BADREDDINE HAMZA,
avocat, Cabinet Seban & Associés

Infractions nombreuses
Nombre d'infractions existent dans le code pénal pour réprimer les atteintes à un système informatique. Sont punies : l'entrave à son fonctionnement, l'introduction de données, l'intrusion…

Systèmes informatiques
Les collectivités territoriales y ont de plus en plus recours dans la gestion de certains services comme les listes électorales, l'état civil, les fichiers sociaux ou encore le cadastre.

Atteintes variées
Les atteintes peuvent viser le système de traitement automatisé de données en lui-même (piratage) ou relever d'infractions, telles des escroqueries ou vols, ayant comme support le système.

Gestion locale et risque pénal (3)

Les nouvelles technologies de l'information et de la communication (NTIC)

L'essor des nouvelles technologies de l'information et de la communication (NTIC) constitue un défi d'actualité que les collectivités, dépositaires d'informations personnelles et de deniers publics, doivent réussir à relever : faire face au risque informatique. Tant en leur qualité d'organisations collectrices de données personnelles qu'émanations de l'Etat, les collectivités territoriales s'avèrent être, et deviennent de plus en plus des cibles privilégiées aux yeux des cyberdélinquants. Elles ne sont pas seulement victimes de piratages informatiques, elles le sont aussi d'infractions de droit commun commises par des moyens électroniques.

En 2015, une enquête de la Gazette des communes (1) avait permis de dresser une carte du niveau de sécurité de plus de 14000 sites web de communes françaises. Elle mettait en lumière un bilan inquiétant : près de 6500 d'entre eux présentaient une vulnérabilité importante à cause de l'absence d'une sécurisation suffisante.

CADRE JURIDIQUE

DÉFINITION DES INFRACTIONS INFORMATIQUES ET SANCTIONS PRÉVUES

Plusieurs infractions existent dans le code pénal afin de réprimer les atteintes à un système informatique, qu'il s'agisse de l'intrusion ou du maintien dans un système informatique, de l'entrave à son fonctionnement ou de l'introduction frauduleuse de données.

Tout d'abord, l'article 323-1 du code pénal punit « le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données » par une peine de deux ans d'emprisonnement et 60000 € d'amende. La répression est même aggravée en cas de suppression ou de modification des données contenues, et également en cas d'altération du fonctionnement du système. Dans ces cas de figure, la peine est alors élevée à trois ans d'emprisonnement et à 100000 € d'amende.

Ensuite, l'article 323-2 du code pénal réprime le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données, l'assortissant d'une sanction de cinq ans d'emprisonnement et de 75000 euros d'amende.

De plus, l'article 323-3 du code pénal stipule que 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 est passible d'une sanction de cinq ans d'emprisonnement et de 150000 euros d'amende.

Enfin, l'article 323-4-1 du code pénal prévoit une peine portée à dix ans d'emprisonnement et 300000 euros d'amende quand les infractions prévues aux articles 323-1 à 323-3-1 ont été commises en bande organisée et à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat.

RESPONSABILITÉ DANS LE CAS DES DONNÉES PERSONNELLES

Les collectivités ont de plus en plus souvent recours aux systèmes informatiques. Les applications qu'ils offrent sont nombreuses dans la gestion de certains services parmi lesquels les listes électorales, l'état civil, les fichiers sociaux, le cadastre, la gestion du parc immobilier et la vidéoprotection figurent en bonne position.

L'ensemble de ces applications collecte un volume important de données à caractère personnel concernant les usagers, qu'ils soient administrés ou non. Elles ont trait à la vie privée des personnes qui les fournissent et peuvent, si elles sont divulguées, entraîner une atteinte à leurs droits et libertés.

La loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée en 2004, pose le cadre législatif à respecter par les acteurs, aussi bien privés que publics, lors de la collecte, du traitement et de la conservation de ces données. Elle fait peser sur eux un

À NOTER

L'élu est garant des fichiers mis en ligne et de leur sécurisation, engageant ainsi sa responsabilité en cas de non-respect des obligations fixées par la loi, notamment au titre de l'article 226-17 du code pénal.

devoir de sécurisation de ces éléments. Ainsi, l'élu est garant des fichiers mis en ligne et de leur sécurisation, engageant ainsi sa responsabilité en cas de non-respect des obligations fixées par la loi, notamment au titre de l'article 226-17 du code pénal. Cet article sanctionne l'absence de sécurisation des données collectées telle qu'imposée par l'article 34 de la loi «Informatique et Libertés» (2).

LA RÉPRESSION PÉNALE

INFRACTIONS VISANT LES COMMUNES

Incrimination centrale du droit pénal de l'informatique, le délit de l'article 323-1 du code pénal trouvera bien sûr à s'appliquer au piratage d'un site internet. La jurisprudence appréciant largement la notion de «site internet» en l'absence d'une définition légale, elle considère qu'il s'agit bien d'un système de traitement automatisé de données (3).

