent et permettent de demeurer confiant quant à l'objectif final d'une vaste diffusion de l'E-administration. À ce propos, il apparaît intéressant de comparer plusieurs initiatives, menées sous l'impulsion de conseils régionaux soucieux de permettre aux citoyens de disposer de véritables portails de services administratifs en ligne et aux collectivités d'envisager plus sereinement le déploiement de ces derniers, au travers d'une mutualisation rassurante.

### E-Mégalis Bretagne

En pays Breton, la diffusion de l'administration électronique a été imaginée autour d'un syndicat mixte. Crée en 1999, E-Mégalis Bretagne est une structure fédérative qui a la particularité de regrouper 77 membres, représentant l'ensemble des structures territoriales existantes : le Conseil régional, les quatre Conseils généraux, 9 communautés d'agglomération, 1 communauté urbaine, 59 communautés de communes et trois villes (Dinard, Landerneau et Quiberon). Depuis sa création, E-Mégalis a eu pour vocation de permettre à l'ensemble des établissements publics de bénéficier d'un accès Internet à haut débit identique sur l'ensemble du territoire du syndicat. À ce titre, il a mis en œuvre une offre de services de télécommunications à haut débit, à laquelle plus de 2500 établissements publics ont été raccordés.

Ses missions allant de l'accompagnement des membres jusqu'à l'incubation de projet, en passant par une activité d'acheteur de service, ce syndicat mixte a créé, en 2006, une plateforme régionale d'administration électronique, ainsi qu'un guichet unique de services dématérialisés au profit des collectivités, selon un principe de coopération territoriale et de mutualisation des moyens. Fort de ses premières réussites, E-Mégalis s'est vu fixer de nouveaux objectifs comme l'adaptation des outils d'administration électronique aux attentes des usagers en termes de simplification et de rapidité, ainsi qu'une recherche de synergies potentielles, susceptibles de contribuer à la réduction de la dépense publique.

### E-Bourgogne

La même volonté de développer l'administration électronique et de permettre un développement harmonieux des TIC sur les territoires se retrouve en Bourgogne où, depuis 4 ans, E-Bourgogne expérimente, avec l'État, le Conseil régional, les 4 Conseils généraux et plus de 1300 collectivités et établissements publics locaux, une plate-forme régionale d'administration électronique. Après la mise en place d'une salle des marchés publics et d'un espace unique d'aides aux entreprises, E-Bourgogne mène de nouvelles actions plus spécifiques en matière de dématérialisation : la gestion électronique des actes soumis au contrôle de légalité, l'archivage électronique légal et plus largement les





## Rémy FÉVRIER

télé-procédures et les e-services destinés aux citoyens, sous la forme de services directement intégrés dans les portails web des collectivités, afin de constituer un guichet électronique d'information et de gestion des démarches administratives.

Le choix d'E-Bourgogne consiste à proposer des solutions de valorisation des sites Internet « clés en mains » à des collectivités ainsi dégagées des impératifs liés à la conception et la réalisation d'un portail web. Celles-ci peuvent choisir entre plusieurs styles visuels et disposent d'un éditeur de contenu permettant d'assembler les pages et de les mettre à jour aisément. Au-delà de cette mise à disposition d'informations, ces solutions permettent également de disposer d'e-services et de téléprocédures prêts à l'emploi et directement intégrables au site Internet et offrent un large éventail de services administratifs en ligne : obtention d'extraits d'acte de naissance ou encore possibilité d'effectuer une pré-inscription scolaire. L'idée générale d'E-Bourgogne est de proposer souplessse et adaptabilité aux collectivités au travers de la mise à disposition de modules adaptés à leurs besoins, tout en déchargeant des problématiques de conception et de développement, afin que ces dernières puissent se concentrer in fine sur le contenu des services offerts au public.

### Réseau Villes et Villages Numériques

La région Nord-Pas-de-Calais n'est pas en reste en matière de développement de

l'administration électronique, puisque sur les 1548 communes que compte la région, 430 disposaient d'un site Internet en 2008, soit 28% et ce taux monte à 67% pour les EPCI<sup>56</sup>. Parmi les projets ayant vu le jour, on peut signaler l'initiative « Réseau des Villes et Villages Numériques » (RVVN), lancée en 2001 sous l'impulsion des villes de Valenciennes, Cambrai et Douai. Constituant l'arc sud de la région, RVVN réunit six EPCI représentant une population totale de 510.000 habitants et propose aux communes de s'inscrire dans une démarche globale d'appropriation des TIC par les collectivités, y compris les plus rurales ou de taille modeste.

Cette volonté de démocratisation des nouvelles technologies se traduit concrètement par l'existence d'une plateforme Internet personnalisée à destination des collectivités, au travers de laquelle celles-ci disposent de la possibilité de promouvoir leur patrimoine respectif et de mieux communiquer avec les citoyens. La mise à disposition des communes de modules interactifs leur permet d'envisager plus sûrement la maîtrise des outils d'administration électronique. L'accompagnement assuré par RVVN dans le déploiement des solutions choisies est de nature à séduire de petites collectivités dont les Elus sont peu à l'aise avec les TIC et demeuraient, jusqu'alors, méfiant à l'égard des outils de l'administration électronique.

Ces exemples, aussi emblématiques soient-ils, ne constituent pas l'essentiel



## *Toujours plus cyber-menacées : les collectivités territoriales*

des projets menés par des collectivités territoriales en vue de faire progresser l'administration électronique : la DGME a recensé plus de 4000 initiatives de collectivités dans ce domaine sur l'ensemble du territoire national. Si l'on peut se féliciter de cette prise en main de l'E-administration par les collectivités territoriales, il apparaît aujourd'hui indispensable de mettre l'accent sur une certaine mutualisation et une mise en cohérence avec les projets issus de l'État afin d'éviter d'être confronté, le moment venu, à une mosaïque de systèmes autonomes. Une expansion équilibrée de l'administration électronique est directement corrélative de la prise en compte, par les collectivités, du respect de certains usages techniques et opérationnels lourds dont la mise en place implique souvent une mutualisation des outils.

### Défis & contraintes

Les enjeux liés au déploiement de l'administration électronique sont complexes et dépassent de beaucoup la simple maîtrise technique ou l'adoption de nouvelles méthodes de management local. C'est un domaine où la crédibilité des services proposés apparaît directement liée à la notion d'interopérabilité et de sécurisation des échanges électroniques. Les citoyens modernes, encouragés en cela par les polémiques récentes concernant l'anonymat réel des informations disponibles sur Internet, ne se contentent plus de disposer d'un canal d'échange direct, mais reven-

dissent, de surcroit, une certaine ergonomie d'utilisation et surtout la garantie de voir des informations relatives à leur vie privée, bénéficier des dernières innovations en matière de sécurisation des flux numériques. Les collectivités territoriales se retrouvent donc au confluent de préoccupations multiples, allant de la satisfaction de l'usager final à la nécessaire imbrication des services proposés, dans une perspective plus large de modernisation de l'État.

### Objectifs et moyens

Les premières contraintes auxquelles sont confrontées les collectivités souhaitant développer l'administration électronique sont d'ordre stratégique et organisationnel. La gouvernance d'un tel dessein implique à la fois un large consensus interne et une vision claire de l'ensemble des variables dont l'évolution pourrait durablement impacter le projet.

### Un sujet consensuel

La mise en place de l'administration électronique fait partie des sujets à propos desquels on peut légitimement s'attendre à trouver un certain consensus de la part de l'ensemble des Élus locaux. L'objectif étant d'améliorer les services rendus aux usagers, la définition d'un programme de déploiement d'E-administration doit transcender les divergences de vues et permettre à l'ensemble des Élus de s'approprier le projet.



## Rémy FÉVRIER

56

Cette adhésion des exécutifs locaux s'avère indispensable à la réalisation finale du projet, notamment du fait des fortes implications de celui-ci en termes d'organisation du travail et des interactions verticales (vers l'État) et horizontales (vers les autres collectivités) qu'il engendre. Or, on peut constater que si l'ensemble des Elus locaux appréhende complètement la nécessité d'adapter leur collectivité respective aux nouvelles réalités techniques et sociales, certains d'entre eux demeurent circonspects à l'égard de systèmes d'échanges qui bouleversent les rapports traditionnels avec les administrés. Face à cette situation paradoxale, il convient de favoriser une approche consensuelle faite d'écoute et de respect mutuel, afin de sanctuariser les actions menées et d'assurer leur pérennité. Cet objectif suppose d'éviter de sombrer dans un technicisme de mauvais aloi : la mise en place d'un SI dédié à l'administration électronique doit être considérée comme un véritable vecteur de développement global de la collectivité.

La définition et le déploiement d'une solution d'administration électronique doivent donner lieu à une gestion en mode projet rigoureuse, à la fois en termes de coûts et de structuration. Les projets d'informatisation sont souvent sous-estimés par les collectivités et l'on arrive finalement à d'importantes dérives financières. Pour éviter cet écueil, il sera utile de faire appel à des compétences spécifiques en matière de gestion de projet, que ce soit

au travers de recrutements temporaires ou d'externalisation de la maîtrise d'ouvrage. La première étape du planning consiste à établir une liste exhaustive des partenaires potentiels et des parties prenantes du projet : collectivités, services de l'État, sociétés spécialisées...afin d'élaborer avec eux l'infrastructure globale et ses implications territoriales et administratives. À l'issue de cette évaluation, la charge financière devra faire l'objet d'une évaluation la plus précise possible pour chaque partenaire, afin d'en déduire l'adéquation avec les possibilités de financement existantes (ainsi que de réfléchir à l'éventualité de bénéficier d'aides spécifiques en provenance de diverses instances en charge du développement).

Par la suite, le choix du prestataire revêtira une importance singulière selon que l'on optera pour une Société de Services et d'Ingénierie en Informatique (SSII ou SS2I) ou une plateforme publique. En tout état de cause, le choix du prestataire final devra répondre à plusieurs problématiques lourdes :

Une connaissance approfondie du secteur des collectivités territoriales ainsi que de leur mode de fonctionnement ;

La connaissance de leurs obligations en matière de collecte et de traitement de l'information ;

Et une perception adéquate de l'ensemble des interactions existantes avec les



## *Toujours plus cyber-menacées : les collectivités territoriales*

services de l'État et d'éventuelles initiatives locales analogues.

Enfin, l'état d'avancement du projet devra faire l'objet d'une communication régulière et transparente, y compris dans ses aspects budgétaires et ceci afin de corriger d'éventuels dysfonctionnements ponctuels sans compromettre sa réalisation finale.

### E-administration et management des processus

Au-delà des aspects pratiques de définition des besoins et de déploiement, la mise en place d'un projet d'administration électronique se double d'un autre enjeu structurel : la nécessité de repenser le management des processus de gestion administrative. En effet, la proximité virtuelle induite par une utilisation judicieuse des nouvelles technologies permet, non seulement d'optimiser la qualité des relations entre l'administration et l'usager, mais aussi d'envisager une refonte complète des processus métiers de la part des administrations concernées. C'est pourquoi, il convient d'impliquer, très en amont, l'ensemble des services directement concernés ainsi que les services transverses, au premier rang desquels la Direction des Ressources Humaines. La résistance au changement demeurant une règle de base de toute structure humaine, il convient de faire en sorte que l'administration électronique fasse l'objet d'un large consensus, même si ce prérequis est de nature à re-

tarder le calendrier initial. Il est naturel que des agents voient avec une certaine inquiétude une évolution portant en elle-même d'importants bouleversements relativement à une façon de travailler ancienne et bien ancrée dans les habitudes.

Une réelle appropriation de l'E-administration par les agents chargés de la faire vivre au quotidien et de gérer cette interactivité nouvelle avec l'usager constitue un de ses facteurs clés de succès. L'implication des agents doit être une réalité et ne pas se limiter à des séances d'informations périodiques. Le management de projet doit laisser une large place à la concertation et à l'écoute dans le double objectif de rassurer les personnels et de prendre en compte toute piste d'amélioration proposée ou toute difficulté soulevée. Ce processus d'accompagnement du changement nous semble cautionner, au moins autant que la solution technique retenue ou le vecteur de communication envisagé, la réussite finale du projet et surtout sa pérennité en tant que vecteur d'évolution majeure de l'administration territoriale.

### Cohérence des projets d'E-administration

A plus grande échelle, on observe que beaucoup de projets de déploiement de l'administration électronique se heurtent à une absence de cohérence en matière de suivi de projet. Bien que les tâches et obligations des différents acteurs administra-



## Rémy FÉVRIER

tifs locaux soient théoriquement clairement établies par les textes, on assiste régulièrement à des chevauchements d'offres et de services, dont la complexité est de nature à nuire fortement à l'efficacité recherchée. Pour éviter de tels désagréments, une gouvernance globale du projet doit être favorisée, au travers de la mise en cohérence de l'ensemble des initiatives menées sur un territoire donné, afin d'optimiser de rechercher des synergies potentielles, tout en cherchant à optimiser les ressources financières nécessaires (appels d'offres globaux, réduction des coûts de sous-traitance, mutualisation des ressources techniques et humaines...).

58

Comme le font justement remarquer les responsables du site edile.fr, portail dédié aux collectivités territoriales, « le développement de l'administration électronique ne saurait être conçu en dehors d'une véritable logique partenariale. Il ne saurait non plus souffrir de tentations de gestions hiérarchiques entre entités publiques »<sup>57</sup>. Les projets d'administration électronique doivent donc faire l'objet d'une « concertation territoriale » entre l'ensemble des collectivités d'un même territoire, ainsi qu'avec les administrations de l'État, souvent destinataires des informations collectées auprès des citoyens. Si la mutualisation des ressources dans une logique partenariale a présidé à la mise en place des plateformes de services préalablement évoquées, ces expériences demeurent néanmoins encore exceptionnelles au

regard de l'abondance de projets d'E-administration menés aujourd'hui sur le territoire. Il est donc essentiel de faire preuve de patience et de pédagogie vis-à-vis de collectivités sincèrement désireuses d'améliorer la qualité des services rendus aux administrés, sans toujours en évaluer clairement l'ensemble des implications.

### Des contraintes structurelles

Face au foisonnement d'initiatives locales en matière d'administration électronique, l'État a élaboré un certain nombre de critères et de contraintes à respecter afin d'éviter, d'une part, une trop grande hétérogénéité technologique et d'autre part, promouvoir un accès égal pour tous à cette nouvelle forme de gestion administrative.

### Respect des standards techniques

Pour faciliter la mutualisation des moyens et susciter une cohérence nouvelle dans le déploiement de l'administration électronique sur le territoire, l'État a défini certaines recommandations d'ordre technique et organisationnel au travers de référentiels élaborés par la DGME. Ces documents énoncent un certain nombre de règles et de critères à respecter lors de la conception d'un bouquet de services électroniques.

### L'accessibilité

Le premier référentiel concerne l'accessibilité des sites dédiés à l'administration



## *Toujours plus cyber-menacées : les collectivités territoriales*

électronique et découle directement de l'application de la loi du 11 février 2005 relative à « l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées »<sup>58</sup>, qui fait de l'accessibilité une exigence pour l'ensemble des services de communication publique en ligne de l'État, des collectivités territoriales et des établissements publics qui en dépendent. Ce référentiel, intitulé Référentiel Général d'Accessibilité pour les Administrations (RGAA)<sup>59</sup>, s'inspire des travaux menés sur le plan international pour améliorer l'accessibilité des contenus de sites Internet : le WCAG 2.0 (Web Content Accessibility Guidelines 2.0)<sup>60</sup>. L'objectif de ce document est de permettre aux 5,5 millions de personnes atteintes d'une invalidité en France et d'une manière générale à tout internaute, quel que soit son équipement ou ses aptitudes physiques ou mentales, d'accéder aux sites web publics sans perte d'informations. Cela passe par de substantiels efforts en termes d'ergonomie, dont la création d'alternatives textuels à l'ensemble des contenus audio et vidéo proposés sur les sites. Ce RGAA est schématiquement structuré autour de quatre principes fondamentaux :

La perceptibilité : Les informations doivent être disponibles en plusieurs formats, sans perte d'information ni de structure.

L'ergonomie : L'ensemble des fonctionnalités inhérentes aux sites doivent être simultanément accessibles par un dispositif

de pointage et directement depuis le clavier.

La lisibilité : Les contenus doivent être univoques et facilement compréhensibles.

La robustesse : L'accès aux sites devra être pérennisé, y compris en cas de changement de matériel informatique chez l'utilisateur final, afin de ne pas restreindre la connectivité de ce dernier.

Contrairement aux efforts menés en matière d'accessibilité physique aux services et bâtiments publics, la notion d'accessibilité aux portails web n'est pas encore complètement rentrée dans les mœurs et nécessite effectivement une prise en compte par les collectivités dès le lancement d'un projet, dans la mesure où il est bien plus confortable de prendre en compte l'ensemble des contraintes techniques dès la phase d'élaboration du projet, plutôt que de devoir développer des modules supplémentaires une fois le produit terminé, avec le risque d'être soumis à une forte dérive des coûts initiaux.

### L'interopérabilité

Le deuxième référentiel mis en place par la DGME est consacré à l'interopérabilité entre les différents systèmes utilisés par l'État et les collectivités territoriales. L'importance apportée à la notion de compatibilité entre les systèmes découle directement du foisonnement d'initiatives en provenance des services de l'État et des





Rémy FÉVRIER

60

## Sécurisation des échanges

À l'instar des interrogations sur la sécurité des sites web commerciaux, la question de la sécurisation des transferts d'informations engendrée par l'E-administration est au cœur des préoccupations des usagers : en 2008 les risques de piratage d'informations confidentielles sont devenus le premier obstacle à l'utilisation des services publics sur Internet (+13 points en 4 ans)<sup>62</sup>. Cet état de fait est symptomatique de l'importance que revêt dorénavant la sécurité de SI de plus en plus intégrés à la vie sociale et personnelle des individus. Consciente du développement du tropisme des collectivités territoriales pour l'administration électronique, la CNIL demeure particulièrement vigilante à cet égard et propose, sur son site<sup>63</sup>, des

collectivités. Sans pour autant aller jusqu'à définir des normes précises ou préconiser des solutions logicielles ou techniques, le Référentiel Général d'Interopérabilité (RGI)<sup>61</sup> vise à élaborer un cadre de référence élaboré à partir de normes et de standards internationaux faisant l'objet d'un large consensus, afin de faciliter l'échange de données entre les SI des administrations françaises, comme entre le secteur public au sens large et les administrés. Il se place résolument dans une perspective européenne, puisqu'il a également pour objectif de favoriser le développement de services européens en ligne et la coopération entre les administrations des États membres.

