

SECURITE INFORMATIQUE

Citation : Anne CANTERO, Les collectivités locales et la sécurité informatique, www.caprioli-avocats.com

Première publication : La Gazette des communes, 15 septembre 2003.

Date de la mise à jour : septembre 2003.

Les collectivités locales et la sécurité informatique

Anne Cantero, Docteur en Droit
contact@caprioli-avocats.com

Plan

I / LES MOYENS INTERNES DE LUTTE POUR LA SECURITE INFORMATIQUE

A) La charte d'utilisation des réseaux et des moyens informatiques : un instrument essentiel (commentaires juridiques et organisationnels)

B) La politique de sécurité

II / LES MOYENS EXOGENES POUR LA SECURITE INFORMATIQUE

A) La protection juridique des outils informatiques et des données électroniques par le droit pénal

B) La sécurisation juridique des échanges électroniques

Conclusion

Les outils informatiques sont désormais communément employés dans les administrations locales. Progressivement, l'information et les communications au sein des administrations ou vis à vis de l'extérieur se font de plus en plus fréquemment par voie électronique. Que les réseaux soient fermés ou ouverts, ils induisent progressivement une nouvelle forme d'organisation, de gestion et de relation. Les mises en ligne d'informations et de documents locaux pour plus de transparence, le développement des moyens de communication électronique avec les agents en intranet par exemple, avec les partenaires (comme les expérimentations du contrôle de légalité électronique) et les citoyens avec le développement de téléservices [1] et de téléprocédures [2] marquent la place de plus en plus grande qu'occupent les technologies de l'information dans l'évolution des administrations locales françaises. Si les avantages de ces nouveaux outils sont manifestes en termes de gain de temps, de bonne gestion et d'efficacité (et donc de coût à terme), les outils informatiques et les réseaux présentent des risques et des vulnérabilités inhérents à leur nature. Les atteintes au patrimoine informationnel de l'administration par des virus, des attaques informatiques, des erreurs ou des maladresses, ainsi que l'anonymat sur les réseaux et la volatilité des données sont des réalités dont on ne peut faire abstraction. La sécurité technique [3] et la sécurité juridique [4] relatives aux réseaux et systèmes informatiques ne sont donc pas absolues (mais le sont-elles dans l'univers papier ?). Pour pallier ces failles, des moyens techniques et juridiques de lutte doivent être adoptés de concert pour gagner en efficacité. D'un point de vue juridique, les collectivités locales disposent d'instruments préventifs dont le rôle est majeur pour une sécurité informatique de qualité. En effet, le droit offre les moyens d'une organisation interne à même de garantir une meilleure gestion des outils et des hommes pour une meilleure sécurité. Principalement, l'instauration d'une charte d'utilisation des réseaux et des moyens informatiques ainsi que l'adoption d'une politique de sécurité constituent les deux piliers internes de la sécurité informatique préventive (I). Par ailleurs, la lutte contre les atteintes aux outils informatiques et aux données électroniques s'articule sur la répression pénale des infractions constituées et sur les obligations légales de protection qui sont à la charge des responsables de traitement. De plus, le droit tend à reconnaître les écrits sous forme électronique sous réserve que certaines conditions soient remplies ; ce qui va dans le sens de rapports juridiques sécurisés. La sécurité passe ainsi par des moyens exogènes (II).

I / LES MOYENS INTERNES DE LUTTE POUR LA SECURITE INFORMATIQUE

La sécurité informatique ne relève pas du domaine réservé des informaticiens, loin s'en faut. Au sein des administrations locales, comme dans tout organisme où plusieurs personnes ont accès aux moyens

informatiques et aux réseaux, la sécurité ne s'impose pas, elle s'inculque. Il ne peut pas y avoir de sécurité si les hommes, qui restent présents dans l'électronique ne l'oublions pas, ne sont ni formés, ni sensibilisés aux risques et vulnérabilités de ces nouveaux moyens de communication, ni responsabilisés dans le cadre de leur utilisation. Pour répondre à ces préoccupations, les collectivités locales ont tout intérêt à établir une charte d'utilisation des réseaux et des moyens informatiques (A) et à mettre en place une politique de sécurité (B) à l'instar de ce qui existe dans le monde des entreprises.