Depuis les attentats de janvier 2015, plusieurs communes ont vu leur site internet piraté au moyen d'une «défiguration» de leur page d'accueil qui consiste en l'affichage de messages faisant l'apologie du terrorisme.

Par ailleurs, l'introduction dans le logiciel de messagerie d'un agent par l'utilisation frauduleuse et non autorisée de codes d'accès afin d'y consulter les messages électroniques constituera un accès pénalement sanctionné dans un système automatisé de données, ainsi qu'une atteinte au secret des correspondances (4).

Une autre forme d'atteinte aux systèmes informatiques des communes a enfin connu une explosion au début de l'année 2016: le «rançongiciel». Cette attaque malveillante se déroule en plusieurs étapes: d'abord les cyberdélinquants s'introduisent dans le réseau informatique de la victime, ils y installent un logiciel bloquant toute utilisation du système et exigent ensuite le paiement d'une «rançon», condition sine qua non pour redonner le contrôle du système et ne pas divulguer des données sensibles.

À NOTER

Visée par des propos injurieux, diffamatoires ou menaçants, la collectivité est en droit d'agir pénalement en qualité de victime. Si ces propos sont dirigés envers autrui, ils peuvent être source de responsabilité pénale pour l'agent directeur de la publication, l'élu ou l'administrateur du site sur lequel ils ont été postés.

RÉFÉRENCES

Code pénal, articles 323-1 et suivants.

Ces actes pourront relever de la qualification d'entrave au fonctionnement d'un système de traitement automatisé de données selon l'article 323-2 du code pénal.

Les enjeux de sécurisation des données sont donc primordiaux, même si ces agissements demeurent souvent impunis, en raison de la technicité des investigations requises, de l'internationalisation de ces attaques et de moyens d'enquête nécessairement limités.

INFRACTIONS COMMISES CONTRE LES COMMUNES PAR LE BIAIS D'UN SUPPORT INFORMATIQUE

Outre les infractions dites «informatiques» du code pénal, d'autres infractions classiques peuvent être commises à l'encontre des communes par des moyens numériques. Par exemple, il peut s'agir d'un vol de documents ayant lieu dans une mairie par un agent qui accède au système informatique de la collectivité, sous l'identité d'un autre agent, afin d'avoir accès à des dossiers confidentiels.

De la même manière, des escroqueries sont possibles en abusant des systèmes informatiques communaux: l'auteur usurpe ses prérogatives d'utilisateur pour commander des produits à son profit ou pour s'attribuer des aides ou contributions financières indues.

L'avènement des réseaux sociaux a conduit les collectivités à y être de plus en plus présentes, en particulier sur les plateformes Facebook, Twitter ou YouTube. Elles ont également souvent développé leurs propres espaces de discussion tels que des forums, blogs et «chats» en direct. Ces nouveaux lieux de communication ne sont pas sans risques car certains utilisateurs profitent de l'anonymat et de la distance qu'offre internet pour y poster des propos injurieux, diffamatoires ou menaçants. Visée par de tels propos, la collectivité est en droit d'agir pénalement en qualité de victime (lire «la Gazette» du 7 novembre, «Les collectivités territoriales et les infractions de presse») . Si de tels propos sont dirigés envers autrui, ils peuvent également être source de responsabilité pénale pour l'élu ou l'agent directeur de la publication, ou encore l'administrateur du site sur lequel ils ont été postés. Il importe donc que ces élus et agents se montrent particulièrement vigilants quant au contenu des publications déposées sur les blogs, forums et espaces de discussion mis en œuvre par la collectivité et qu'ils sont chargés d'administrer ou de modérer.

VERS UNE CULTURE DU RISQUE INFORMATIQUE

Si le nombre de piratages de sites internet augmente, le risque informatique n'est pas seulement externe: il peut aussi provenir du personnel, qu'il soit permanent ou temporaire, de la collectivité.

Le renforcement de la sécurité informatique s'appuie à cet égard sur l'application de premières mesures simples: identification par login de chaque utilisateur du système, mise en place, modification régulière et confidentialité des mots de passe personnels, y compris pour les agents employés temporairement et dont les identifiants seront désactivés après leur départ.

De manière générale, cette sécurisation informatique nécessite d'abord une sensibilisation et une acculturation des personnels aux risques encourus.

(1) http://www.lagazettedescommunes.com/337105.

(2) Lire Romain Perray & Pierrick Salen, «Données personnelles : La responsabilité de l'administration en cas de divulgation «La Gazette 29 août 2016, p. 62.

(3) TGI Lyon, ch. corr., 27 mai 2008.

(4) TGI Paris, 12e ch., 1er juin 2007, Sté O. et a. c/ T. N. et M. T.

DÉJÀ PARUS

«Le fonctionnaire territorial, un citoyen soumis à un régime spécifique», «la Gazette» du 24 octobre, p. 60-61.
«Les collectivités territoriales et les infractions de presse», «la Gazette» du 7 novembre, p. 54-56.

À PARAÎTRE

«Les marchés publics»
«L'urbanisme et l'insalubrité»
«Les collectivités territoriales et leurs satellites»