La DGME, consciente des conséquences néfastes que pourraient avoir des failles de sécurité sur l'avenir de l'administration électronique, a mis au point, avec la l'Agence Nationale de la Sécurité des Systèmes d'Informations (ANSSI)<sup>64</sup>, un remarquable Référentiel Général de Sécurité (RGS). Si ce document est extrêmement complet et vise un objectif beaucoup plus large que la seule sécurisation des traitements liés à l'E-administration, il constitue néanmoins un outil complet à la disposition des DSI. Il permet d'appréhender l'ensemble des problématiques liées à la SSI :

Disponibilité de l'information ;

Intégrité de l'information ;

Confidentialité des données ;

Authentification de l'auteur ;

Traçabilité des actions effectuées sur les données.

Les recommandations prévues dans ce référentiel en font un élément incontournable de tout projet de portail web administratif. S'il ne dispense pas de faire appel



## *Toujours plus cyber-menacées : les collectivités territoriales*

à des compétences techniques spécifiques, il permet néanmoins de disposer d'un véritable manuel de sécurité et d'homogénéisation des bonnes pratiques de SSI, contribuant ainsi à la standardisation des outils d'administration électronique.

### Avantages escomptés

La définition de Référentiel Général d'Interopérabilité a fait l'objet d'une évaluation, par la DGME, en matière d'impact sur le développement de l'administration électronique. Selon cette dernière, le respect des normes contenues dans le RGI devraient notamment se traduire dans les faits par :

#### L'amélioration de la qualité de service

L'interopérabilité devrait permettre une meilleure efficacité administrative en permettant aux administrés de bénéficier des dernières évolutions techniques, afin de faciliter leurs relations quotidiennes avec les différentes administrations. Sachant que la définition de standards communs devrait accélérer les phases de conception et d'intégration des systèmes.

De surcroît, le fait d'utiliser les mêmes normes constitue une source d'économie pour les équipes chargées du déploiement d'un projet car cela évite de se poser la question éminemment délicate de la compatibilité entre les systèmes. De plus, la référence à des normes externes permet pareillement aux partenaires de limiter les

coûts liés à la réalisation de développements spécifiques et permet de standardiser les connectivités existantes.

#### Une convergence dans un cadre plus vaste

L'utilisation d'un langage commun permet à l'ensemble des acteurs (usagers, collectivités, administrations) de mieux se comprendre. Le respect de normes d'interopérabilité permet potentiellement aux administrations de rapprocher leurs SI respectifs, a fortiori dans un futur cadre d'interopérabilité européen : une quinzaine d'États européens développent actuellement leur propre cadre d'interopérabilité, ainsi que la Commission Européenne pour les applications transfrontalières (European Interoperability Framework).

#### Le respect de l'autonomie des acteurs

Si les recommandations du RGI constituent les objectifs à atteindre, les moyens d'y parvenir sont intégralement laissés aux responsables. Si la notion d'interopérabilité est source de diffusion de l'administration électronique et des services rendus, il n'en demeure pas moins que les normes choisies n'imposent aucune solution technique et leur qualité fait l'objet d'un vaste consensus international.

L'accessibilité des sites et l'interopérabilité des systèmes sont indispensables au développement de l'administration électronique, mais son appropriation définitive





## Rémy FÉVRIER

tive par les citoyens demeurera consubstantielle de la certitude qu'auront les internautes que ce nouveau mode de transmission d'informations relatives à leur vie personnelle est totalement sécurisé, ce qui est encore loin d'être toujours le cas aujourd'hui.

Les collectivités territoriales ont également à gérer une deuxième mutation bouleversant leurs rapports avec leurs administrés et qui dépasse le strict cadre des rapports administratifs : l'E-démocratie.

- *La E-Démocratie*

62

Le concept de démocratie électronique (E-démocratie), bien que plus polémique qu'il n'y paraît de prime abord, semble devoir s'imposer comme un des nouveaux vecteurs d'engagement citoyen. Largement encouragée par des instances européennes soucieuses de favoriser un renouveau démocratique, l'E-démocratie ne peut s'établir durablement qu'au travers de son appropriation par les collectivités territoriales. Or, à l'image de l'administration électronique, l'E-démocratie nécessite des investissements humains et technologiques, a fortiori en termes de SSI, souvent hors de portée de nombreuses collectivités locales.

### Le concept de démocratie électronique

Si on associe progrès technologique et participation démocratique, force est de

constater que ce lien s'est singulièrement renforcé depuis la fin de la seconde guerre mondiale et l'apparition, puis la diffusion, de l'informatique. Aujourd'hui, le concept même de démocratie électronique a été pris en compte par de nombreuses collectivités en tant que piste d'amélioration de la participation démocratique. Ainsi, si l'on se réfère au constat établi par la structure spécialisée DREAM+, mise en place par la région Nord-Pas-de-Calais relativement à l'action régionale en matière de nouvelles technologies et de démocratie territoriale, il s'avère que « les tendances vont dans le sens de la participation citoyenne : évolution du cadre incitatif légal, développement de la notion de gouvernance, pressions citoyennes de plus en plus fortes pour avoir un droit de regard et de parole concernant la décision publique... »<sup>65</sup>.

### Une attention soutenue

Devenue partie intégrante de la recherche en sciences politique et sociale, cette nouvelle « forme » de démocratie fait également l'objet d'une attention réelle au niveau international. On peut mentionner, à ce titre, l'étude menée par l'OCDE qui expose clairement, dans son introduction, le caractère dorénavant incontournable des TIC en matière de participation citoyenne : « Tous les membres de l'OCDE ont conscience que les nouvelles technologies de l'information et de la communication sont de puissants instruments pour renforcer la participation des citoyens à l'élaboration des politiques »<sup>66</sup>.



## *Toujours plus cyber-menacées : les collectivités territoriales*

### Les 3 « Âges » de la démocratie électronique

Afin de mieux comprendre l'importance prise par cette nouvelle approche, il est indispensable d'en tracer la genèse : si l'on se réfère aux travaux de T. Vedel relatifs aux origines et à l'évolution de la démocratie électronique<sup>67</sup>, il est possible de distinguer trois « Âges » successifs de la démocratie électronique, correspondant à trois époques traversées d'évolutions sociétales différentes, voire divergentes :

La période allant de la fin de la deuxième guerre mondiale à la fin des années soixante est marquée par une forte intervention de l'État et l'apparition du management public. Ces années se caractérisent par une approche extrêmement rationnelle de l'État vis-à-vis de la société dans son ensemble. C'est l'époque où la conduite des affaires publiques est synonyme de pilotage scientifique, favorisée en cela par la montée en puissance de l'ordinateur et des architectures informatiques centralisées.

Les années 1970 et 1980, qui constituent une ère de contestation sociale et de remise en cause des institutions politiques centralisées. De cette période date le retour en force du niveau local et de la décentralisation. Ce mouvement centrifuge étant accompagné d'une modernisation de la démocratie représentative, au travers d'une meilleure relation entre les citoyens et leurs Élus.

Depuis le début des années 1990, la mondialisation a induit beaucoup d'inter-

rogations sur le devenir des États-nations et provoqué une montée en puissance de l'individualisme et des valeurs libérales. Parallèlement à cela, on a vu apparaître une certaine transformation des liens sociaux qui se poursuit et s'amplifie à l'heure actuelle, au travers de l'apparition des communautés virtuelles. Le citoyen devient un « individu pleinement autonome au sein d'un espace public globalisé ».

Cette évolution, même si elle a été largement influencée par plusieurs facteurs exogènes importants, montre toutefois qu'Internet se trouve à la croisée des chemins en termes de participation à la vie démocratique.

### Des approches divergentes

Aujourd'hui, deux approches globales peuvent être envisagées relativement à l'utilisation des TIC et notamment d'Internet, en tant qu'outils de démocratie électronique : la première consiste à considérer les nouvelles technologies comme un moyen parmi d'autres de recherche d'une démocratie plus « contributive » de la part du citoyen.

### Internet comme « contribution » démocratique

C'est cette approche qui a prévalu à la création et la mise en place des comités de quartier ou des commissions extra-municipales. Cette approche revient à considé-





## Rémy FÉVRIER

rer Internet comme un simple vecteur de circulation de l'information permettant, de surcroit, un gain de temps incomparable par rapport à l'utilisation des moyens traditionnels de communication avec le citoyen.

Pour illustrer cette conception des choses, T. Vedel (2003) évoque l'exemple très poussé d'une ville de la banlieue de Londres qui, utilisant Internet comme outil au service d'une politique institutionnelle, s'appuie sur un dispositif très conséquent d'écoute et de recueil de la parole citoyenne : jury composé de seize administrés représentant la diversité de la ville pour émettre un avis sur les questions de criminalité – y compris les trafics de stupéfiants –, commission de quartiers en charge des problèmes locaux, panel de 1000 citoyens tirés au sort et consultés sur les décisions à prendre. Il convient, à ce propos, d'observer que les anglo-saxons sont très friands de cette possibilité d'établir un lien avec les administrés. Peut-être doit-on voir là une illustration supplémentaire de la notion culturelle de « communauté » à l'image de leur concept de « community policing » dans le domaine de la sécurité.

### Internet vecteur de « mutation démocratique »

L'autre approche revient à considérer le réseau Internet comme portant intrinsèquement les germes d'une nouvelle forme de démocratie : à la fois vecteur et cata-

lyseur, son originalité serait de constituer potentiellement une vaste « Agora » virtuelle au sein de laquelle chaque citoyen pourrait contribuer à l'élaboration des politiques publiques. Cette vision, en prenant bien garde à ne pas sombrer dans des considérations excessives visant à élaborer une alternative – pour le moins hasardeuse et non dénuée de dangers – à la démocratie représentative, postule l'émergence d'un nouveau « rapport de force entre gouvernants et gouvernés ». Ce changement de paradigme se traduirait par un « renouveau démocratique » au travers de l'appropriation par l'ensemble des citoyens, des enjeux politiques et économiques les impactant à court et moyen terme. La considération sous-jacente à cette théorie réside dans une volonté naturelle et récurrente des citoyens de s'approprier les enjeux de leur époque, volonté constamment contrariée par l'impossibilité de disposer des informations nécessaires préalablement aux choix finaux effectués par les assemblées délibérantes.

Selon les partisans de la démocratie électronique, Internet dispose de plusieurs caractéristiques susceptibles d'améliorer la qualité de l'espace public<sup>68</sup> :

C'est un lieu de liberté et d'authenticité où chaque individu peut s'exprimer sincèrement sans crainte d'une quelconque censure et de manière égalitaire sans considération de statut social ou de diplômes.



## *Toujours plus cyber-menacées : les collectivités territoriales*

C'est un lieu qui transcende les frontières géographiques ou sociales, permettant la mise en relation d'individus n'ayant a priori qu'une faible probabilité de se rencontrer et d'échanger effectivement dans la vie réelle.

C'est un lieu de compréhension mutuelle où l'on peut confronter librement ses idées et partager des expériences et approches différentes.

C'est un lieu générateur de lien social et de création d'identités collectives, à l'image des réseaux sociaux fédérant des groupes plus ou moins larges de personnes.

C'est un lieu d'auto-régulation soumis à un ensemble de règles de courtoisie et de bienséance : la « Net-étiquette » empêchant des débordements préjudiciables à la qualité des débats.

Sans vouloir troubler les tenants d'une démocratie électronique pure et sans entraves, qu'il nous soit ici permis de douter quelque peu quant au caractère effectif des bienfaits évoqués : cette vision nous semble empreinte d'un grand optimisme, aussi bien relativement à l'impact réel d'Internet en matière de comportements sociaux, qu'en termes de qualité des échanges induits.

Entre idéalisation et déni de légitimité

La mise en place de la démocratie électronique doit incontestablement s'accom-

pagner d'une réflexion préalable qui, tout en tenant compte de l'appétence réelle ou supposée des citoyens pour ce genre d'innovation démocratique, nécessite une prise de recul salutaire relativement à certains présupposés sociaux de nature à provoquer, finalement, une grande confusion dommageable à la crédibilité du processus.

### Une opinion réceptive

Si on en croit Pierre Rosanvallon (2006) « le développement des formes d'implication des citoyens dans les décisions qui les concernent est l'un des traits majeurs de l'évolution récente des régimes démocratiques [...] Ils veulent voir leurs opinions et leurs intérêts plus concrètement et plus continûment pris en compte »<sup>69</sup>. Dans le cadre de ce constat, Internet devrait théoriquement constituer une aubaine pour tous les citoyens soucieux de participer plus activement à la vie de la Cité et au suivi des textes les concernant. À ce propos, un sondage effectué par l'Institut Opinionway pour le Forum mondial de la démocratie et de l'administration électronique (World E-Gov Forum)<sup>70</sup> tend à confirmer cette hypothèse. Il apparaît ainsi que près de 80% des personnes interrogées considèrent que la France est plutôt en retard en matière d'E-démocratie alors même que la demande d'être consulté sur l'ensemble des sujets concernant la conduite des affaires de l'État est forte : de 57% pour la politique de Défense à 76% pour l'avenir du système de santé en pas-



## Rémy FÉVRIER

66

sant par l'avenir de l'École (72%) ou la réforme des Institutions (66%).

Les personnes interrogées considèrent également, à une forte majorité, qu'Internet est un bon moyen d'améliorer le fonctionnement de la démocratie (78%) et de réconcilier les citoyens avec leurs Élus (59%). Ce phénomène n'est pas nouveau, mais il s'est clairement accentué au cours des dernières années : cette enquête ayant été réactualisée à plusieurs reprises, on peut constater une progression de la prise en compte d'Internet comme vecteur démocratique, notamment auprès des jeunes de moins de 25 ans qui sont les plus demandeurs de dialogue avec leurs Élus. Cette tendance devrait encore s'accentuer corrélativement à l'importance toujours croissante que prennent les TIC dès le plus jeune âge : la grande majorité des écoles élaborent des cours d'éveil à l'information pour des enfants de plus en plus jeunes et qui disposent, le plus souvent, de la possibilité de s'exercer à la maîtrise d'Internet chez eux, accompagnés par leurs parents.

Nonobstant l'idée d'utiliser Internet comme vecteur démocratique, il paraît nécessaire de nuancer quelque peu une vision par trop embellie et optimiste de l'image du citoyen-internaute.

### Une certaine idéalisation

L'utilisation d'Internet comme instrument majeur d'un nouveau schéma démo-

cratique présuppose l'existence intrinsèque d'un internaute au profil particulier, cumulant idéalement un nombre de qualités personnelles assez impressionnantes, allant du civisme le plus développé à une large maîtrise des problématiques, en passant par un souci de l'intérêt général transcendant ses propres intérêts particuliers.

La principale objection que chercheurs et universitaires apportent à la notion de démocratie électronique réside dans l'image idéalisée du citoyen-internaute car l'idée de démocratie électronique, au sens le plus prononcé du terme, repose sur l'existence d'une majorité de citoyens soucieux de s'impliquer personnellement dans la vie politique et exclusivement freinés par un déficit structurel d'informations, rejoignant en cela la vision théorique développée par certains philosophes du 19<sup>e</sup> siècle, comme Locke ou Tocqueville. Aujourd'hui, un simple survol de l'évolution des taux d'abstention aux différentes élections depuis plus d'une trentaine d'années suffit à mettre à mal cette vision idéale. L'accélération de la vie sociale, associé à une disponibilité informationnelle de plus en plus grande sont de nature à réduire considérablement le nombre, déjà restreint, d'internautes correspondant à ce profil très particulier.

Comme l'a très pertinemment établi Anne Le Bot<sup>71</sup>, une implication optimale d'un citoyen en matière de partie prenante de la démocratie virtuelle se heurte, dans les faits, à plusieurs obstacles bien réels :



## *Toujours plus cyber-menacées : les collectivités territoriales*

### Des obstacles techniques

L'anonymat : Internet offre à ses utilisateurs la possibilité de masquer leur identité lors de discussions sur des forums participatifs : bien qu'il soit possible de s'enregistrer sous son vrai nom, il suffit de créer un pseudonyme pour pouvoir dialoguer avec les autres membres. On peut légitimement s'interroger sur la crédibilité finale d'un participant préférant se cacher derrière un alias pour échanger des points de vue.

La surabondance d'informations : La quantité d'informations disponibles sur le réseau mondial est telle que le fait de souhaiter disposer d'un point de vue exhaustif sur un sujet implique un considérable effort de synthèse, ainsi qu'un recul substantiel relativement aux opinions et idées exprimées.

Le référencement : Si le nombre d'opinions et de points de vue disponible est souvent colossal, il n'en demeure pas moins que l'internaute est tributaire de la sélection automatique opérée par les moteurs de recherche lorsqu'il effectue une requête de recherche d'informations sur un sujet. Il existe systématiquement là une dichotomie entre la pertinence réelle de l'information et son rang de présentation, selon le principe de référencement qui priviliege souvent la notion de popularité ou de visitorat au détriment de la pertinence réelle, alors même qu'une grande majorité des internautes ont uniquement recours à la première page de résultats affichés par

un moteur de recherche et que la quasi-totalité ne va jamais au-delà de la troisième page.

La circulation d'idées : Comme les membres d'une association de type Loi de 1901, les internautes intéressés par un sujet ont tendance à se regrouper aux travers de réseaux sociaux, ou de communautés virtuelles spécialement créées autour de leur thème de prédilection. Comme dans tout groupe structuré, leurs membres vont avoir tendance à rechercher une meilleure visibilité, afin de peser au maximum sur le débat public en cours. Cette recherche d'influence s'effectuera au détriment direct de « cyberecitoiens » isolés et minoritaires qui auront, conséquemment, bien plus de difficultés à faire émerger des arguments contradictoires dans le sens où, ils devront réaliser les efforts indispensables à se faire préalablement reconnaître en tant qu'interlocuteurs légitimes, avant même de participer au débat en lui-même.