A) La charte d'utilisation des réseaux et des moyens informatiques : un instrument essentiel (commentaires juridiques et organisationnels)

Afin d'éviter, ou plus exactement de tenter d'éviter, les intrusions externes et internes indésirables, l'adoption d'une charte d'utilisation des réseaux et des moyens informatiques constitue un instrument essentiel. Les collectivités ne s'y sont pas trompées et les demandes en la matière sont de plus en plus fortes. Touchant à l'organisation des services, la charte devra être adoptée après consultation du comité technique paritaire. Pour récolter une adhésion forte et donc une efficacité renforcée de la charte, la diffusion de ce document devrait être accompagnée si possible par une démarche pédagogique auprès des personnes concernées. Sur le fond, ce document devra contenir des dispositions qui fixeront les règles de bonne conduite que les utilisateurs (agents et élus) s'engagent à respecter au sein de la collectivité. Par exemple, il pourra y être rappelé qu'ils ont l'obligation de ne pas se connecter à des sites illicites (pédophile, raciste, etc.) ou dont les noms de domaine notamment laissent à penser que leur contenu est à caractère pornographique. La charte d'utilisation va également permettre d'établir une séparation entre la sphère personnelle et la sphère professionnelle. Ainsi, la charte pourra préciser que les utilisateurs disposent d'une adresse électronique professionnelle ayant une racine commune pour tout le personnel. Leur attention sera attirée sur le fait que leur messagerie professionnelle doit servir exclusivement pour leurs activités professionnelles. Bien entendu, il est difficile d'interdire au personnel de se servir de la connexion à l'internet pour consulter sa messagerie personnelle lorsqu'il en a une. Toutefois, certaines règles peuvent lui être très clairement posées. Qu'il s'agisse de sa messagerie professionnelle ou personnelle, il faut attirer l'attention de l'utilisateur sur le fait qu'il ne doit pas ouvrir un message qui paraît suspect et notamment ses pièces jointes. Il lui sera recommandé le cas échéant d'appliquer systématiquement l'anti-virus mis à jour régulièrement par le service informatique. En outre, la charte pourra prévoir qu'il est interdit de télécharger sur les postes de travail tous programmes, logiciels ou fichiers indifférents aux activités professionnelles de l'intéressé (tels par exemples les jeux, musiques, photos de sites, ...). Ceci est particulièrement important dans la mesure où ce sont ces types de produits qui en règle générale sont, outre leur possible origine contrefaisante, les lieux de prédilection des virus, vers et autres maladies électroniques aux effets souvent dévastateurs. La charte d'utilisation constitue un instrument de première importance dans une démarche de sécurité informatique. Son efficacité se trouve renforcée par la mise en place d'une véritable politique de sécurité dont elle constitue le prolongement.

B) La politique de sécurité

La politique de sécurité est un document qui doit être élaboré en étroite collaboration avec le service informatique dans la mesure où elle répond à des préoccupations également inhérentes à la sécurité informatique. Y seront donc déterminées les règles de gestion informatique devant être respectées afin de garantir un certain niveau de sécurité informatique ; étant entendu que ce terme est ici entendu de façon large, c'est à dire pour la sécurité des outils, des systèmes, des réseaux, des programmes, des applications, des données et des fichiers. Deux aspects doivent notamment retenir l'attention des responsables locaux.