### Des prérequis individuels

En plus de ces écueils d'essence technique, la participation idéale d'un internaute à la démocratie électronique est également soumis à plusieurs prérequis cognitifs majeurs, déterminant une personnalité devant cumuler certains traits de caractères et caractéristiques précises :

La disponibilité : Dans l'absolu, l'internaute qui souhaite résolument s'engager dans le cadre de la démocratie électro-



## Rémy FÉVRIER

nique doit pouvoir disposer du temps nécessaire pour collecter, trier puis analyser des données, quelquefois contradictoires mais toujours abondantes. Ces étapes indispensables à la compréhension globale d'une problématique et de l'ensemble de ses enjeux sous-jacents potentiels sont spécialement chronophages et encore ne s'agit-il ici que d'une préhension raisonnable du sujet. Il conviendra ensuite de consacrer également du temps à la discussion, au questionnement des pouvoirs publics et à la confrontation d'idées avec l'ensemble des parties prenantes.

68

La culture et l'esprit d'analyse : En plus de nécessiter du temps, la phase de recherche, d'interprétation et de synthèse des informations disponibles (a fortiori sur un thème incluant des considérations d'ordre technique : urbanisme, transports, fiscalité...) implique de réelles connaissances ainsi qu'une maîtrise consommée en matière d'analyse puis de synthèse. Ces dispositions, sans – fort heureusement – demeurer hors de portée, favorisent, en tout cas a priori, à la fois les internautes ayant suivi des études universitaires et ceux qui sont confrontés aux mêmes tâches dans le cadre de leur activité professionnelle quotidienne, sachant que le taux de corrélation entre ces deux catégories est assez élevée.

Une abnégation certaine : Théoriquement, la participation de l'internaute-citoyen à la démocratie électronique suppose un sens particulièrement aigu de

l'intérêt collectif : ce dernier ne doit rechercher que le triomphe de l'intérêt général sur la somme des intérêts personnels, ce qui s'avère nécessairement beaucoup plus complexe lorsque ce dernier est, de près ou de loin, partie prenante du débat en cours...

La somme des prérequis évoqués permet de relativiser la vision très favorable des tenants de la démocratie électronique en tant que terreau d'un renouveau démocratique radical. Au-delà de la critique de cette vision, de nombreux Elus se posent la question légitime du risque de voir les citoyens internautes chercher à excessivement influencer l'action de représentants ayant reçu l'onction du suffrage universel et dont l'action, inscrite dans la durée, est néanmoins régulièrement soumise à la sanction des urnes.

### De réelles interrogations

Afin d'éviter de cautionner un débat politique sans rapport avec notre sujet, nous évoquerons les appréhensions relatives à la démocratie électronique comme faisant partie d'interrogations sociologiques plus vastes quant à la légitimité d'une démocratie plus participative. Nous nous appuierons à ce propos sur une récente étude du Centre d'Analyse Stratégique (CAS) qui, au-delà de constituer une remarquable synthèse des réflexions menées à ce propos selon les époques<sup>72</sup>, permet de comprendre en quoi l'apparition d'Internet a ravivé certaines craintes et in-



## *Toujours plus cyber-menacées : les collectivités territoriales*

terrogations quant à la possibilité d'une évolution dans le système démocratique représentatif.

### Des critiques récurrentes

Un des premiers penseurs à avoir théorisé la différence entre le système démocratique des anciens (au sens Athénien du terme) et son évolution moderne est Benjamin Constant qui voyait l'indépendance individuelle comme le premier des besoins contemporains et pour qui des institutions reposant sur le concept de démocratie directe n'était pas viable dans le cadre d'une démocratie moderne, dans le sens où le système représentatif constitue une organisation par laquelle une nation tend ni plus ni moins qu'à se décharger sur quelque uns de ce qu'elle ne veut ou ne peut pas faire elle-même. Cette critique du manque d'appétence pour la chose publique trouve un prolongement sous une forme bien différente mais néanmoins complémentaire chez Joseph Schumpeter pour qui « le citoyen typique, dès qu'il se mêle de politique, régresse à un niveau inférieur de rendement mental [...] Il redevenant un primitif. Sa pensée devient associative et affective »<sup>73</sup>. Selon lui, la notion de démocratie revient globalement à la capacité qu'a le peuple « d'accepter ou d'écartier les hommes appelés à le gouverner ».

La confiance en la capacité qu'auraient les citoyens de se mêler plus directement des affaires de l'État se trouve également

fortement minorée chez Emile Durkheim dont la réflexion sur la démocratie place le savoir au rang de notion primordiale, ou chez Max Weber, pour lequel de fortes interrogations demeurent quant à la capacité du peuple de disposer de la compétence démocratique indispensable au suivi des affaires publiques. La critique la plus achevée à l'égard de la distinction entre le peuple et ses représentants revient à Pierre Bourdieu pour qui le domaine politique, à l'image du champ religieux, se caractérise par « une coupure entre les professionnels et les profanes ». Si la science politique estime généralement que la démocratie directe est aujourd'hui tout simplement inapplicable eu égard à la taille du corps électoral et à la complexité des affaires politiques, certains chercheurs tentent néanmoins de pousser plus avant la réflexion sur la possibilité d'émergence d'une véritable démocratie directe. On peut citer à ce propos Loïc Blondiaux (2008) qui porte un regard plus nuancé sur le sujet et cherche à réellement mettre en perspective les avantages et les inconvénients de la démocratie participative.

### Une synthèse raisonnable

Tout en reconnaissant une certaine justesse aux réserves émises sur la démocratie participative – fondement sur lequel repose le concept d'E-démocratie – on peut vraisemblablement effectuer un changement de perspective et considérer, avec René Sève<sup>74</sup> que « plutôt que d'en



## Rémy FÉVRIER

70

faire une panacée, mieux vaut considérer qu'elle constitue un registre complémentaire de la démocratie représentative ». En effet, loin d'effacer la démocratie représentative, une démocratie électronique bien conçue et pourvue des garde-fous adéquats peut, à contrario, y insuffler une dynamique nouvelle. En tout état de cause, comme le rappelle Stephen Coleman<sup>75</sup> « Le gouvernement et les Elus ne doivent pas rester à l'écart des initiatives de démocratie en ligne. Ils doivent apprendre à mieux les comprendre, à y participer et à y réagir. Ils doivent reconnaître que l'interactivité démocratique implique une circulation d'énergie dans les deux sens. Sinon, le public verra dans les initiatives de démocratie en ligne une imposture et se retirera... ». Et ce, d'autant plus que certaines expériences ont montré que de simples citoyens, interrogés sur une politique publique déterminée, peuvent tout à fait énoncer des pistes d'actions pertinentes, pour peu que le système mis en place soit performant et bien parfaitement structuré<sup>76</sup>.

Les initiatives de démocratie électronique sont le plus souvent menées par des collectivités territoriales dans la mesure où celles-ci sont considérées comme étant les plus « proches » du citoyen. En dépit du soutien de l'Union Européenne, on constate que la mise en place des outils et portails nécessaires à ces consultations nécessite simultanément méthode dans l'organisation générale et vigilance en matière de sécurité informatique.

### Collectivités territoriales et E-démocratie

Les collectivités territoriales apparaissent généralement comme l'échelon le plus pertinent en matière de mise en place d'initiatives d'E-démocratie. Cela tient essentiellement à leur proximité avec le citoyen, ce qui constitue l'un des archétypes forts de la science politique. C'est aussi le niveau auquel il est le plus aisément de tisser des liens avec les administrés, notamment dans le cas des communes et des EPCI.

### Europe et démocratie participative

La mise en place d'une meilleure participation des citoyens se trouve clairement encouragée par les instances européennes, au premier rang desquelles le Conseil de l'Europe. Ainsi, la Résolution 1121 (1997) de l'Assemblée parlementaire du Conseil de l'Europe, relative aux instruments de la participation des citoyens dans la démocratie représentative, affirme que : « une démocratie véritable et vivante dépend du concours actif des citoyennes et des citoyens. Leur participation à la vie politique et leur coopération au sein des institutions politiques est ainsi un facteur déterminant pour le bon fonctionnement des institutions démocratiques ».

### Des collectivités territoriales fortement sollicitées

Dans cette perspective, les collectivités territoriales se voient mises en avant en tant que maîtres d'ouvrage de cette volonté participative : la Recommandation



## *Toujours plus cyber-menacées : les collectivités territoriales*

N°R (96) 2 du Comité des Ministres concernant les référendums et les initiatives populaires au niveau local rappelle que : « ... le droit des citoyens de se prononcer sur des choix importants qui engagent l'avenir pour une longue période ou portent sur une décision difficilement réversible intéressant une majorité de citoyens fait partie des principes démocratiques communs à tous les États membres du Conseil de l'Europe ». Puis elle ajoute : «... c'est au niveau local que ce droit peut être exercé le plus directement et qu'il convient de rendre plus effective la participation des citoyens à la gestion des affaires locales importantes tout en sauvegardant l'efficacité de celle-ci ». Dans le même sens, aux termes de la ligne directrice n° 14 en annexe à la Recommandation N°R (97) 7 du Comité des Ministres aux États membres du Conseil de l'Europe sur les services publics locaux et les droits de leurs usagers : « les collectivités locales encouragent la participation des usagers ou de leurs représentants à la gestion des services publics locaux selon des formes appropriées à la nature du service et aux circonstances ».

### Les trois niveaux de participation directe

Cette volonté s'est trouvée officiellement confirmée lors de la conférence des Ministres européens responsables des collectivités locales et régionales des 15 et 16 octobre 2007 consacrée à « la bonne gouvernance locale et régionale – le défi

européen ». Cette réunion a donné lieu à une déclaration solennelle<sup>77</sup> par laquelle les Ministres reconnaissent que « La démocratie représentative et la démocratie participative ne sont pas alternatives, mais se complètent l'une l'autre. L'existence de mécanismes de participation donne aux représentants locaux élus par les citoyens un outil précieux pour améliorer leur performance. Parallèlement, un solide tissu social et une société participative et bien structurée fournissent le meilleur environnement pour renforcer la démocratie locale et améliorer la base de sélection des représentants locaux. Nous renouvelons par conséquent notre engagement de faciliter la participation des citoyens à la vie publique locale ». Les instances européennes considèrent que la participation directe « peut se situer à trois différents niveaux du processus décisionnel : l'étude des questions à traiter et l'initiative normative, l'adoption des décisions et la mise en œuvre des décisions ». Sachant qu'à chaque phase on peut associer des formes de participation qui diffèrent de par leur nature, portée et effets :

- la participation informationnelle et consultative ;
- la participation par la prise de décisions ;
- la participation dans l'exécution.

Cette impulsion européenne trouve écho auprès des autorités françaises qui n'ont



## Rémy FÉVRIER

eu de cesse, depuis les lois de décentralisation de 1982 et 1983, de favoriser l'émergence d'une véritable participation des citoyens à la vie locale.

Une déclinaison locale corrélative de la décentralisation

Comme le souligne le CAS, le développement de la participation a été mené simultanément avec la montée en puissance de la décentralisation, le plus souvent au sein des mêmes textes législatifs.

Une évolution perceptible

72

Ce processus itératif a été marqué par plusieurs étapes essentielles :

La loi du 31 décembre 1982 qui prévoit la mise en place à Paris, Lyon et Marseille d'un « comité d'initiative et de consultation d'arrondissement » ;

La loi du 12 juillet 1983 qui réforme la notion d'enquête publique ;

La loi du 6 février 1992, qui permet au conseil municipal de créer des comités consultatifs sur tout problème d'intérêt communal, qui institue les commissions consultatives des services publics locaux et qui met en place les référendums municipaux consultatifs ;

La loi du 4 février 1995, qui organise les conseils de développement des Pays.

Et surtout :

La loi du 27 février 2002, dite « loi relative à la démocratie de proximité » qui prévoit la mise en place obligatoire -dans les villes de plus de 80.000 habitants- de conseils de quartier et élargit le rôle des commissions consultatives des services publics locaux ;

La loi organique du 1<sup>er</sup> août 2003, la loi du 13 août 2004 et la loi organique du 21 janvier 2007 qui organisent et précisent le régime du référendum local, ainsi que celui des consultations et des pétitions locales.

Le choix de favoriser l'émergence d'une véritable participation citoyenne aux politiques publiques locales s'est encore accentué avec les politiques de la ville. Cette volonté de participation s'articule schématiquement autour de quatre types de formules distinctes :

Les dispositifs ponctuels de consultation sur des opérations précises (ensemble des concertations ou débats publics liés à des opérations d'urbanisme ou d'aménagement du territoire : enquêtes publiques, débats publics locaux...)

Les dispositifs consultatifs structurels permettant aux citoyens de faire connaître leurs avis aux exécutifs locaux : commissions consultatives des services publics locaux, comités consultatifs, conseils de quartier...



## *Toujours plus cyber-menacées : les collectivités territoriales*

Les procédures de démocratie directe : consultation, pétition, référendum.

Et enfin, les procédés originaux qui ne rentrent dans aucune des catégories précédentes mais qui tendent à rendre compte d'une nouvelle organisation de la gouvernance. C'est dans ce cadre que la démocratie électronique prend tout son sens.

Si les opportunités créées par Internet ne sont pas à l'origine du mouvement visant à mieux faire participer les citoyens aux débats publics, elles ont néanmoins ouvert de nouvelles perspectives en matière d'interactions réelles entre les collectivités et leurs administrés.

### L'élaboration des consultations

L'utilisation d'Internet comme vecteur démocratique nécessite de réfléchir préalablement à l'ensemble des problématiques liées à la mise à disposition du public d'un outil, certes novateur, mais qui doit demeurer efficace et surtout pérenne. Pour répondre à ce défi et favoriser l'avènement d'une E-démocratie raisonnée et élément de bonne gouvernance, l'OCDE a énoncé un ensemble de « Principes directeurs d'une consultation en ligne réussie ».

Ces dix règles sont simples et uniformément adaptables à l'ensemble des initiatives de démocratie électronique, aussi les reprendrons-nous, en les explicitant, afin de mieux comprendre l'ensemble des pro-

cessus sous-jacents à la mise en place de nouveaux liens virtuels entre collectivités territoriales et citoyens :

Procéder à une analyse en amont : L'ensemble des buts recherchés, des moyens à mettre en œuvre ainsi que la totalité des parties prenantes doivent être préalablement identifiés de manière à circonscrire les périmètres d'action de chacun et les vecteurs d'échange informationnels les plus pertinents ;

Afficher une volonté hiérarchique manifeste : Aucun projet de déploiement de démocratie électronique ne peut se faire sans une implication forte et directe de l'exécutif local. Cet engagement doit également s'accompagner d'un souci d'informations à l'égard des citoyens dès le début du projet ;

Garantir la protection des données personnelles : La collecte d'informations à caractère personnel implique que la collectivité suive scrupuleusement les recommandations de la CNIL en la matière et qu'elle désigne un Correspondant Informatique et Liberté (CIL) afin de veiller aux respects des obligations légales en la matière ;

AdAPTER L'APPROCHE À L'ENSEMBLE DES CITOYENS : La clarté et l'ergonomie doivent être privilégiées lors de la mise en place d'un portail d'échanges citoyens. A ce titre il convient de penser aux aménagements indispensables à mettre en place pour per-





## Rémy FÉVRIER

mettre aux personnes souffrant de handicaps d'utiliser le site dans les meilleures conditions possibles (on pourra par exemple penser à des modules audio spécifiques à destination des personnes malvoyantes, à des claviers virtuels pour les internautes souffrant de difficultés à mouvoir leurs mains, etc.) ;

**Intégrer la consultation en ligne aux moyens traditionnels :** Sachant qu'une approche multicanaux à plus de chance d'aboutir à un échange informationnel réussi, il paraît pertinent d'envisager le recours à d'autres méthodes de consultations plus traditionnelles en parallèle de l'utilisation d'Internet ;

74

**Tester les instruments :** L'ensemble des interfaces techniques envisagées doivent faire l'objet d'un test préalable, afin de procéder aux ajustements indispensables à une qualité d'échange optimale ;

**Assurer la promotion du site :** La mise en service d'un portail de démocratie électronique doit faire l'objet d'une publicité préalable de la part de la collectivité, afin de susciter l'intérêt des internautes ;

**Analyser les résultats :** En cas de consultation, les résultats devront faire l'objet d'un traitement minutieux ce qui nécessite, en amont, d'estimer les ressources humaines nécessaires en terme de traitement, selon la nature du questionnaire : questions à choix multiples facilement automatisables, ou questions

ouvertes nécessitant un traitement qualitatif et donc plus de personnel ;

**Assurer un retour d'informations :** par souci de transparence, les résultats seront mis à disposition des citoyens sur le site Internet. Cela permettra, d'autre part, de fidéliser des citoyens soucieux de connaître l'impact réel de leur implication ;

**Evaluer le processus de consultation :** À l'issue de la consultation, il est indispensable de procéder à un retour d'expérience de la part de l'ensemble des parties prenantes, y compris un panel d'utilisateurs, afin d'améliorer simultanément les moyens engagés et la qualité des prochaines enquêtes.

Bien que très générales, les règles énoncées ci-dessous sont assez pertinentes dans la mesure où elles permettent de définir précisément les infrastructures techniques et humaines nécessaires, ainsi que de circonscrire judicieusement l'ensemble des procédures à mettre en place pour obtenir une réelle adhésion du public à une forme innovante de participation citoyenne. Pour autant, on ne peut manquer de se préoccuper, ici encore, des aspects liés à la sécurité des outils indispensables aux traitements des flux de données inhérents à la démocratie électronique.

**E-démocratie : des Elus sous pression**

Qu'on le veuille ou non, Internet apparaît aujourd'hui de plus en plus comme



## *Toujours plus cyber-menacées : les collectivités territoriales*

l'un des vecteurs d'engagement civique, que ce soit au travers de blogs citoyens évoquant des thématiques souvent environnementales, politiques, ou liées à la vie locale, ou de leur pendant institutionnel : les forums initiés par une collectivité territoriale pour échanger avec les administrés sur ses problématiques spécifiques. On trouve ici une structuration horizontale consultative, voire participative, qui s'est – en partie du moins – substituée à l'ancienne logique verticale et hiérarchisée, dans les relations entre l'Elu et la population. Engagé dans ce processus réclamé par ses électeurs et de plus en plus souvent soumis aux désiderata de groupes associatifs ou communautaires, l'Elu subit, de fait, une pression sociétale d'autant plus forte qu'elle s'accompagne la plupart du temps d'une importante pression économique, les entreprises n'étant pas en reste en matière de démarches de lobbying vis-à-vis des collectivités territoriales.

### Des risques numériques

Le réseau Internet constituant un vecteur essentiel en matière d'échanges informationnels, le portail web apparaît, de fait, comme le point de passage obligé de la démocratie électronique. Or, les sites web constituent une des cibles les plus exploitées en matière de pénétration des SI institutionnels.

De nombreux portails ont été conçus avec comme objectif principal de séduire

l'internaute au travers d'une ergonomie et d'une fonctionnalité optimales. Si ces considérations constituent des prérequis indispensables pour assurer une consultation régulières des sites, cela ne doit pas s'effectuer au détriment de la sécurité. Or, on constate trop souvent que les aspects liés à la sécurité ont été ignorés, ou du moins largement minorés, lors de la conception des sites. Il s'agit là d'une véritable erreur stratégique car cela revient à rendre vulnérable l'ensemble du SI de la collectivité, ainsi qu'à faire fuir le citoyen internaute soucieux de ne pas voir ses informations personnelles faire l'objet d'une interception, a fortiori dans le cadre d'une expérience de démocratie électronique. Nous reviendrons sur ce sujet en détails étant donné les risques que les pénétrations de portails web font courir aux collectivités, à leurs responsables administratifs et surtout aux Elus locaux.

- *La dématérialisation des appels d'offres*

Le troisième défi numérique auquel sont confrontées les collectivités territoriales s'inscrit dans une volonté générale de simplification des relations commerciales entre les organisations publiques et leurs prestataires. La dématérialisation des appels d'offre devient une réalité incontournable et sa mise en place impose de respecter un ensemble de normes et procédures extrêmement complexe d'un point de vue technique et assez coûteux à mettre en place. L'obligation qui est dorénavant



Rémy FÉVRIER

faire aux collectivités territoriales d'accepter les réponses numériques à leurs appels d'offres nécessite de revoir complètement les anciennes méthodes de traitement et ce, d'autant que ces flux informationnels doivent nécessairement s'accompagner d'une sécurisation optimale des données traitées.

Parallèlement à ces mutations du rapport démocratique et administratif au citoyen, les collectivités territoriales ont à intégrer, dans leur activité quotidienne, la transformation des rapports avec leurs prestataires : la dématérialisation croissante des appels d'offres décidée par les pouvoirs publics sera définitivement achevée en 2012. Cette mutation implique de nouveaux risques dont les Elus locaux ont de plus en plus conscience, ces derniers étant simultanément tributaires d'un durcissement de la législation et d'obligations légales extrêmement strictes, en relation avec les processus misent en place pour substituer le canal électronique aux anciens échanges épistolaires. Les collectivités territoriales et leurs établissements publics – y compris les Établissements Publics Industriels et Commerciaux (EPIC) – sont soumis au Code des Marchés Publics (CMP) dans la mesure où les marchés publics sont des contrats passés afin de satisfaire aux besoins d'une personne publique et sont conclus à titre onéreux.

### La dématérialisation des appels d'offres

Depuis plusieurs années, de nombreuses voix se sont élevées contre la supposée « ri-

gidité » du corpus de règles régissant les relations commerciales entre entités publiques et entreprises privées : le CMP. La plus célèbre critique provient d'Alain Lambert, ancien Ministre du Budget et rédacteur d'un rapport préconisant l'alignement du CMP sur la législation européenne : « Comment peut-on aller vers l'efficacité de l'action publique avec un Code des Marchés Publics si complexe qu'il est inintelligible pour la majorité des humains d'intelligence normale. Optons pour la seule législation européenne puisque, de toute manière, elle s'applique ! Pourquoi ajouter toujours de la complexité à la complexité ? »<sup>78</sup>.

Sans rentrer dans une quelconque polémique on peut néanmoins observer que depuis plusieurs années des textes de lois visant à faire évoluer ce code se sont succédés, que ce soit au travers de la baisse régulière des seuils financiers imposant un appel d'offre, ou de la définition des conditions nécessaires à la mise en place de la dématérialisation. Cette évolution est marquante dans la mesure où la commande publique représente un pourcentage non négligeable du Produit Intérieur Brut (PIB) français et que la part des transactions commerciales effectuées par les collectivités territoriales représente plus de 40% de la totalité des montants dépensés au travers des marchés publics.

### Le poids des marchés publics en France

Si les chiffres relatifs à la commande publique en France divergent beaucoup



## *Toujours plus cyber-menacées : les collectivités territoriales*

en fonction des sources et des champs d'activités considérés, tous les observateurs s'accordent pour attribuer à cette dernière un poids considérable au sein de l'économie nationale. En ce qui nous concerne, nous reprendrons les chiffres publiés par l'Observatoire économique de l'achat public<sup>79</sup>. Selon ce dernier, le montant des marchés publics recensés se montait à 53 milliards d'euro en 2005 pour atteindre 68 milliards en 2008, puis 81 milliards<sup>80</sup> en 2009, sous l'influence des efforts consentis par l'État pour lutter contre l'impact de la crise financière de 2008.

Pour autant, ces chiffres établis sur la base de la comptabilité nationale agrègent les dépenses effectuées une année donnée par un certain nombre d'entités. Ils n'incluent pas les entreprises publiques mais les seules administrations publiques et comprend en revanche certaines dépenses ne relevant pas du CMP. On estime que le montant de la dépense prenant en compte la globalité des commandes en provenance du secteur public au sens le plus large nécessite de multiplier par trois les sommes évoquées. Ces montants, après être longtemps demeurés autour de 10% du PIB, représentent conjoncturellement aujourd'hui près 15% de celui-ci.

### Part des collectivités territoriales

La part des collectivités territoriales en matière de commande publique atteint 40% du total de celle-ci en 2009, après

avoir culminé à 47% en 2008, ce qui fait des collectivités territoriales des partenaires commerciaux majeurs pour un grand nombre d'entreprises françaises voire européennes. En matière de structuration de l'offre, l'étude de consolidation de l'ensemble des données issues du recensement économique des marchés publics réalisée par la Direction des Affaires Juridiques du Ministère de l'Economie et des Finances (DAJ) et intitulée « Place des PME dans les marchés publics en 2009 »<sup>81</sup>, montre que la part des PME en termes de nombre de marchés attribués paraît plus forte pour les collectivités territoriales que pour l'État (65% contre 43%), sachant que cette différence est encore plus marquée en termes de montant puisque cette part représente 43% pour les collectivités contre seulement 16% pour l'État. Si cette présence majoritaire des PME en matière de contrats publics territoriaux constitue incontestablement une bonne chose pour les tissus économiques locaux, force est néanmoins de constater que de nombreuses PME ne répondent à aucun appel d'offre public du fait des contraintes inhérentes à ce genre d'exercice.

On peut classer les marchés publics en trois thèmes principaux en fonction des prestations à réaliser : les marchés de travaux, de fournitures et de services. Ce recours au secteur marchand nécessite le respect de règles strictes rassemblées au sein d'un recueil de textes administratifs : le CMP. Cette réglementation précise, entre



## Rémy FÉVRIER

78

autres, les conditions générales de l'accès aux marchés publics, ainsi que les procédures que les prestataires doivent respecter pour pouvoir contracter avec une entité publique.

### Structuration des marchés publics

Par principe, les marchés publics doivent faire l'objet d'un allotissement, c'est-à-dire d'une division en lots homogènes, afin de faire jouer les mécanismes de la concurrence et d'éviter que le pouvoir adjudicateur (maître d'ouvrage) soit par trop dépendant d'un unique fournisseur (maître d'œuvre). Cette règle peut néanmoins être exceptionnellement contournée lorsque le fait d'établir une dichotomie induit un inconvénient d'ordre technique ou financier.

Les candidatures sont donc examinées lot par lot et chaque entreprise souhaitant soumissionner pour plusieurs lots doit de fait présenter une offre correspondante à chaque lot cible. L'attribution de plusieurs lots à la même entreprise est possible à condition que le règlement initial de consultation ne l'interdise pas.

Certains marchés peuvent également faire l'objet d'un fractionnement temporel, que ce soit pour des raisons de manque de visibilité sur les besoins (marchés à bons de commandes) ou en cas de programmes d'investissements lourds directement dépendants de la conjoncture économique (marchés à tranches conditionnelles).

### Les procédures formalisées

L'appel d'offre constitue la procédure standard (« formalisé ») de passation de marchés publics. Néanmoins, il existe deux types d'appels d'offres : l'appel d'offre ouvert<sup>82</sup> et l'appel d'offre restreint<sup>83</sup>. Dans le cadre d'un appel d'offre, la procédure fait l'objet d'un encadrement strict durant l'ensemble du processus : aucune marge de négociation n'est possible entre l'acheteur et les candidats.

Les procédures d'appels d'offre se déclenchent lorsque le montant estimé du marché dépasse 210.000€ pour la collectivité en matière de fournitures ou de services (et de 5.150.000€ en matière de travaux). Lorsque ce seuil est franchi, le pouvoir adjudicateur doit obligatoirement émettre un avis de publicité dans le Bulletin Officiel des Annonces des Marchés Publics (BOAMP), ainsi qu'au Journal Officiel de l'Union Européenne (JOUE).

L'appel d'offre restreint<sup>84</sup> se distingue uniquement par une analyse préalable des offres, suite à laquelle une limitation du nombre de candidatures pourra être mise en place, pour autant que le principe ait fait l'objet d'une annonce préalable au moment du lancement de la procédure initiale.

### Les procédures non-formalisées

Parallèlement aux règles strictes régissant les procédures d'appels d'offre, le législateur, tenant en cela compte de l'accroissement de la concurrence entre



## *Toujours plus cyber-menacées : les collectivités territoriales*

fournisseurs, ainsi que de la montée en puissance de la dématérialisation, a souhaité assouplir les règles d'engagement en matière de marchés publics en offrant l'opportunité aux collectivités de disposer de nouveaux outils de gestion de leurs besoins tout en assortissant leur usage à certains seuils d'engagement financier.

### Les marchés de gré à gré

En cas de montant de marché inférieur à 6.000€ HT, celui-ci est passé librement (marché de gré à gré<sup>85</sup>), c'est-à-dire en dehors de toute publicité, voire même sans mise en concurrence préalable. Si la collectivité peut s'adresser ainsi au prestataire de son choix, il est néanmoins vivement conseillé de faire établir plusieurs devis afin d'éviter tout surcoût injustifié.

### Les Marchés Passés selon la Procédure Adaptée (MAPA)

La mise en place d'une procédure adaptée<sup>86</sup> par une collectivité territoriale, plus souple que celle de l'appel d'offre, est possible lorsque le montant de l'appel d'offre est inférieur à 135.000€ HT dans le cas d'achats de fournitures et de services, ou à 210.000€ HT dans le cas de travaux.

Pour les marchés de plus de 90.000€ HT, les avis doivent obligatoirement faire l'objet d'une publication au BOAMP ou dans un journal habilité à diffuser des annonces légales (JAL). En dessous de ce seuil, le pouvoir adjudicateur peut em-

ployer le vecteur publicitaire de son choix.

### Les marchés négociés

La procédure du marché négocié permet au pouvoir adjudicateur de choisir le titulaire du marché après consultation de candidats et négociation. Il peut passer un marché négocié dans les cas définis ci-après<sup>87</sup> :

- Marchés et accords-cadres pour lesquels, après appel d'offres ou dialogue compétitif, il n'a été proposé que des offres irrégulières ou inacceptables que le pouvoir adjudicateur est tenu de rejeter ;
- Marchés et accords-cadres de services, notamment certains marchés de services financiers mentionnés et marchés de prestations intellectuelles telles que la conception d'ouvrage, lorsque la prestation de services à réaliser est d'une nature telle que les spécifications du marché ne peuvent être établies préalablement avec une précision suffisante pour permettre le recours à l'appel d'offres ;
- Marchés et accords-cadres de travaux conclus uniquement à des fins de recherche, d'essai, d'expérimentation ou de mise au point sans finalité commerciale immédiate ;
- Ainsi que dans certains cas exceptionnels, lorsqu'il s'agit de travaux, de



Rémy FÉVRIER

fournitures ou de services dont la nature ou les aléas qui peuvent affecter leur réalisation ne permettent pas une fixation préalable et globale des prix.

### Le dialogue compétitif

La procédure de dialogue compétitif a été mise en place afin de permettre au pouvoir adjudicateur de conduire un dialogue avec les soumissionnaires admis à participer à la procédure afin de « définir ou de développer une ou plusieurs solutions de nature à répondre à ses besoins et sur la base de laquelle ou desquelles les participants au dialogue seront invités à remettre une offre »<sup>88</sup>. Le recours à la procédure de dialogue compétitif est uniquement possible lorsqu'un marché public est considéré comme complexe, c'est-à-dire lorsque l'une au moins des conditions suivantes est remplie:

- Soit le pouvoir adjudicateur n'est objectivement pas en mesure de définir seul et à l'avance les moyens techniques pouvant répondre à ses besoins ;
- Soit le pouvoir adjudicateur n'est objectivement pas en mesure d'établir le montage juridique ou financier d'un projet.

L'avantage de cette forme de procédure est de permettre à l'acheteur de mieux évaluer ses besoins ainsi que d'avoir une idée précise des diverses solutions dispo-

nibles ou adaptables susceptibles d'être proposées par les prestataires. Le dialogue compétitif est notamment adapté aux marchés visant à la mise en place de SI.

### Mise en place de la dématérialisation

Les pouvoirs publics européens et nationaux, soucieux de profiter des opportunités offertes par les nouvelles technologies de l'information en matière de rationalisation de la commande publique, imposent dorénavant à l'ensemble des entités publiques et des collectivités de se tourner vers la dématérialisation des appels d'offres et le traitement des réponses sous format électronique.

### Une obligation légale

La dématérialisation des appels d'offres doit permettre d'optimiser l'efficacité de la commande publique au travers, notamment, d'une plus grande facilité de traitement et de comparaison entre les offres reçues. Le caractère difficile du passage à l'échange électronique avec les fournisseurs tient en partie au fait de l'impérative nécessité de respecter, lors de la mise en place d'un processus de dématérialisation, les principes intangibles du droit des marchés publics, à savoir la liberté d'accès à la commande publique, la transparence des procédures ainsi que l'égalité de traitement entre les candidats. La logique voudrait que l'ensemble des parties prenantes prennent conscience du potentiel de ce nouveau mode opératoire, en ma-



## *Toujours plus cyber-menacées : les collectivités territoriales*

tière de transparence et d'efficacité, et s'y adaptent rapidement.

Pourtant, certaines réticences se sont fait jour au fil du temps et les pouvoirs publics ont été contraints d'imposer le recours à ces nouvelles pratiques, sachant qu'il s'agit là d'un sujet dont s'est emparé la Commission Européenne et qui a abouti à énoncer des directives ultérieurement transposées dans les droits nationaux respectifs des pays de l'Union Européenne.

### Droit européen relatif à la commande publique

La prise en considération des technologies de l'information et de la communication en tant que nouveau vecteur des marchés publics date de 2004, au travers de l'élaboration de deux directives transposées par la suite : la directive 2004/17/CE du Parlement et du Conseil du 31 mars 2004, portant coordination des procédures de passation des marchés dans les secteurs de l'eau, de l'énergie, des transports et des services postaux et surtout la directive 2004/18/CE du 31 mars 2004 du Parlement et du Conseil et relative à la coordination des procédures de passation des marchés publics de travaux, de fournitures et de services.

Le point 12 du considérant de la directive 2004/18/CE explicite clairement les raisons de la prise en compte des potentialités de dématérialisation de la com-

mande publique : « Certaines nouvelles techniques d'achat électroniques sont en développement constant. Ces techniques permettent d'élargir la concurrence et d'améliorer l'efficacité de la commande publique, notamment par les gains de temps et les économies que l'utilisation de telles techniques comporte. Les pouvoirs adjudicateurs peuvent utiliser des techniques d'achat électroniques, pour autant que leur utilisation soit faite dans le respect des règles établies par la présente directive et des principes d'égalité, de traitement, de non-discrimination et de transparence ».

### De nouvelles armatures techniques

81

À cette déclaration de principe s'ajoute la nécessaire définition des armatures techniques appropriées pour profiter de ces nouvelles opportunités : « Compte tenu de l'expansion rapide des systèmes d'achat électroniques, il convient de prévoir, d'ores et déjà, des règles adéquates pour permettre aux pouvoirs publics adjudicateurs de tirer pleinement profit des possibilités offertes par lesdits systèmes. Dans cette perspective, il convient de définir un système d'acquisition dynamique entièrement électronique pour des achats d'usage courant et de fixer des règles spécifiques pour la mise en place et le fonctionnement d'un tel système afin de garantir le traitement équitable de tout opérateur économique qui souhaite en faire partie ». Il est même envisagé un recours accru au principe des enchères





Rémy FÉVRIER

82

électroniques : « Les enchères électroniques constituant une technique appelée à se répandre, il convient de donner une définition communautaire de ces enchères et de les encadrer par des règles spécifiques afin d'assurer qu'elles se déroulent dans le plein respect des principes d'égalité de traitement, de non-discrimination et de transparence ».

Cette directive a largement ouvert la voie à une dématérialisation globale des appels d'offres, en considérant que l'ensemble des échanges de documents consubstantiels à la passation d'un marché public peuvent être opérés par voie électronique. Toutefois, les instances de l'Union Européenne insistent fortement sur la nécessité d'utiliser des vecteurs d'échanges interopérables, permettant de garantir non seulement l'intégrité des informations transmises, mais également une confidentialité absolue des offres et candidatures soumises. La transposition de la directive 2004/18/CE a été l'occasion, pour la France, d'adapter le CMP aux nouvelles opportunités offertes par la dématérialisation.