D'une part, en matière informatique, la politique de sécurité déterminera précisément la gestion des mots de passe utilisés par les personnes concernées. Il pourra être exigé que ceux-ci soient conservés à l'abri des tiers ; ce qui se traduira par une disposition responsabilisant les utilisateurs en les engageant à ne pas coller sur leur écran ni même inscrire sur un papier laissé sur le bureau les mots de passe permettant l'accès à leur poste informatique. De même, il peut être demandé que les mots de passe choisis soient plus recherchés que le simple nom de l'agent et qu'ils contiennent obligatoirement des chiffres et des lettres, des minuscules et des majuscules. On peut également imposer à l'utilisateur de protéger son poste par une mise en veille qui ne peut être réactivée que par l'introduction d'un mot de passe et par l'obligation de fermer à clé son bureau dès qu'il quitte son poste (le mieux étant évidemment de l'éteindre en cas d'absence prolongée ; les longues veillées - soirées, week-ends, jours fériés -, étant les moments préférés des pirates qui peuvent repérer les postes ainsi allumés et connectés de façon continue). Il est enfin possible de réserver l'accès à l'internet ou à d'autres réseaux numériques à certaines catégories d'agents et d'élus au sein de la collectivité.

D'autre part, la politique de sécurité permettra de déterminer les règles en matière de sauvegarde informatique. Cette exigence n'est pas liée uniquement à la protection contre des virus ou autres atteintes frauduleuses. Elle concerne également les erreurs de manipulation, les vols, incendies, dégâts des eaux, ... Or, la volatilité des données et des informations caractérise les technologies de l'information. En conséquence, il est nécessaire de s'organiser pour que la mémoire " informatique " soit sauvegardée. D'abord, il est indispensable de prévoir la sauvegarde des disquettes ou des CD Rom des programmes et des applications. Cette opération suppose que la collectivité ait acquis les licences auprès des titulaires pour le nombre de postes concernés afin de pouvoir bénéficier de ces documents indispensables en cas de perte ou de destruction. Ensuite, la sauvegarde des fichiers peut se décliner en plusieurs temps. Une sauvegarde quotidienne et personnelle sera

réalisée par l'utilisateur pour le travail effectué dans la journée. Une sauvegarde hebdomadaire de toutes les données y succédera. Une sauvegarde mensuelle supplémentaire sera opérée. Pour plus de sécurité, la copie réalisée sera conservée dans un endroit physiquement protégé (contre le vol, les dégâts des eaux, incendie, ...). Enfin, il est préconisé une sauvegarde annuelle étant noté que les données peuvent être conservées sur CD Rom, ce qui présente l'avantage d'être sûr et peu encombrant. En outre, les services informatiques, lorsqu'ils existent dans les collectivités, pourront également conserver les journaux de connexion qu'ils gèrent. La politique de sécurité en déterminera les règles, conditions et modalités. Certains postes et certaines données peuvent enfin nécessiter des précautions renforcées. Le cas échéant, la politique de sécurité fixera notamment les dispositions particulières quant à l'accès physique à certains locaux.

Ces dispositifs préventifs qui reposent également sur des procédés techniques peuvent facilement être développés en interne. Ils sont relayés par des moyens de lutte exogènes.

II / LES MOYENS EXOGENES POUR LA SECURITE INFORMATIQUE

La protection des outils informatiques et des données électroniques repose d'abord sur un régime répressif (A). Les conditions et les modalités de reconnaissance juridique des échanges électroniques apportent ensuite une certaine sécurité en la matière (B).

A) La protection juridique des outils informatiques et des données électroniques par le droit pénal

La mise en réseaux des outils informatiques et plus particulièrement l'ouverture des postes sur l'internet présente par nature une entrée de l'extérieur vers les outils et les données contenues dans les machines ou circulant sur les réseaux. La technique apporte un certain nombre de réponses pour limiter les risques d'intrusion et d'attaques notamment [5]. Du point de vue juridique, deux axes sont principalement exploités.

1°) La protection des systèmes d'information [6]