### L'évolution du Code des Marchés Publics

En ce qui concerne la France et suite à des évolutions successives en 2002, 2004 et 2006, le CMP est aujourd'hui très explicite quant à la notion de dématérialisation des procédures d'appels d'offres publiques.

### Des étapes successives

Au travers de l'article 56<sup>89</sup> du CMP et relatif aux communications et échanges d'informations par voie électronique, le Législateur a procédé par étapes : dans un premier temps, liberté de choix a été donnée aux pouvoirs adjudicateurs (entités publiques acheteuses) en matière d'échanges : « dans toutes les procédures de passation [de marchés publics], les documents écrits mentionnés par le présent code peuvent être remplacés par un échange électronique ou par la production de supports physiques électroniques, selon les dispositions prévues au présent article », sous réserve que « le pouvoir adjudicateur indique, dans l'avis d'appel public à la concurrence ou, pour les marchés négociés sans publicité préalable, dans la lettre de consultation et le mode de transmission qu'il retient ».

Une nouvelle étape a été franchie depuis le 1<sup>er</sup> janvier 2010 : depuis cette date, le pouvoir adjudicateur « peut imposer la transmission par voie électronique des documents ». De plus, les achats de biens et services informatiques font l'objet d'une attention particulière : « à compter de la même date, pour les achats de matériels informatiques et de services informatiques d'un montant supérieur à 90.000 € H.T, les documents requis des candidats sont transmis par voie électronique ».

L'instauration de la voie électronique par le pouvoir adjudicateur achevée, restait à définir une échéance postérieure-



## *Toujours plus cyber-menacées : les collectivités territoriales*

ment à laquelle les entreprises pourraient également faire valoir leur droit à utiliser la dématérialisation des procédures afin de soumissionner. Cette possibilité nécessite un préalable de taille : l'ensemble des entités publiques soumises au code des marchés publics doivent être en mesure de traiter les réponses électroniques en provenance des entreprises candidates. Or, c'est loin d'être le cas pour ce qui est des collectivités territoriales de taille réduite. C'est finalement la date du 1<sup>er</sup> janvier 2012 qui a été choisie puisque à compter du 1<sup>er</sup> janvier 2012, pour les achats de fournitures, de services ou de travaux d'un montant supérieur à 90.000 € H.T, le pourvoir adjudicateur ne peut refuser de recevoir les documents requis des candidats qui sont transmis par voie électronique. Dans tous les cas, le pouvoir adjudicateur doit assurer « la confidentialité et la sécurité des transactions sur un réseau informatique accessible de façon non discriminatoire ». Parallèlement aux nouvelles opportunités offertes aux collectivités territoriales, c'est tout un nouveau champ de compétence qu'elles sont dorénavant fortement invitées à maîtriser.

### Les prérequis juridiques

Le corollaire direct de la mise en place d'une véritable dématérialisation des appels d'offre publics réside dans une fiabilité absolue quant à l'identification des documents échangés ainsi qu'à leur authenticité, ce qui a entraîné la définition d'un cadre légal spécifique, déclinable en

outils juridiques et techniques d'identification susceptibles d'établir un réel lien de confiance entre la puissance adjudicatrice et les soumissionnaires. La principale innovation juridique a consisté en l'élaboration d'une véritable reconnaissance de l'écrit électronique et de la notion de signature électronique par le code civil, sachant que cette évolution était rendue indispensable par la nécessaire transposition, dans le droit français, de la directive européenne 1999/93/CE du 13 décembre 1999 relative à la signature électronique, renforcée par la directive 2000/31/CE du 8 juin 2000 sur le commerce électronique.

Cette transposition s'est finalement traduite par l'adoption de la loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique. Cette loi a fait évoluer le code civil en y introduisant des articles spécifiques donnant à l'écrit électronique – sous certaines conditions – la même force probante que l'écrit papier.

Selon ces textes, « l'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité »<sup>90</sup>, ce qui constitue une évolution légale majeure dans le sens où la signature électronique se voit reconnaître un véritable caractère probant, ce qui est clairement confirmé par l'article



## Rémy FÉVRIER

1316-3 du Code Civil selon lequel « l'écrit sur support électronique a la même force probante que l'écrit sur support papier », sachant que l'on entend par signature « une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles, dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission »<sup>91</sup>.

De par le caractère incorporel des documents échangés dans le cadre d'un marché dématérialisé, le législateur a souhaité mettre un accent particulier sur la notion de fiabilité de la signature électronique, afin d'en faire le réel pendant du paraphe manuscrit : « La signature, lorsqu'elle est électronique, consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve du contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'État »<sup>92</sup>.

Selon la Direction des Affaires Juridiques du Ministère de l'Économie, de l'Industrie et de l'emploi<sup>93</sup>, la signature électronique garantit trois fonctions simultanées :

- L'identité de l'émetteur du message : la signature permet à la fois de se faire connaître et d'être reconnu ;
- Le fait qu'il ne peut être revenu sur ce qui a été signé (principe de non répu-

diation) : le signataire atteste la volonté de donner son approbation aux dispositions contenues dans l'acte, il ne peut renier sa signature ;

- L'intégrité du document signé : le document arrive sans altération, dans le cas contraire, il arrive signalé comme ayant été modifié.

L'utilisation de la signature électronique passe tout d'abord par l'utilisation d'un certificat numérique comprenant l'identité du titulaire, la période de validité, la clé publique et la signature de l'autorité de certification ou de l'entité qui a délivré le certificat<sup>94</sup>. Ce certificat est délivré par une autorité de certification. Généralement, la durée de validité du certificat est de deux ans et son coût annuel moyen se situe aux alentours d'une centaine d'euros. Suite à l'obtention du certificat en question, il convient de faire l'acquisition d'un logiciel de signature qui va permettre de chiffrer les données transmises par les entreprises afin de les rendre hermétiques à toute personne, ou entité, ne disposant pas de la clé de décodage.

L'ensemble de ces impératifs indispensables à la légalité et à la sécurisation des procédures de dématérialisation constitue autant d'obstacles devant être maîtrisés par les collectivités territoriales dans la perspective de l'échéance du 1<sup>er</sup> janvier 2012. Toutefois, la dématérialisation des appels d'offre constitue encore un sujet de préoccupation pour de nombreuses collec-



## *Toujours plus cyber-menacées : les collectivités territoriales*

tivités territoriales et entreprises soumissionnaires qui éprouvent certaines difficultés à évoluer vers le tout-électronique.

### Des objectifs ambitieux

Les pouvoirs publics ont lancé la dématérialisation des appels d'offre avec pour objectif de simplifier les relations entre les collectivités publiques et les entreprises soumissionnaires. Théoriquement, il paraît intéressant pour l'ensemble des parties prenantes de disposer d'un outil réactif et performant de gestion de la commande publique. Afin d'expliquer les bienfaits attendus d'une dématérialisation aboutie, nous reprendrons les présentations élaborées par le Ministère de l'Économie, de l'Industrie et de l'emploi, afin de convaincre acheteurs et vendeur de dématérialiser leurs échanges.

### Une recherche d'optimisation en matière de gestion

Le but premier de la dématérialisation est d'optimiser les processus d'achat publics pour réduire les coûts relatifs à des appels d'offres diffusés sous format papier et d'un suivi engendrant de nombreuses opérations lourdes et coûteuses.

### Pour les collectivités

Les gains envisagés pour les entités publiques sont loin d'être négligeables :

- Amélioration des procédures d'achat : la souplesse induite par le recours aux

TIC est sans commune mesure avec la nécessité de fournir l'ensemble des dossiers généraux et techniques aux entreprises candidates ;

- Diversification des sources d'approvisionnement : du fait de la facilité de mise à disposition des dossiers, de nombreuses PME n'ayant jusqu'alors pas saisie l'opportunité de répondre à des appels d'offres publics pourront désormais s'enquérir des marchés en cours et télécharger facilement l'ensemble des pièces indispensables à la constitution d'une réponse commerciale ;
- Réduction des durées des procédures de passation des marchés publics : l'un des principaux griefs fait au CMP réside dans la durée souvent excessive s'écoulant entre le choix préalable des produits et leur date de livraison, a fortiori dans le domaine des hautes technologies pour lequel l'obsolescence des matériels intervient très rapidement, ce qui peut entraîner une fuite en avant perpétuelle couteuse et source d'inefficacité. La dématérialisation des procédures doit également permettre une meilleure réactivité, elle-même gage de rentabilité économique accrue ;

- Professionnalisation de la fonction achat : il va sans dire que la dématérialisation va provoquer une spécialisation accrue des agents en charge de



Rémy FÉVRIER

86

l'élaboration des marchés publics. Il sera donc indispensable de former spécifiquement ces derniers aux procédures électroniques, aussi bien sur le plan juridique que relativement aux techniques utilisées avec, pour résultat final, une professionnalisation de fait, de la fonction achat des collectivités.

Corrélativement à une réduction des coûts de publication des avis publicitaires et de transmission des dossiers à destination des entreprises soumissionnaires, d'autres avantages indirects découlent de la mise en place de ce nouveau procédé, comme la combinaison simultanée d'une meilleure sécurisation et d'une traçabilité complète de l'ensemble des échanges électroniques entre la collectivité et les entreprises.

#### Pour les entreprises

De leur côté, les entreprises peuvent également tirer parti de la dématérialisation afin d'optimiser leur offre à destination des collectivités. À condition, toutefois, de relever le défi posé par ce nouveau type de rapport au client, notamment au travers de la mise en place de nouveaux processus de gestion des propositions commerciales et l'automatisation de la veille économique.

Les entreprises qui feront l'effort de s'adapter à cette nouvelle manière d'envisager les procédures publiques, améliore-

ront fortement leur réactivité commerciale et disposeront de nouvelles capacités d'accès aux marchés publics. La possibilité de mettre en place des alertes ciblées relativement aux appels d'offres touchant à leurs domaines d'activités respectifs, constituera un avantage concurrentiel important et de nature à permettre aux entreprises d'avoir accès à un grand nombre d'opportunités commerciales sur l'ensemble du territoire. La dématérialisation des réponses permet également aux groupements d'entreprises d'élaborer des réponses groupées aux appels d'offres à moindre coût et bien plus aisément qu'au travers d'échanges de courriers et de dossiers préliminaires par voie postale, sachant que l'accusé de réception électronique offre pareillement aux entreprises soumissionnaires la certitude de la bonne réception de leurs candidatures.

#### Réalité de la perception

Comme dans le cadre de toute innovation, il s'avère opportun de mesurer le degré d'adhésion des parties prenantes. Deux enquêtes récentes ont été menées, l'une à la demande du Ministère de l'Économie, de l'Industrie et de l'Emploi, en octobre 2008<sup>95</sup> (enquête qualitative) et l'autre à celle de la Direction des Journaux Officiels (enquête quantitative) effectuée en mai 2008 auprès d'un échantillon représentatif d'« Acheteurs » du service public et d'entreprises soumissionnaires<sup>96</sup>. L'analyse de ces deux études complémentaires permet de mettre en évidence une approche



## *Toujours plus cyber-menacées : les collectivités territoriales*

assez paradoxale de la dématérialisation des appels d'offre dans le sens où, bien que l'ensemble des acteurs s'accorde sur les bienfaits de ce passage à des procédures numériques, il demeure néanmoins un certain nombre d'interrogations et quelques résistances pouvant nuire à une utilisation optimale de ce nouvel outil économique.

### Perception des collectivités

En ce qui concerne les collectivités territoriales, la taille et le type de collectivités sont encore à l'origine d'une dichotomie manifeste dans le rapport à la dématérialisation : si 82% d'entre elles considèrent la dématérialisation des procédures d'appels d'offres publics comme une bonne initiative, il n'en demeure pas moins que l'un des facteurs clés réside dans le fait, pour la collectivité, de disposer ou non d'un service dédié à la gestion des marchés publics. Or, la probabilité de disposer d'un tel service varie considérablement selon le type de collectivité : si 72% des Conseils régionaux et généraux en possèdent, cette proportion n'est que de 42% pour les communes, avec de grandes disparités, puisque les villes de plus de 50.000 habitants en sont dotées contre 9% pour les communes de moins de 3000 habitants. Encore faut-il préciser que seuls 51% de ces services dédiés disposent d'un progiciel de traitement spécialisé dans la gestion de ces échanges électroniques.

Les collectivités ayant déjà utilisé la procédure de dématérialisation l'ont fait à

sens unique, c'est-à-dire à des fins de signalement de l'appel d'offres vis-à-vis de soumissionnaires potentiels : alors que 79% d'entre elles ont mis à disposition des entreprises un cahier des charges en ligne, elles ne sont que 39% à avoir examiner une offre déposée sur une plateforme de dématérialisation, la motivation des collectivités étant très largement liée au caractère obligatoire de la dématérialisation (77%). La mise en œuvre d'une procédure de dématérialisation n'est pas toujours aisée pour ces dernières : plus de 70% d'entre elles expliquent avoir rencontré des difficultés lors de sa conception.

Pourtant et c'est là l'un des paradoxes mis en évidence par ces études, 85% des utilisateurs ayant procédé à une expérience de dématérialisation se déclarent satisfait de celle-ci, et 65% considèrent qu'il est facile de traiter une offre électronique. Enfin, alors même qu'une majorité de collectivités interrogées se déclare déçue par le peu d'intérêt que suscite la dématérialisation auprès des entreprises, elles ne sont que 30% à encourager ces dernières à répondre électroniquement aux appels d'offre et 23% à avoir mis à leur disposition une assistance téléphonique spécifique afin de les conseiller. Il apparaît également que les collectivités territoriales sont extrêmement soucieuses des menaces d'annulation des marchés par le juge administratif et nombreuses sont celles qui considèrent les procédures de dématérialisation comme un vecteur supplémentaire de risque.



Rémy FÉVRIER

88

## Perception des entreprises

Du côté des entreprises, la perception de la dématérialisation apparaît également ambiguë : alors même que 77% d'entre elles considèrent comme positive la possibilité de dématérialiser les procédures d'appel d'offres, seules 36% des sociétés interrogées disposent effectivement d'un service dédié à l'organisation des réponses ou au suivi des marchés publics ; avec, là encore, une probabilité directement liée à la taille de l'entité : la proportion va de 17% dans les entreprises de moins de 20 salariés à 52% dans les entreprises de 100 à 499 salariés. Encore faut-il pondérer ce fait en précisant que dans 51% des cas, le « service » en question ne comporte qu'une personne. Il est à noter, de surcroît, que le taux moyen d'équipement en progiciels spécialisés de gestion n'est que de 15% !

Au travers de l'analyse des réponses à ces questionnaires, on constate que si les entreprises plébiscitent (93%) la possibilité qui leur est offerte de télécharger en ligne les cahiers des charges des appels d'offre, le taux tombe à 35% en ce qui concerne la transmission de l'offre par courrier électronique. Cette situation laisse à penser que dans de nombreux cas, la dématérialisation n'est donc utilisée que dans un cadre descendant : depuis la collectivité vers les entreprises. Parmi les raisons évoquées par les établissements n'ayant jamais répondu à un appel d'offre dématérialisé, la crainte d'une excessive complexité de ces nouvelles procédures arrive en première position (40%), suivie de près par un manque de

formation et d'explication (37%) et l'appréhension face à une trop grande complexité (33%). Pourtant, à l'inverse, les entreprises ayant déjà soumissionné électroniquement sont 67% à estimer que cette nouvelle forme d'interaction économique leur permet un gain de temps et d'argent (67%) et leur facilite des démarches administratives auparavant fastidieuses (41%).

Finalement, si 60% des entreprises interrogées considèrent qu'il serait souhaitable, y compris après 2012, d'avoir le choix des canaux de réponse à un appel d'offre public (électronique ou épistolaire), on peut néanmoins présumer que cette frilosité manifeste décroîtra à mesure que les efforts d'explications engagés par les pouvoirs publics porteront leurs fruits. Il est étonnant de constater que la notion de sécurisation des échanges n'est évoquée que de manière très marginale parmi les préoccupations des différentes parties prenantes, alors que la notion même de dématérialisation suppose une extrême rigueur étant donné la diversité des risques susceptibles d'impacter le processus.

## Dématérialisation et risques numériques

Si les entreprises et les collectivités territoriales s'inquiètent de ne pas toujours maîtriser les problématiques d'ordre technique liées à la dématérialisation, rares sont celles qui mettent en avant la sécurisation des échanges en tant qu'élément indispensable à cette nouvelle forme de commerce électronique. Il s'agit pourtant d'un préalable



## *Toujours plus cyber-menacées : les collectivités territoriales*

indispensable à la sérénité des échanges, afin d'éviter aux Élus locaux d'être soupçonnés de favoritisme car la conjonction simultanée d'une nouvelle souplesse dans les échanges et d'une traçabilité accrue, consubstantielle à l'utilisation des nouvelles technologies, fait qu'il devient indispensable d'examiner l'ensemble des problèmes relatifs à la sécurité de ces vecteurs d'échanges avec la plus extrême attention. Cela permet d'éviter tout désagrément ultérieur susceptible, non seulement, d'induire une mise en cause judiciaire pour des Élus potentiellement négligents, mais également de jeter fort injustement l'opprobre sur la collectivité territoriale dans son ensemble.

### Du risque numérique au risque pénal

Si l'utilisation des moyens numériques permettra de développer les échanges entre les collectivités et leurs fournisseurs, il reste que celle-ci devra s'effectuer dans le respect du CMP. La mise en place d'une dématérialisation vertueuse passera donc principalement par l'égalité de traitement des entreprises, la transparence des procédures, l'intégrité des documents et la possibilité d'archiver convenablement ces derniers. On peut d'ores et déjà émettre l'hypothèse que la notion même de dématérialisation des appels d'offre va largement faciliter le travail des magistrats car les données des appels d'offres en question seront d'un accès bien plus pratique et rapide.

Il serait même envisageable d'utiliser les opportunités offertes par l'interconnexion

des systèmes et les capacités de traitement des ordinateurs modernes en termes d'accès aux dossiers archivés pour réaliser, le cas échéant, des vérifications systématiques de la sincérité et de la légalité des procédures d'achat. Tout concourt donc à faire en sorte de sécuriser au maximum les échanges liés à la dématérialisation, car une fuite d'informations vers des tiers ou un manque de sécurisation des données archivées peut s'avérer fâcheux pour les collectivités – et leurs Élus – car, selon les textes, c'est à elles que revient la charge d'assurer la sécurisation des données échangées.

Si le risque pénal peut se décomposer en trois catégories : le délit de corruption, le délit d'ingérence et le délit de favoritisme, nous étudierons plus particulièrement le dernier, dans la mesure où un passage non maîtrisé ou trop rapide à la dématérialisation peut avoir des conséquences directes sur le respect d'une nécessaire neutralité vis-à-vis de l'ensemble des fournisseurs. Il serait pour le moins aberrant qu'une collectivité soit condamnée pour favoritisme alors même qu'aucune intention n'ait présidé à l'attribution du marché considéré. Or, une mauvaise prise en compte de l'ensemble des contraintes liées à la dématérialisation peut s'avérer source de problèmes ultérieurs.

### Sécurisation de la chaîne de dématérialisation

Afin d'éviter aux collectivités d'être confrontées à de tels désagréments, la



## Rémy FÉVRIER

Mission pour l'économie numérique dépendant du Ministère de l'Économie, de l'Industrie et de l'Emploi, a élaboré un document de grande qualité, intitulé « guide technique pour la sécurité de la dématérialisation des achats publics ». Ce guide liste l'ensemble des étapes indispensables à la mise en place d'une procédure de dématérialisation et donne des conseils précis pour chacune d'entre elles, organisées en grands items.

### L'organisation du service en charge de la dématérialisation

L'accent est mis, ici, sur la nécessaire compétence des agents et leur sensibilisation aux risques liés à l'utilisation des TIC tout au long du processus. Est également évoquée la confidentialité des données vis-à-vis des techniciens informatiques en charge de la maintenance des systèmes. En tout état de cause, la Personne Responsable du Marché (PRM), ainsi que les acheteurs, devront bénéficier d'une attention spécifique en matière de formation et d'identification.

### Les postes de travail et le réseau

La mission insiste sur la nécessité, pour tous les membres du service, de disposer sur son poste de travail d'un mot de passe, d'un antivirus et d'un détecteur de spyware (logiciels espions) correctement paramétrés et mis à jour en permanence. La sauvegarde et le chiffrement des dossiers sensibles sont aussi fortement recommandés. En ce qui concerne le réseau, la mise

en place d'un firewall est définitivement jugée indispensable.

### Plateforme de dématérialisation

La mise en place d'une plateforme de dématérialisation devra répondre à des normes strictes en matière de sécurité, comme de disposer d'un antivirus performant, garantir l'intégrité des documents et la confidentialité des informations transmises et stockées, au travers de la définition et de la conservation sécurisée de clés de chiffrement et de déchiffrement, d'un horodatage précis des documents et d'une politique de sécurité déclinée en procédures et modes opératoires précis, dont la description figurera sur le site de la collectivité afin de rassurer les entreprises soumissionnaires sur la qualité de la prise en compte de leurs dossiers et le respect de règles optimales de sécurisation des données.

La majeure partie des activités d'une collectivité territoriale est dorénavant effectuée au travers d'un recours de plus en plus poussé aux TIC. Or, bien peu d'entre elles ont une vision véritablement claire des risques juridiques liés à l'utilisation d'un SI, en dépit du fait qu'une pénétration clandestine d'un pirate informatique dans le réseau informatique d'une collectivité, ou qu'une utilisation frauduleuse d'un poste de travail par un agent, sont des risques susceptibles d'induire une mise en cause civile et surtout pénale de la hiérarchie administrative et des Elus au premier rang desquels le président de la collectivité ou le Maire.



## Toujours plus cyber-menacées : les collectivités territoriales

### Notes

1. Source : Guide « Les collectivités locales » de la CNIL.
2. Articles L.2131, al. 1 et 2 (Communes), L. 3131, al. 1 et 2 (Départements), L4141, al. 1 et 2 (Régions) et L 5211, al. 3 (EPCI).
3. Loi n°2007-297 du 5 Mars 2007 relative à la prévention de la délinquance.
4. Selon les modalités prévues dans le Décret n°2005-937 du 2 août 2005 pris pour l'application de l'article L. 211-7 du code de l'entrée et du séjour des étrangers et du droit d'asile et portant sur le traitement automatisé de données à caractère personnel relatif aux demandes de validation des attestations d'accueil.
5. Loi n°2000-230 du 13 Mars 2000 modifiant l'article 1316 du Code civil.
6. Art. 1316 al. 3 du Code civil.
7. Livre II du Code du patrimoine relatif aux archives.
8. Partie réglementaire du CGCT, Première partie, Livre IV, Ch. 1<sup>er</sup>.
9. Décrets n° 79-1037, 79-1038 et 79-1039 du 3 décembre 1979.
10. Loi n°78-17 du 6 janvier 1978, modifiée par la Loi n°2004-801 du 6 août 2004.
11. Décret n°2005-1309 du 20 octobre 2005.
12. [www.archivesdefrance.gouv.fr/gerer/textes](http://www.archivesdefrance.gouv.fr/gerer/textes)
13. [www.references.modernisation.gouv.fr](http://www.references.modernisation.gouv.fr)
14. Source : La lettre du cadre territorial, N°381 – Juin 2009.
15. Premier système d'exploitation de Microsoft.
16. « 5<sup>e</sup> enquête sur les Systèmes d'Information dans les collectivités territoriales », menée auprès de 2500 collectivités (Communes, EPCI, Départements et Régions) avec un taux de retour de 18%. (2008).
17. « Systèmes d'Information et collectivités territoriales », menée auprès des 110 plus grandes collectivités françaises (21 Régions, 19 Départements, 36 Villes et 34 EPCI). (2009).
18. Flux RSS (*Really Simple Syndication*) : format particulier de données, constamment mis à jour et visant à diffuser automatiquement des informations à l'intention des internautes selon un principe de « fil d'actualité ».
19. <http://www.lunion.presse.fr/article/marne/le-site-de-la-mairie-pirate>
20. [http://www.clichy-sous-bois.fr/jsp/site/Portal.jsp?article\\_id=154&portlet\\_id=118](http://www.clichy-sous-bois.fr/jsp/site/Portal.jsp?article_id=154&portlet_id=118)
21. Journal « Le parisien », édition du 27 octobre 2009 : <http://www.leparisien.fr/longjumeau-91160/le-reseau-informatique-de-la-mairie-pirate-27-10-2009-689371.php>
22. <http://nkm-blog.org/les-miseres-du-piratage/>
23. [http://www.lepoint.fr/politique/le-site-Internet-de-l-aeroport-de-montpellier-et-sarkozy-attaques-par-des-pirates-17-08-2010-1226038\\_20.php](http://www.lepoint.fr/politique/le-site-Internet-de-l-aeroport-de-montpellier-et-sarkozy-attaques-par-des-pirates-17-08-2010-1226038_20.php)
24. <http://www.libertaland.com/2010/03/nouvelles-attaques-de-sites-par-les-pirates-eymz-et-wazo/>
25. <http://www.crashdebug.fr/index.php/securite/1260-interview-daun-defaceur-repent>
26. [http://www.lavoixdunord.fr/Locales/Arras/actualite/Secteur\\_Arras/2010/08/04/article\\_croisilles-le-site-Internet-de-la-commun.shtml](http://www.lavoixdunord.fr/Locales/Arras/actualite/Secteur_Arras/2010/08/04/article_croisilles-le-site-Internet-de-la-commun.shtml)
27. <http://hightech.nouvelobs.com/actualites/20030616.OBS2313/la-ville-de-toulouse-porte plaintecontre-un-site-pirate.html>
28. <http://redaction.blogs.paris-normandie.fr/2009/05/14/balilove-la-mairie-de-toulouse-piratee/>
29. <http://www.clubic.com/antivirus-securite-informatique/virus-hacker-piratage/trojan-cheval-de-troie/actualite-343508-inculpes-piratage-compte-bancaire-mairie-états-unis.html>
30. <http://www.dhnet.be/infos/new-tech/article/181425/le-site-de-la-ville-de-rochefort-pirate.html>



## Rémy FÉVRIER

31. [http://www.rtb.be/info/medias/detail\\_le-site-de-l-union-de-la-ville-et-des-communes-pirate?id=5584623](http://www.rtb.be/info/medias/detail_le-site-de-l-union-de-la-ville-et-des-communes-pirate?id=5584623)
32. L'Ethical Hacking est une pratique SSI qui consiste à tester la vulnérabilité des SI en détectant et exploitant les failles potentielles de ces derniers, puis de proposer des mesures correctrices.
33. Uniform Ressource Locator : lien d'accès à un site web particulier.
34. Audit, Conseil, Installation & Sécurisation des Systèmes d'Informatiques.
35. P2P : Peer-to-Peer (ou Pair à Pair) : Réseau d'échange et de partage de fichiers entre internautes.
36. Technique d'intrusion particulière consistant à récupérer des informations directement auprès des utilisateurs d'un SI en tablant sur leur crédulité.
37. Ou « Cheval de Troie » : logiciel invisible pour l'utilisateur et qui va effectuer des opérations programmées à l'avance.
38. Ou « Porte dérobée » : canal logique ouvert depuis le poste cible à l'insu de son utilisateur.
39. Logiciel d'enregistrement de l'ensemble des séquences de touches tapées sur un clavier.
40. Adresse de connexion au réseau Internet attribuée par le fournisseur d'accès. Identifie l'ordinateur lors de sa connexion. Peut être fixe ou dynamique.
41. Absolute Software corporation: Human Factor in Laptop Encryption Study 2010, France. Étude réalisée auprès de 309 praticiens en informatique et 366 managers.
42. Source : Creative commons.
43. Système d'exploitation libre et alternatif à Microsoft Windows®.
44. Circulaire du 15 Mai 1996 relative à la communication, à l'information et à la documentation des services de l'État sur les nouveaux réseaux de télécommunication.
45. Rapport «Pour une administration électronique citoyenne, Méthodes et moyens», 2000.
46. Crozier M. et Friedberg E., L'Acteur et le système. Ed. Seuil. Paris, 1977.
47. PIERRE DE LA COSTE, Bâtir l'administration en réseau autour du citoyen, 2003.
48. Circulaire du 12 septembre 2003 relative au développement de l'administration électronique.
49. 7,4 Millions de déclarations souscrites en ligne en 2007. (Source : Ministère du Budget).
50. Sondage IPSOS effectué par Internet puis étude de cadrage réalisée par téléphone auprès de 2 000 personnes.
51. « Les Français et l'administration électronique en 2008 : Performance des services publics en ligne et fossé numérique », Capgemini Consulting/TNS Sofres (Sept. 2008).
52. Rapport « La diffusion des TIC dans la société française » (2009), réalisé à la demande du Ministère de l'Economie, de l'Industrie et de l'emploi et de l'Autorité de régulation des communications électroniques et des postes.
53. Nicolas Sarkozy, Discours inaugural du 1<sup>er</sup> sommet Franco-allemand des TIC, 3 Mars 2008.
54. Baromètre Ineu Consulting-La Gazette.
55. Étude « Les priorités de simplification vues par les collectivités territoriales » menée par l'Institut BVA auprès de 804 collectivités (500 communes/230 EPCI, 56 départements, 18 régions). Novembre 2008.
56. Enquête « TIC et collectivités en Nord-Pas de Calais », Région Nord-Pas de Calais, 2001.
57. [www.edile.fr](http://www.edile.fr), « Les collectivités locales face à l'administration électronique ».
58. Loi n°2005-102 du 11 février 2005.
59. [www.references.modernisation.gouv.fr/le-rgaa-en-ligne](http://www.references.modernisation.gouv.fr/le-rgaa-en-ligne)
60. Issu de l'Initiative sur l'Accessibilité du Web (Web Accessibility Initiative) lancée en 1999 par le « Word Wide Web Consortium ».
61. [www.references.modernisation.gouv.fr/rqi-interoperabilite](http://www.references.modernisation.gouv.fr/rqi-interoperabilite)
62. Capgemini Consulting/TNS Sofres, op cit.
63. [www.cnil.fr](http://www.cnil.fr)



## Toujours plus cyber-menacées : les collectivités territoriales

64. www.ssi.gouv.fr
65. Région Nord-Pas de Calais, DREAM+, Dossier de présentation de l'action, 2006.
66. OCDE, Rapport (2003) « Promesses et limites de la démocratie électronique », Les défis de la participation citoyenne en ligne.
67. Vedel, Thierry (2003) : « L'idée de démocratie électronique : origines, visions, questions », paru dans Le désenchantement démocratique, Perrineau Pascal (dir.), La Tour d'Aigues, Ed. de l'Aube, p243-266.
68. T. Vedel, op. cit.
69. Rosenvallon, P. « La ContrE-démocratie. La politique à l'âge de la défiance », Paris, Seuil, 2006.
70. Sondage Opinionway : « E-Démocratie et E-administration », réalisé pour le Forum Mondial de la Démocratie et de l'Administration Electronique, Juillet 2006.
71. Anne Le Bot, « Entre idéalisme, indifférence et cynisme, y a-t-il une place pour la démocratie électronique territoriale », Mémoire de M2 web éditorial, Université de Poitiers, 2001.
72. Centre d'Analyse Stratégique : « La participation des citoyens et l'action publique », La documentation française, 2001.
73. Joseph Shumpeter : « Capitalisme, socialisme et démocratie », 1942, trad. fr. 1951, rééd. Payot.
74. Directeur Général du Centre d'Analyse Stratégique.
75. Professeur à l'Oxford Internet Institute, Université d'Oxford.
76. Expérience de participation citoyenne menée par la région Nord-Pas-de-Calais dans le cadre de l'évaluation des Fonds de participation des Habitants.
77. Déclaration dite « de Valencia ».
78. <http://www.alain-lambert-blog.org/2008/02/1525-a-quoi-sert-le-code-des-marches-publics/>
79. Organisme créé en 2005 et dépendant du Ministère de l'Economie et des Finances
80. [http://www.economie.gouv.fr/directions\\_services/daj/marches\\_publics/oep/recensement/Presentation\\_recensement\\_2009.pdf](http://www.economie.gouv.fr/directions_services/daj/marches_publics/oep/recensement/Presentation_recensement_2009.pdf)
81. [http://www.minefe.gouv.fr/directions\\_services/daj/marches\\_publics/oep/recensement/place\\_pme\\_dansmp\\_2009.pdf](http://www.minefe.gouv.fr/directions_services/daj/marches_publics/oep/recensement/place_pme_dansmp_2009.pdf)
82. Articles 33, 57, 58 et 59 du Code des marchés publics.
83. Articles 34, 60 à 64 du Code des marchés publics.
84. Au sens de l'ordonnance n°2005-649 du 6 juin 2005.
85. Article 28 du Code des Marchés Publics.
86. Articles 34 et 60 à 64 du Code des Marchés Publics.
87. Article 35 du Code des Marchés Publics.
88. Article 36 du Code des Marchés Publics.
89. Décret n°2006-975 portant code des marchés publics (CMP 2009).
90. Article 1316-1 du Code Civil.
91. Article 1316-4 du Code Civil.
92. Article 1316-4, al. 2 du Code Civil.
93. Note « Les outils de la dématérialisation des marchés publics formalisés ».
94. Voir décret n°2002-535 du 18 avril 2002 et arrêté du 26 juillet 2004 du Ministre chargé de l'Industrie.
95. « La perception de la dématérialisation », enquête qualitative TNS Sofres, oct. 2007.
96. Etude quantitative sur la dématérialisation dans les marchés publics, Sept 2001.

# BULLETIN D'ABONNEMENT OU DE RÉABONNEMENT

## Sécurité Globale

### Bulletin d'abonnement ou de réabonnement

À retourner accompagné de votre règlement aux  
 Éditions ESKA – 12, rue du Quatre-Septembre, 75002 PARIS  
 Tél. : 01 42 86 55 65 – Fax : 01 42 60 45 35

<http://www.eska.fr>

M, Mme, Mlle \_\_\_\_\_ Prénom \_\_\_\_\_

Société/Institution \_\_\_\_\_

N° \_\_\_\_\_ Rue \_\_\_\_\_

Code postal \_\_\_\_\_ Ville \_\_\_\_\_

Pays \_\_\_\_\_

Adresse électronique \_\_\_\_\_

#### TARIFS D'ABONNEMENTS\*

|                      | France particulier             | France société/<br>institution | Etranger particulier           | Etranger société/<br>institution |
|----------------------|--------------------------------|--------------------------------|--------------------------------|----------------------------------|
| 1 an (2016)          | <input type="checkbox"/> 107 € | <input type="checkbox"/> 135 € | <input type="checkbox"/> 129 € | <input type="checkbox"/> 161 €   |
| 2 ans (2016 et 2017) | <input type="checkbox"/> 191 € | <input type="checkbox"/> 239 € | <input type="checkbox"/> 229 € | <input type="checkbox"/> 286 €   |

\* Abonnements souscrits à l'année civile (janvier à décembre).

Je souscris un abonnement pour       1 an       2 ans

Je joins mon règlement de \_\_\_\_\_ Euros

par chèque bancaire à l'ordre des Éditions ESKA

par virement bancaire aux Éditions ESKA – BNP Paris Champs Elysées 30004/00804/  
compte : 00010139858 36

par carte bancaire : merci d'indiquer votre numéro de compte et la date d'expiration

N° carte bancaire :  Visa     Eurocard/Mastercard

\_\_\_\_\_    \_\_\_\_\_    \_\_\_\_\_    \_\_\_\_\_

Date d'expiration : \_\_\_\_\_ Signature :

#### Derniers numéros parus

Sécurité globale 2 | 2015 (nouvelle série) : Bandes, Braquages, Terreur

Sécurité globale 1 | 2015 (nouvelle série) : Iran 2015 : Qui gouverne à Téhéran (et comment) ?