Dès 1988, la loi dite " Godfrain " [7] a introduit dans le code pénal des dispositions réprimant les atteintes aux systèmes de traitement automatisés de données et constitutives d'infractions. Ainsi, l'article 323-1 du code pénal punit d'un an d'emprisonnement et de 15.000 euros d'amende, le fait d'accéder ou de se maintenir frauduleusement, dans tout ou partie d'un système de traitement automatisé de données et de deux ans d'emprisonnement et 30.000 euros d'amende s'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système. L'article 323 -2 du code pénal sanctionne quant à lui le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données. De la même façon est puni le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient, en application de l'article 323-3 du code pénal. Les tentatives de commission de ces infractions sont pénalement sanctionnées. La responsabilité pénale des personnes morales est légalement prévue. Avec ces dispositions, le régime répressif français en matière de sécurité informatique intègre les atteintes aux outils informatiques sans se limiter à un mode spécial d'attaques (virus, intrusions, cheval de Troie, ...) mais en visant plus concrètement les effets de telles atteintes sur les outils et les systèmes [8]. Ce dispositif répressif a précédé la convention du Conseil de l'Europe sur la cybercriminalité du 23 novembre 2001 [9] et la proposition de décision-cadre de la Commission européenne du 19 avril 2002 modifiée relative aux attaques visant les systèmes d'information [10]. Même si le droit français a le mérite de prévoir et de sanctionner un certain nombre d'infractions liées aux technologies de l'information, l'harmonisation aux niveaux international et communautaire apparaît indispensable pour lutter efficacement contre la cybercriminalité, qui fait fi des frontières géographiques et politiques. Il en va de même pour la protection des données.

2°) La sécurité des données personnelles: une obligation pénale à la charge du responsable du traitement

Avec l'utilisation des moyens informatiques, les collectivités locales ont de plus en plus recours à des traitements informatisés de données. Ces dernières peuvent concerner aussi bien les agents (liste du personnel, gestion des payes, ...) que les citoyens (liste électorale, liste des contribuables, ...). Dès lors qu'elles permettent d'identifier la personne physique concernée, elles deviennent des données nominatives ou à caractère personnel selon l'acception de la loi du 6 janvier 1978 ou de la directive du 24 octobre 1995 [11]. Le traitement de telles données doit se faire dans le respect des obligations légales posées par ces textes [12]. Plus particulièrement, en application de l'actuel article 29 de la loi du 6 janvier 1978, les personnes qui ordonnent ou effectuent un traitement de données nominatives doivent " prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés. ". Cette obligation qui est renforcée dans le cadre du projet de loi portant transposition de la directive européenne du 24 octobre 1995 [13] impose donc aux responsables de traitement de mettre en place toutes les mesures nécessaires afin de protéger les données nominatives traitées. Les collectivités locales et plus précisément les responsables locaux sont directement concernés par

cette disposition. Notons à cet égard que la C.N.I.L. recommande "la désignation d'un délégué à la protection des données" [14] et préconise le recours à des moyens de cryptologie à des fins de confidentialité [15]. On ne saurait que conseiller de suivre cette sage préconisation. Ce d'autant plus que les manquements à ces obligations ou les atteintes irrégulières aux données traitées peuvent donner lieu à des sanctions administratives prononcées par la C.N.I.L. qui voit d'ailleurs ses pouvoirs accrues dans le cadre du projet de loi. Les responsables des traitements encourent également des sanctions pénales en application des articles 226 -16 à 226-19 du code pénal. En conséquence, la sécurité des données traitées doit être considérée comme un tout qui repose à la fois sur des dispositifs spécifiques et des outils plus généraux. En outre, les articles 226 -13 et 226-15 du code pénal respectivement relatifs au secret professionnel et au secret des correspondances et des communications s'appliquent également. De la sorte, les collectivités locales doivent impérativement protéger leur patrimoine informationnel et ce, notamment lorsque des données sont couvertes par le sceau de la confidentialité.

La sécurité juridique consiste également à connaître la valeur juridique des échanges réalisés par voie électronique entre les personnes concernées.