Sécurité globale 25-26 | 2013 : La France face à ses ESSD

Sécurité globale 24 | 2013 : Cyber : la guerre a commencé (2<sup>e</sup> partie)

Sécurité globale 23 | 2013 : Cyber : la guerre a commencé (1<sup>re</sup> partie)

Sécurité globale 22 | 2012 : La Suisse : nation militaire

Sécurité globale 21 | 2012 : L'eau, enjeu de sécurité et de développement

**ÉDITIONS ESKA**  
 12 rue du Quatre-Septembre - 75002 Paris, France  
 Tél. : 01 42 86 55 65 | Fax : 01 42 60 45 35  
<http://www.eska.fr>



# « Police prédictive » : les belles histoires de l'Oncle Predpol

*Xavier RAUFER*







# « Police prédictive » : les belles histoires de l'Oncle Predpol

Xavier RAUFER

## 1. "Police prédictive" : bobards et réalité

Le scénario est constant. Soudoyé ou naïf, mais toujours extatique, un journaliste annonce la Bonne Nouvelle. À l'automne 2015 encore, c'est "Kevin", du site *Science Post*. Le titre : "Une intelligence artificielle capable de prédire les crimes est en développement" – pas moins. Suit l'inévitable référence à "*Minority Report*" et un déluge de mots techniques visant à fasciner et sidérer le lecteur. On va "arrêter les criminels... avant qu'ils ne commettent de crime". De la science-fiction ? Non, c'est pour demain.

Sauf qu'aujourd'hui, la vraie incertitude n'est pas plus modélisable qu'au temps d'Aristote (sur lequel repose encore notre acception du temps). En clair : une base

documentaire contenant tout sur le terrorisme depuis l'antiquité jusqu'au 10 septembre 2001, ne prédira en rien les attentats du 11 septembre. On rougit de devoir rappeler que si le connu d'hier résolvait mécaniquement l'inconnu de demain, tout le monde gagnerait à la loterie...

97

À les lire, les naïfs propageant ces bobards pour le compte de marchands de *software* semblent ignorer le fonctionnement des logiciels de "police prédictive". Aidons-les : des algorithmes brassent des données sur des crimes passés pour en annoncer de futurs. Or – insistons – cela est absolument *impossible*. Que font vraiment ces logiciels ? Ils assument que, comme hier un crime s'est commis à tel endroit, demain, il s'en commettra peut-être un autre. Ce raisonnement n'est pas de la prédition, mais du *wishful thinking*.



Xavier RAUFER

98

Et quelle crédulité chez ceux qui diffusent ces contes de fées : en août 2015, "Le Parisien" nous assénait ainsi ainsi qu'à Munich, l'usage d'un logiciel de "police prédictive" a fait "baisser les cambriolages de 30%". Vérifions, avec les statistiques officielles du *Bundeskriminalamt* (Office fédéral allemand de police criminelle). De 2003 à 2012, les cambriolages augmentent de 16,9% en Allemagne. Mais en 2014, alors qu'on installe à Munich le fameux logiciel-miracle ? Augmentation encore, de 1,8% – pas même une stagnation. Clairement, l'usage de la baguette magique "prédictive" fait juste jouer l'effet de déplacement : se sentant observés, les cambrioleurs changent de crèmerie et partent piller la ville d'à côté. Mais à l'échelle nationale, effet zéro.

Au mieux, le logiciel-miraculeux permet à la police d'ordonner son travail et d'intervenir plus souvent au bon endroit et au bon moment – mais rien de "prédictif" là-dedans, bien sûr. En prime, cet effet positif est forcément temporaire. Depuis l'âge des cavernes, le réflexe humain est constant : s'il se sent observé, l'homme modifie son comportement – qu'on le regarde à l'œil nu ou électroniquement. Ainsi, vous payez des dizaines de milliers d'euros un logiciel-miracle qui, six mois plus tard, n'annonce plus rien de pertinent. Cela s'appelle une arnaque.

La recherche américaine de pointe confirme ce diagnostic. Discrètement, IARPA lançait en mars 2015 une étude sur

un outil informatique visant à "prévoir des événements rares". Rappelons ici qu'IARPA (*Intelligence Advanced Research Projects Activity*) est le laboratoire *high tech* du renseignement des États-Unis. Si IARPA cherche cet outil informatique, c'est bien sûr qu'il ne l'a pas. Or s'il était vrai qu'"une intelligence artificielle capable de prédire les crimes soit en développement", IARPA aurait fait 95% du chemin, car les infréquents crimes graves sont de ces "événements rares" que le renseignement US aimeraient prévoir.

Conclusion : les actuels "logiciels de police prédictive" naïvement vantés par certains médias sont considérés comme de la daube par l'élite américaine de la recherche scientifique de renseignement. Ce qu'il fallait démontrer.

## 2. Plus largement, l'hyper-technologie peut-elle remplacer l'intelligence humaine ?

Il existe en effet des idolâtres de l'intelligence des machines, vantant la capacité des ordinateurs à tout résoudre bien plus vite que la pauvre cervelle humaine. Or face à de tels élans amoureux, le vrai problème ne réside pas dans le progrès technique – Merveilleux ? inquiétant ? Il est là, c'est ainsi. Nul ne veut revenir à la pierre taillée et l'auteur moins encore, enchanté qu'il est du confort de travail offert par cette réelle prothèse du cerveau hu-



## « Police prédictive » : les belles histoires de l'Oncle Predpol

main qu'est l'informatique, de bureau ou portable.

Le problème n'est pas non plus dans l'exaltation mystique de Silicon Valley devant ses cyber-créations, l'idée qu'un jour Super-Google règnera sur le monde, empêchant une bête humaine enfin domptée de sévir comme elle le fait depuis toujours. Les Californiens ont l'âme techno-religieuse : laissons-les jouer avec leurs cyber-sectes à la "Singularity".

Le vrai problème, encore, est le traitement que la presse-des-milliardaire (les quotidiens rachetés par de grosses fortunes) réserve à ces affaires. Devenus les serviteurs de milliardaires de la nouvelle économie, d'ex-journalistes désormais voués aux relations publiques réservent un accueil exatique à tous ces progrès techniques, e-commerce, etc. – par une amusante coïncidence, à tout ce qui par ailleurs, enrichit les magnats qui les emploient.

Exemple parmi d'autres : la publicité faite dans ces médias pour les logiciels de "police prédictive" – en fait ni plus ni moins efficaces que ceux des sites de rencontre en ligne, car usant des mêmes algorithmes. Là encore, nulle critique ! L'extase hi-tech, obligée et unique voie du progrès. Qui héberge un doute n'est qu'un ringard.

Pour être édifié, il suffit de lire la presse-des-milliardaires depuis qu'en mars 2014, le vol MH 370 de Malaysian Airlines a disparu corps en bien. Depuis lors, nous

avons vécu en direct l'effarant échec d'*Eye in the sky*, Washington en étant réduit à implorer les internautes d'aller scruter les océans. Et bientôt deux ans après le drame on ne sait en fait, toujours rien du sort de cet aéronef. Or là-dessus, la presse dite d'information se tait.

Dans un premier temps, on crie au miracle. Vient le désastre et les mêmes regardent ailleurs. On nous a certes beaucoup parlé de cet avion et du mystère de sa disparition. mais pas un mot sur le fait que les merveilleux systèmes High-tech, soi-disant capables de lire, depuis le fin fond des cieux, la marque d'un paquet de cigarettes jeté au sol, ont manifesté une totale impuissance à retrouver un avion de 300 tonnes et de 70 mètres de longueur et d'envergure. Le fait d'avoir enseveli dans le silence cet échec flagrant d'un high-tech que ces médias encensent chaque jour, là est le vrai scandale.

99

### 3. Extase médiatique et "police prédictive"

Dans le domaine de l'immobilier, avez-vous aimé l'arnaque des *Subprimes* ? Alors, vous devriez adorer la suivante, celle de la "police prédictive" en matière de sécurité. Cette arnaque emballé bien sûr les médias. Le *Journal du Dimanche* s'ébahit devant "La machine à déceler le crime", *Le Monde Magazine* vante "Le logiciel qui prédit les délits", etc. A y regarder d'un



Xavier RAUFER

peu près, l'enthousiasme semble moins spontané qu'il n'y paraît, puisque tous ces articles sont quasi-identiques et sentent la com' à un kilomètre.

Indice sérieux, ils évoquent pour la plupart le film *Minority Report*, tiré d'une nouvelle de Philip K. Dick. Film dont à l'évidence, nos enthousiastes journalistes ignorent tout, car il n'a rien à voir avec le "*predictive policing*" ! Dans l'œuvre de Dick, des "voyants" ("*Precogs*"), pressentent d'imminents homicides et alertent ensuite la police, ce qui est tout différent.

Venons-en aux cyber-Madoff prétendant "prédir" les crimes, attentats, etc., pour souligner d'emblée cette imparable évidence (développée plus bas) : aujourd'hui encore, et durablement, certains phénomènes irréductiblement complexes sont *imprédictibles* ; exemple, les séismes. D'autres phénomènes à risque seraient-ils, eux, prévisibles ? Au mieux, faiblement – voyons plutôt.

Dans les domaines où l'on pense savoir prédire, et où on le fait de longue date : économie-finance, météorologie, séismes, etc., le bilan de la prévision est plutôt catastrophique, dès lors qu'il s'agit de risques. Prouvons-le : avant la crise des *Subprimes* les agences de notation (Standard & Poor, Moody's,etc.) disposaient toutes d'estimations chiffrées du risque de défaut de remboursement par les acheteurs de maisons à crédit.

Ces risques étaient alors estimés grâce à l'analyse quantitative, discipline issue de la physique des probabilités, supposée maîtriser "scientifiquement" les risques de *trading*. Or quand éclata la crise, le risque réel se révéla... *deux cent* fois pire que les prévisions des agences ! Se croire hors risque grâce aux estimations des agences de notation, ricana alors un expert, revenait à se protéger du feu nucléaire en s'enduisant de crème solaire...

Ceci n'empêche pas les Cyber-Madoff de nous offrir le nouveau miroir aux alouettes qu'aux États-Unis, on nomme "Crime predictor" ou "Predictive Policing" (*Pred Pol* pour faire *cool*). Il s'agit de "logiciels d'analyse prédictive" supposés prévoir les crimes, et même, pourquoi pas, les crises politiques, les révolutions ou les attentats.

Lisons plutôt les articles que la presse leur consacre : "Le logiciel qui prédit les délits... XXX (*la marque du logiciel*) débarque au Royaume-Uni. Un logiciel qui "prédit à quel endroit les criminels peuvent attaquer, et quand", ou qui peut "prédir où des cambriolages, vols, agressions, vont se produire dans l'avenir... Avec des résultats convaincants."

Or les Cyber-Madoffs qui, pour des médias naïfs, prétendent "prévoir les crimes", usent de l'analyse quantitative et des "algorithmes prédictifs" mêmes qui ont provoqué l'effondrement de Wall Street ! Mais au fait, comment nourrit-on ces "logiciels prédisant les crimes" ? Avec un



## « Police prédictive » : les belles histoires de l'Oncle Predpol

“algorithme conçu pour prédire où et quand un crime va se produire, grâce à une base de données *recensant les infractions passées*” ; ou par “l'utilisation de *statistiques historiques*” ; ou en usant de “bases de données criminelles *datant des années 1960*”. Tous ces logiciels tirent sans exception leurs références du passé. Leur carburant est *strictement* rétroactif.

On ramasse tout ce qui traîne sur Internet en habillant cette récolte, opérée plus ou moins à l'aveuglette, de noms pompeux-high tech : *Big Data... Data Mining...* puis l'on passe cette matière brute dans une moulinette à algorithmes. Résultat plausible : sans doute une possible et momentanée optimisation du travail policier – en attendant que les bandits fassent, comme d'usage, jouer l'effet de déplacement en leur faveur – mais capacité de prédiction, certainement pas – et voici pourquoi.

Car posons ici la question cruciale – qu'ignorent (sciemment ou non) nos enthousiastes médias : ce qu'on sait du passé permet-il de prévoir le futur ? Par exemple : le temps qu'il faisait hier certifie-t-il celui de demain ? D'évidence non, du fait de *l'incertitude*, immuable et non-négociable élément de toute prévision – que les Cyber-Madoff et leurs thuriféraires se gardent bien d'évoquer. Et même, les choses ne risquent pas de s'arranger dans l'avenir, par amélioration progressive des systèmes type *Pred Pol* – mais ne peuvent à l'inverse qu'empirer. Pour les experts en effet, les algorithmes et logiciels dits “prédictifs”

possèdent une capacité forte à pré-formater la réalité, à influer sur elle – suscitant donc leur propre validité et ainsi, persuadant le client que tout marche au mieux – alors que sur le terrain, dans la vraie vie, là où opèrent les vrais voyous et dealers, rien n'a vraiment changé.

Mirage technologique, ces “logiciels de prédiction des crimes” ne font en fait que prolonger des courbes. Ils partent pour cela d'une idée simple : ce qui était là hier, sera là demain. Comme lundi, des bandits ont opéré dans tel coin, montons mardi une embuscade là où le logiciel l'indique et hop ! On les pince à coup sûr. Or cela ne relève nullement de la prévision, mais de la pétition de principe.

Enfin, les algorithmes type *Pred Pol* servent aussi à des prestations d'un tout autre genre : les rencontres en ligne sur Internet. À leur propos, voici l'avis d'un expert : “les gens paient pour ces services de rencontres quoique, après examen, les algorithmes supposés trouver leur partenaire idéal ne marchent sans doute pas”. Après les amoureux numériques, les Cyber-Madoff ciblent maintenant les policiers et les élus. Bienvenue au club des gogos.

### 4. Plus largement : peut-on tout prédire ?

Parmi les pires excès de cette cyber-propagande, le domaine du prédictif. De gros





Xavier RAUFER

ordinateurs, des algorithmes appropriés, le *Big Data* – tout cela réuni en un dispositif approprié, permettrait de prédire tout et le reste... Grâce à Wikipedia par exemple, et à un modèle mathématique approprié, on pourrait désormais annoncer *avec précision, un mois à l'avance*, le succès d'un film au *box-office*. Une recette également utilisable dans l'agroalimentaire, pour les sodas et les sandwiches nouveaux.

Dès 2030 annoncent même certains gourous, nous disposerons de planétaires machines-à-prédire (*"global precognition machines"*) pour débarrasser le monde de tout le négatif qui l'encombre. D'ores et déjà, racontent des VRP du logiciel, des spécialistes disposent du pouvoir – l'expression est trop belle en anglais – *"to predict whether you're going to click, buy, lie or die"*. Pour ces VRP, prédire le comportement humain permet de prendre de meilleures décisions, dissipe les risques financiers, renforce la santé publique, détruit le *Spam*, stimule les ventes et bien sûr renforce la lutte contre le crime. (Rien à ce jour sur un quelconque effet vermiclige, ou capacité à guérir les écrouelles. Mais espérons.)

Intéressons-nous donc plus précisément à la "prédiction du crime". Depuis 2010 environ, des articles éclosent dans les médias papier ou électroniques du monde anglo-saxon ; tous nous racontent la même histoire. Bientôt, il en ira du crime comme de la météo... Des logiciels spécialisés comme PredPol permettront à la police de pré-dire

les crimes. Et ça marche déjà en Californie ! "Quand le système a été testé, la criminalité constatée a baissé de 12% et les cambriolages, de 27%". Et tout le monde se précipite : Silicon Valley bien sûr, les militaires, l'université, l'édition et même Hollywood.

Les livres d'abord : *"Predictive analytics for dummies"* est assez caractéristique du lot. Sur le ton de l'enthousiasme, de l'affirmation sans nuances, les auteurs nous présentent le Saint-Graal. Mais que contient en fait ce livre ? Des banalités-marketing pour école de commerce. On y prolonge des courbes, rien de plus. Surtout, dans une table des matières détaillée de 7 pages, et dans un index qui en fait le double, on ne trouve rien, pas un mot, ni sur le *temps*, ni sur la *temporalité* – concepts d'évidence cruciaux dans tout le domaine du "pré" (prédir, prévoir, présumer, etc.).

Second ouvrage typique : *"Predictive analytics"*, œuvre de marchand de gadgets où ce qu'est une *prédiction* n'est jamais défini. Car observer des comportement, ou des habitudes, user de sa jugeote, optimiser, prolonger les courbes, estimer des probabilités : est-ce cela, prévoir ou prédire ?

Exemple, quand un magasin voit une cliente acheter une robe de grossesse, est-il besoin de mobiliser un super-calculateur pour lui proposer ensuite un biberon et des couches ? De même, quand un lecteur commande un roman policier sur un site,

## « Police prédictive » : les belles histoires de l'Oncle Predpol

faut-il un cyber-génie pour lui en suggérer d'autres ? N'est-on pas là plutôt dans le classique "*Customers who bought this item also bought...*" des sites marchands ?

Car voilà comment fonctionne ce dispositif plutôt grossier, qui tente de donner du sens à des données diffuses, chaotiques et recueillies en vrac. Un système qui a tout à voir avec de l'optimisation, ou du *marketing* de bon sens, mais rien avec de la prévision. Cas concret : avec la vitesse et la puissance de l'informatique, ici, indéniablement supérieures au cerveau humain, un logiciel trie en quatre catégories les clients du *e-commerce* :

- A. Ceux qui achètent un produit en négligeant la publicité : *laissés de côté*,
- B. Ceux qui n'achètent un produit qu'en l'absence de publicité : *laissés de côté*,
- C. Ceux qui flânen sur Internet sans acheter en ligne : *laissés de côté*,
- D. Ceux qui n'achètent rien sans publicité, mais achètent s'ils en voient : ces "réceptifs confirmés" sont placés dans une base de donnée spécifique, puis bombardés de pub'.

La répétition du mot "*predictive*" dans *Predictive analytics* veut exercer un effet hypnotique sur le lecteur. Mais rien n'y permet de vraiment prédire quoi que ce soit. Et puisque les collections portant ce

titre sont à la mode, on est plutôt ici dans "le behaviorisme pour les nuls".