B) LA SECURISATION JURIDIQUES DES ECHANGES ELECTRONIQUES

Cet aspect de la sécurité renvoie aux concepts d'écrit, de preuve et de date électroniques. D'abord, le certificat de serveur du site de la collectivité est un procédé utile pour rassurer les citoyens - internautes quant au fait qu'il sont sur le bon site. Ensuite, les besoins d'identification des interlocuteurs connectés dépendent de la procédure concernée. Les demandes d'informations relatives à la vie municipale ou aux démarches administratives ne nécessitent ainsi pas d'identification des citoyens. En revanche, l'échange réalisé par voie électronique, lorsqu'il est légalement possible, commande parfois une identification forte du demandeur ou du déclarant. La collectivité locale devra alors informer les personnes intéressées des modalités d'authentification exigées. Il s'agira par exemple d'un mot de passe personnel pour accéder au service ou de l'utilisation de certificats électroniques d'identité. Plus les procédés d'identification reposeront sur des modalités précises et des données vérifiées, plus le niveau de sécurité sera fort et donc fiable. Ceci étant, l'identification d'une personne n'est pas forcément suffisante. Plus précisément, il peut être nécessaire que la personne soit non seulement identifiée de façon certaine mais également que le lien entre l'acte adressé par voie électronique (son contenu) et sa non-dénégation par l'intéressé soient souhaités voire exigés. En d'autres termes, la signature électronique de l'acte échangé peut s'avérer indispensable. Notons qu'en droit administratif, aucun texte de portée générale ne traite de cette question à ce jour [16]. Néanmoins, à l'instar de ce qui a été établi et reconnu en droit privé avec la loi du 13 mars 2000 portant réforme du droit de la preuve et le décret n° 2001 -272 du 30 mars 2001 relatif aux signatures électroniques, les signatures électroniques basées sur la cryptologie à clé publique et reposant sur un dispositif de création de signature certifié et sur un certificat qualifié apparaissent à l'heure actuelle comme les procédés les plus fiables [17]. L'utilisation de tels procédés s'inscrit donc dans une démarche sécuritaire plus générale. La même logique se retrouve pour la datation électronique. Si les technologies de l'information abolissent les contraintes physiques liées aux horaires d'ouverture des services publics, il n'en demeure pas moins que la date continue à jouer un rôle très important au regard notamment des délais pour des demandes, des déclarations ou des recours. En conséquence, il est essentiel que la datation électronique repose sur un procédé fiable. Le législateur a pris conscience de cette évolution. L'article 16 de la loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations tout en disposant que c'est la date d'envoi de la demande ou de la déclaration qui doit être retenue lorsqu'une date limite ou un délai est imposé à l'administré, sauf exceptions, reconnaît le recours à " un procédé télématique ou informatique homologué permettant de certifier la date d'envoi ". Dès lors, les échanges et la date électroniques sont légalement admis. A l'heure actuelle, le décret prévu pour préciser les conditions d'application de cette disposition et les modalités d'homologation n'a pas encore été adopté. L'absence de ce texte n'empêche pas le développement de téléprocédures par les pouvoirs publics. En cas de litige, il appartiendra au juge d'apprécier la fiabilité du procédé utilisé. Enfin, signalons que le décret n° 2001 -492 du 6 juin 2001 pris en application de l'article 19 de la loi du 12 avril 2000 traite de l'accusé de réception des demandes présentées aux autorités administratives. Malheureusement, ce texte ne détermine pas quel procédé doit être retenu dans le contexte électronique entre un accusé de réception délivré de façon logique (automatique) ou délivré par l'intervention du destinataire (agent). Cette lacune laisse la porte ouverte à des applications divergentes qui pourraient être sources d'insécurité.

Conclusion

En définitive, la sécurité informatique n'est pas et ne doit pas être considérée comme l'apanage des seuls informaticiens. Parce que l'utilisation des technologies de l'information se développe au sein des administrations locales, les risques et les vulnérabilités qu'elles présentent méritent attention. Les moyens de lutte que les collectivités locales peuvent développer en interne ainsi que les moyens juridiques exogènes offrent des réponses à ces failles. Les pouvoirs locaux ont tout intérêt à prendre le train en marche !

Notes

[1] Les exemples sont de plus en plus nombreux et faute de pouvoir tous les citer nous renvoyons au dossier établi par La gazette des communes Sites Internet - Cap sur les services aux usagers, 26 août 2002, p. 44 et s.

[2] V. sur le sujet A. Cantéro, Les actes unilatéraux des communes dans le contexte électronique - Vers la dématérialisation des actes administratifs ?, PUAM, décembre 2002, cf. plus précisément p. 99 et s. ; T. Carcenac, Pour une administration électronique citoyenne, La documentation française, Paris, 2001 ; Forum des droits sur l'internet, Téléprocédures : le cadre juridique, décembre 2002, consultable à partir du site www.foruminternet.org (publications - décembre 2002).

[3] V. sur le sujet et pour des illustrations d'attaques informatiques, M. Desfontaines, Sécuriser son réseau informatique, La gazette des communes, 2 décembre 2002, p. 52 et s.

[4] V. sur cette notion, B. Pacteau, La sécurité juridique, un principe qui nous manque ?, A.J.D.A. 1995, n° spécial, p. 151 et s.

[5] La mise en place de fire-wall, un nombre limité de postes connectés à l'internet, l'utilisation de moyens de cryptologie à des fins de confidentialité... constituent autant de solutions pratiques qui, mises en œuvre cumulativement, peuvent constituer des parades contre les intrusions frauduleuses et leurs conséquences.

[6] Pour plus d'information en matière de répression pénale et de sécurité informatique, v. la rubrique " e-docs " dans " Publications " sur le site www.caprioli-avocats.com.

[7] Loi n° 98-19 du 5 janvier 1988 modifiée notamment par l'ordonnance n° 2000-916 du 19 septembre 2000, J.O. 22 septembre 2000. Eric Caprioli, Les moyens juridiques de lutte contre la cybercriminalité, Rev. Risques, Les cahiers de l'assurance, n°51/Septembre 2002, p. 50-55.

[8] Les peines énoncées devraient être alourdies avec l'adoption du projet de la loi pour la confiance dans l'économie numérique (article 33) adopté par l'Assemblée nationale le 26 février 2003. Ce projet succède à celui de la loi sur la société de l'information et à celui de la loi pour l'économie numérique. Le texte adopté à l'Assemblée nationale le 26 février 2003 est téléchargeable à l'adresse <http://www.assemblee-nationale.fr/12/ta/ta0089.asp>.

[9] Le texte est consultable sur le site <http://conventions.coe.int>.

[10] Pour la dernière version du texte, v. COM(2002)173, J.O.C.E., 27 août 2002, C203E/109.

[11] Directive 95/46 du 24 octobre 1995 sur la protection des données à caractère personnel, J.O.C.E., L. 281/31 du 23 novembre 1995.

[12] V. sur le sujet, A. Cantéro, Les actes unilatéraux des communes dans le contexte électronique - Vers la dématérialisation des actes administratifs ?, op. cit. supra, p. 115 et s.

[13] Pour le projet de loi adopté en première lecture au Sénat le 1er avril 2003, v. notamment http://ameli.senat.fr/publication_pl/2001-2002/203.html.

[14] V. C.N.I.L., 22ème rapport d'activité 2001, La documentation française, Paris, 2002 (consultable en ligne à l'adresse <http://www.ladocumentationfrancaise.fr/brp/notices/024000377.shtml>, v. p. 61).

[15] V. C.N.I.L., 22ème rapport d'activité 2001, op. cit. supra, version électronique, p. 112-113, note 2. La même préconisation est faite par P. Truche et alii, in Administration électronique et protection des données personnelles, rapport consultable et téléchargeable en ligne à l'adresse <http://www.ladocumentationfrancaise.fr/brp/notices/024000100.shtml>, v. notamment p. 42.

[16] En revanche des textes ponctuels dans des domaines précis ont été adoptés. Tel est le cas par exemple en matière de marchés publics. V. sur cette question, Anne Cantéro, Marchés publics et signature électronique, Lettre informatique et collectivités locales, 2003, n° 400, p. 4 s.

[17] Eric Caprioli, La loi française sur la preuve et la signature électronique dans la perspective européenne, J.C.P., 2000, éd. G, I, 224 et Ecrit et preuve dans la loi n°2000-230 du 13 mars 2000, J.C.P. 2000, éd E, cah. Dr. Entr. n°2, p. 1 s.