Après les livres, la stratégie : on apprend ainsi en novembre 2013 que l'armée américaine expérimente en Afghanistan un "nouveau modèle prédictif", *Global Database Events*, conçu par un professeur de sciences politiques de l'Université d'Etat de Pennsylvanie. Ce logiciel "recueille des nouvelles sur Internet" et "catalogue des événements, des élections locales jusqu'aux génocides". Il en extrait des "prédictions à court et à long terme", utiles pour "gérer les crises" et "prévoir les niveaux de conflits en Afghanistan".

103

Les séries-télé se joignent à la meute : diffusé sur TF1, "*Person of Interest*" a eu en 2012, 14 millions de téléspectateurs en moyenne sur CBS-États-Unis. Dans cette série "un génie de l'informatique invente une machine sachant déjouer les attentats", qui "prédit aussi les crimes crapuleux". Quelle machine sympa ! Un "ordinateur intelligent et même doué d'émotions... une intelligence artificielle touchante"... Aux prises avec "le gouvernement, la mafia, les policiers corrompus de New York", son héros "prévient bien sûr les crimes avant qu'ils ne soient commis". Une ambiance, dit la critique, "à la *Minority Report*". Notons la référence à ce film, qui est l'immuable marqueur de l'escroquerie au prédictif. Même les universités américaines, se ruent désormais pour proposer aux étudiants "des certificats ou Masters en analytique prédictive".



Xavier RAUFER

104

### "Prédire le crime" : ce que racontent étourdiment les médias

Pour tous ces articles, la "police prédictive" "réduit la criminalité par l'analyse de données sur des crimes et le lieu de leur commission"... "S'agissant de personnes à risque, la méthode prédictive peut être efficace"... "Par voie électronique, le Maryland génère des prédictions sur les malfaiteurs placés en liberté provisoire, pour savoir qui tuera et qui sera tué"... "Des chercheurs et des policiers ont conçu des systèmes prédictifs qui, parmi les individus déjà condamnés pour homicide, prédit lesquels tueront encore"... "Grâce à des analyses informatiques sophistiquées, on peut prédire où et quand des crimes seront commis"... "Des programmes de police prédictive fondés sur des algorithmes et des données historiques, estiment la localisation et la nature de crimes futurs"...

Dans ces articles, notons une forte odeur de "communication", pas une critique – au point qu'on dirait plutôt de la publicité rédactionnelle : "Le logiciel de police prédictive est deux fois plus efficace qu'un analyste humain disposant des mêmes données"... "Dans un secteur de Los Angeles, un outil de police prédictive a fait, en 5 mois, baisser d'un tiers les cambriolages"... Dans tous les États-Unis, des dizaines de services de police ont déjà acquis de tels dispositifs"... Pour *The Police Chief*, organe de la puissante *International Association of Chiefs of Police*, "la police prédictive marque le début d'une ère nouvelle".

### De mieux en mieux : la "justice prédictive"

Décidément mis à toutes les sauces, le "prédictif" a également contaminé la justice. Car de fait les magistrats s'interrogent fort légitimement : ce détenu en instance de libération peut-il commettre un crime grave dans les prochaines années ? Ce primo-délinquant a-t-il l'étoffe d'un multirécidiviste ? Or d'usage, ces juges n'ont que leur expérience, ou leur flair, pour les aider. Et si des logiciels "prédictifs" pouvaient contribuer à sélectionner les détenus avec pertinence ? orienter leurs choix pour des peines avec sursis, des libérations conditionnelles, sans risque pour la société ?

Bref : peut-on concevoir un système objectif permettant *à la fois* de multiplier les libérations conditionnelles et de réduire le nombre des récidives ? De bien choisir les détenus envoyés dans des programmes de réinsertion, durant la peine ou après celle-ci ? De décider (dans un système de *common law*) qui reste incarcéré, et pour combien de temps ? De détecter les jeunes détenus influençables à ne surtout pas incarcérer avec des criminels confirmés ?

Aux États-Unis, 4/5<sup>e</sup> des comités d'évaluation de libération sous condition utilisent désormais de tels logiciels "prédictifs". Qu'y introduit-on pour évaluer un détenu ? Son âge, son sexe, ses antécédents ; la date de sa première arrestation, son éducation, les infractions qu'il a com-



## « Police prédictive » : les belles histoires de l'Oncle Predpol

mises, son comportement en prison ; aussi, le casier judiciaire de ses plus proches amis et le résultat des tests psychologiques qu'il a subis ; et même, l'éthylique de sa mère durant sa grossesse. Ensuite, on compare avec des profils analogues.

Que des décisions soient prises sur la base de tels calculs peut inquiéter mais – se doit de préciser ici le criminologue – un peu moins cependant quand on a lu l'effrayante étude “*Extraneous factors in judicial decisions*” (Princeton, février 2011) qui, ayant comparé des centaines de cas, démontre qu'en fin de matinée, des juges américains affamés tendent à condamner plus sévèrement que quand ils sont repus, deux heures plus tard...

Aléa informatique, aléa stomacal... Aléa toujours. Il demeure que tout ce qui relève de la justice, ou de la police, “prédictives” repose exclusivement sur du rétrospectif : “Les modèles prédictifs analysent des données *historiques...*”, “Nous collectons toutes ces données dans des occurrences passées...”, etc. Et là, commencent les problèmes conceptuels.

### 5. Comment fonctionnent les logiciels prédictifs ?

Vu le prix, 73 000 dollars pour acquérir un logiciel de “police prédictive”, plus ensuite 45 000 dollars d'abonnement annuel, il importe de voir comment tout cela

marche. Là encore, tous les articles publiés fournissent les mêmes explications. On commence toujours par saisir “toutes les données sur des crimes commis, et leur localisation, remontant à l'année XXX” ; ou bien “on analyse les dossiers d'environ 1,5 million de crimes commis de 2003 à 2012”... Pourquoi ? Parce que “les infractions à venir seront souvent commises sur les lieux d'anciens délits”. Là, le criminologue sursaute pour la première fois.

Les algorithmes maintenant. Docilement, les journalistes ou publicitaires ayant rédigé les articles sur la “police prédictive” répètent la même leçon : “l'algorithme comprend (*au sens de “digère”*) le schéma criminel et produit une prédition”... Ici, second sursaut du criminologue.

Preuve, ajoutent ces thuriféraires, que l'affaire est sérieuse “ces algorithmes sont fondés sur les modèles de prédition des séismes” (*variante*) sur les modèles de prédition des répliques des séismes”. Une “preuve” d'efficacité qui sans cesse revient, article après article. Là, le criminologue effectue un véritable bond car il sait, et le prouvera plus bas, que *les séismes sont, à ce jour, absolument imprédictibles*, ce que nul des rédacteurs des contes de fées précités ne s'est un instant avisé de vérifier.

Mais bien sûr, cela n'empêche pas l'Amérique du Sud de se lancer dans l'aventure : Au Chili, des ingénieurs “mê-



Xavier RAUFER

lant la criminologie à la modélisation mathématique”, ont entrepris de prédire en quels points de la frontière terrestre (en effet gigantesque, 6 170 kilomètres) du pays, se produiraient des crimes et des migrations illégales. Au Brésil, au printemps 2014, la ville de São Paulo acquiert le système *Detecta* de Microsoft, qui permet de combattre le crime en “agrégant des données” et en “créant entre elles des associations automatiques”. Les policiers de la ville sont dotés d’ordinateurs portables, tablettes et smartphones pour accéder au système, et orienter ainsi leurs patrouilles dans un esprit préventif.

106

Mais pourquoi se borner à l’Internet ? Patrouiller sur les réseaux sociaux peut aussi contribuer à “prédir le crime”. Comment ? Pour le *Predictive Technology Lab* de l’Université de Virginie, *Twitter* peut en effet “prédir” certains types de crimes. Dans la revue scientifique *Decision Support Systems* de mars 2014, les chercheurs de ce laboratoire affirment que des *Tweets* géo-localisés (qu’on peut donc situer finement), peuvent “prédir de 19 à 25 types d’infractions : harcèlement, vols, agressions...”. Comment cela ? “Si assez de *twitteurs* annoncent vouloir se saouler dans le même secteur, alors on peut y “prédir” des infractions liées à l’alcoolisme”. Il faut en outre comparer ces analyses *Twitter* avec “les concentrations d’actes criminel historiquement fortes”. Cette opération relève-t-elle un seul instant de la prévision ? Non, on le verra plus bas.

Résumons : l’analyse prédictive fonctionne selon le dispositif suivant : *data mining* (recherches de données présentes sur Internet, mais souvent cachées) + statistiques + algorithmes sophistiqués et logiciels spécifiques (*mining tools*) = modélisation, supposée pré-dire.

#### • Ces logiciels sont-ils sérieux ?

En juger nécessite de préalablement fournir au lecteur des éléments contextuels pertinents. Les voici.

– D’abord, le point le plus décisif. Aujourd’hui et pour longtemps encore, l’incertitude... l’entropie.. l’aléatoire.. le désordre (au sens scientifique), relèvent de l’imprévisible et de l’imprédictible. Pour le dire autrement, tout ce qui est à un moment donné possible, n’advient pas nécessairement. Ce que Donald Rumsfeld, ministre américain de la défense lors de la guerre d’Irak, exprima fameusement en ces termes : “Il y a le *connu-connu*, le domaine de ce qu’on sait et sait savoir. Il y a le *connu-inconnu*, ce qu’on sait ne pas savoir. À quoi s’ajoute *l’inconnu-inconnu*, ce qu’on ignore sans le savoir”.

Affirmer que l’observation algorithmique permet de modéliser ou de standardiser l’inconnu-inconnu relève clairement de l’escroquerie intellectuelle. Car le *réactif* n’est jamais *prédictif* : sinon, avoir en sa possession la liste de tous les



## « Police prédictive » : les belles histoires de l'Oncle Predpol

tirages passés d'une loterie permettrait de gagner au coup suivant. Or si tout ce qu'on introduit dans une moulinette algorithmique provient du passé, il n'en sort qu'une probabilité, souvent maladroite, prolongeant plus ou moins grossièrement des courbes : les criminels étaient là hier à telle heure, ils y seront donc aussi demain.

- Depuis qu'existent les premiers ordinateurs, l'idée de prédire taraude les savants. Au début de la seconde Guerre Mondiale, Norbert Wiener, père de la cybernétique, tenta-t-il de concevoir un modèle prédisant les évolutions des avions de chasse allemands, pour pouvoir les abattre plus aisément. Ce fut un échec, par manque, dit-on alors, de capacités de calcul.
- Depuis trente ans et plus, des organismes de recherche militaire, comme la Darpa aux États-Unis, cherchent, à coup de millions de dollars, comment agréger, combiner, maintes données d'apparence déconnectées, hétéroclites ; pour y découvrir des corrélations permettant de poser des diagnostics ou de faire des prédictions, par exemple sur de futures émeutes, de futurs attentats.

En 2010, la Darpa a lancé ainsi un programme "Data to decisions" doté d'un budget de 92 millions de dollars. Il visait à concevoir un algorithme permettant de

connecter, exploiter, donner un sens, anticiper ; à partir des masses d'informations stockées, commercialisées, échangées dans l'Internet. Avec toujours le même rêve : prédire l'agitation sociale... Les attaques terroristes...les événements stratégiquement significatifs. Or à en juger par les présents soubresauts affectant la politique étrangère américaine, de l'Afghanistan à l'Irak, la Darpa ne semble toujours pas avoir trouvé cet équivalent prédictif de la pierre philosophale...

*Rien de moins neutre  
qu'un algorithme...*

Les ordinateurs et l'informatique ne sont pas neutres. Et les outils de collecte et d'analyse des données ne le sont pas plus. Les algorithmes ne sont pas le mètre-étalon, mais renferment les biais de leurs créateurs, qui sont des humains faillibles et ont donc pu y instiller du *wishful thinking* en lieu et place de science...

Car ces algorithmes, outils de compilation du monde que les naïfs entourent d'une adoration quasi-théologique, peuvent avoir été truqués par leurs créateurs (en leur faveur à eux) ; ou par des pirates, facétieux ou stipendiés. Entrevoit-on alors ce qu'il advient du dispositif de "police prédictive" ainsi "arrangé" par des *hacktivists* embusqués dans le *dark web*? Les patrouilles de police envoyées là où rien n'arrive ? Et à l'autre bout du quartier, les cambrioleurs fort tranquilles pour agir ? Ici, insister serait cruel.



Xavier RAUFER

108

Plus largement, il est ardu de vérifier si des algorithmes remplissent vraiment leur tâche, du fait de leur capacité à influer sur la réalité, à la pré-formater ; de par leur masse, leur puissance même. Si leur usage est assez massif, ces algorithmes suscitent leur propre validité, exercent un effet “banc de poisson” sur les faits matériels. Tout cela, les médias devraient le savoir, car en matière de truandage d’algorithmes, les exemples récents ne manquent pas :

- Dans la décennie 1970 déjà, le “Black-Scholes Model” “prédit” la valeur future des actions. Mais en 1998, algorithmes géniaux ou pas, le *hedge-fund* Long Term Capital Management s’effondre, conduisant au bord du gouffre le marché mondial du crédit,
- En 2001, un modèle trafiqué – bien sûr fondé sur de fascinants algorithmes – permet à la société Enron d’attribuer une valeur astronomique à des actifs évanescents. Puis Enron s’effondre et ses dirigeants filent durablement en prison.
- Lors de la crise des subprimes, on découvre que des agences de notation “adaptent” leurs logiciels (reposant, on l’aura compris, sur d’ésotériques algorithmes) au résultat souhaité.
- Après ladite crise, le géant bancaire JP Morgan doit “s’excuser” de l’usage d’un logiciel “inadapté” – fondé sur des algorithmes sophistiqués – ayant

pourtant conduit la banque à perdre 6 milliards de dollars,

En 2008, trois importants *hedge-funds* subissent des pertes énormes, du fait de “mouvements imprédictibles du marchés”. Mouvements que les magiques algorithmes de ces *hedge-funds* étaient censés prévoir...

Au-delà, les algorithmes peuvent carrément permettre de juteuses escroqueries. Dès 2005 un businessman texan prétendument “ex-officier du renseignement militaire” et professeur d’université, se disait l’inventeur d’un algorithme permettant de faire fortune sur le marché des devises étrangères. Il escroque 33 millions de dollars à ses clients naïfs puis écope de 20 ans de prison. Mais venons-en au fond. La “police prédictive” est-elle sérieuse ?

Résolvons d’abord l’affaire de la “prédition des séismes”. Voici ce qu’en dit le géophysicien Bill Ellsworth, chercheur à l’*United States Geological Survey* : “Nul ne sait prédire les tremblements de terre... Si les séismes sont prédictibles, nous ne savons pas le faire. Et ils sont sans doute pour de bon imprédictibles... Nous ignorons même quelles équations régissent la mécanique des séismes...” Commentaire de l’interviewer “Un savant comme Bill Ellsworth, qui *sans limites financières*, (nous soulignons) dispose de toutes les données et de toutes les capacités informatiques possibles, admet qu’il ne voit pas vraiment comment prédire les tremblements de terre”.



## « Police prédictive » : les belles histoires de l'Oncle Predpol

Or de même, le milieu criminel s'inscrit clairement “dans le monde réel, là où les interactions humaines complexes ne peuvent pas toujours être saisies, même par les modèles les plus sophistiqués”, là où les outils d’analyse statistique tendent à produire des résultats dénués de sens. “Nous ne pouvons donc plus nous fier aux expériences en laboratoire pour une analyse de causalité”.

### *L'homme, le crime et la machine*

D'abord, une remarque, banale pour tout criminologue, mais qui échappe aux informaticiens et aux thuriféraires de *Big Data*. L'activité humaine n'est pas une ressource naturelle qu'il suffirait d'extraire du *cloud* pour le rentabiliser ; elle n'est pas une sorte de charbon, ou de pétrole, qu'on peut exploiter à son gré. Car – millénaire réalité ! – l'être humain, criminel ou non, *ne se laisse jamais observer passivement*. Dans son cerveau reptilien – dans ses gènes – l'imémoriale trace des millions d'années passées à éviter, pour survivre, les prédateurs équipés de griffes et de crocs mortels. Or l'être humain n'a rien de ces dangereux appendices. Ni de cornes, sabots ou carapace. Pour seule arme, l'homme a son gros cerveau ; il s'adapte, se cache, ruse ou triche : il *réagit*.

Constamment, l'homme joue contre l'observateur/ordinateur. Il est actif. Extraire le *Big Human Data* n'est donc pas une banale activité minière type extrac-

tion de charbon ou de pétrole – c'est une partie d'échec, voire un match de boxe.

Dans le domaine de l'illicite, un exemple sur ce point, si parlant. En France, les autorités multiplient les radars au long des routes et autoroutes ? Les conducteurs s'adaptent en trichant. Les usurpations de plaques d'immatriculation des véhicules (ce que “*flashent*” les radars) explosent littéralement : en 2010 : + 98% de ce type d'infractions constatées ; en 2011, + 73%. De 2010 à 2012 on passe de 5079 de ces “usurpations”, à 17 479...

### *L'utilité de Big Data et sa capacité à prévoir*

109

Si donc, la “police prédictive” est clairement illusoire dans sa conception actuelle ; ni plus ni moins efficace que les sites de rencontres en ligne (usant d'analogues algorithmes...). La voie du prédictif n'est pas pour autant bouchée :

- Les outils de *data mining* sont utiles dans le vaste domaine du connu connu : nul mieux que l'informatique ne sait trier, classer, ordonner – donc *optimiser* ; ce, à toute vitesse,
- Les logiciels spécialisés améliorent les diagnostics médicaux, ou l'efficacité thérapeutique ; *idem* pour le ciblage publicitaire ou l'estimation des primes d'assurances. Là dedans, un travail croisé entre informaticiens et criminologues susciterait à coup sûr



Xavier RAUFER

des outils policiers préventifs fort utiles,

- L'exploration du Big Data permet aussi de pré-voir les tendances nouvelles ; de révéler des émergences, d'entrevoir des dynamiques discrètes ;

ce qui, en matière de sécurité est d'évidence utile.

Dans l'attente de percées technologiques à ce jour inouïes, aller plus loin serait périlleux.

