DOSSIER : La cybersécurité, l'affaire de tous
Dossier publié à l'adresse https://www.lagazettedescommunes.com/1030221/assurer-la-securite-des-donnees-au-niveau-local-en-5-points-cles/

CYBERSÉCURITÉ

Assurer la sécurité des données au niveau local en 5 points-clés

Auteur associé | Actu juridique | Fiches de droit pratique | France | Publié le 25/03/2026 | Mis à jour le 26/03/2026

Le cadre juridique des données est dense et porteur d'une obligation générale de sécurité. L'ignorer n'est pas seulement un risque : c'est une faute. La question n'est pas de savoir si un incident surviendra, mais quand.

[1]

Avouer ses péchés

Les collectivités sont devenues les cibles privilégiées des cybercriminels. Piratage, rançongiciel et hameçonnage sont désormais monnaie courante et si certaines collectivités territoriales ont pris les devants pour y remédier, force est de constater que de nombreuses communes manquent à l'appel.

Le risque « cyber » s'est banalisé et sa gravité est, aujourd'hui encore, largement sous-estimée. Si beaucoup parient sur la chance en estimant – à tort – qu'ils ne sont pas exposés, les conséquences sont pourtant trop importantes pour être ignorées : fuite des données, désorganisation, voire paralysie des services, préjudices financiers, dommages aux biens et aux personnes… sans parler de la détérioration du lien de confiance entre administration et administrés.

Le constat est malheureusement sans appel, le niveau d'exigence appliqué aux achats informatiques reste bien inférieur à celui d'un marché classique. On ne signerait jamais un marché de travaux sans connaître le contenu du contrat ; c'est pourtant ce que l'on fait encore, trop souvent, avec les contrats informatiques.

Face à la promesse commerciale des éditeurs, les collectivités signent des contrats déséquilibrés, rédigés unilatéralement, sans que les services juridiques et les directions des systèmes d'information (DSI) ne dialoguent vraiment.

Évidemment, face au jargon technique, l'épreuve semble parfois insurmontable. L'enjeu n'est pourtant pas de maîtriser tous les détails techniques : il est de piloter une démarche structurée, proportionnée à la taille de la collectivité et à son niveau de maturité technologique.

Admettre que la cybersécurité n'est pas une option

En pratique, le cadre juridique applicable à la sécurisation des systèmes d'information (SI) publics est assez largement méconnu. Souvent jugé complexe, il repose sur un corpus réglementaire dense, dont les obligations s'imbriquent et se superposent.

Pour ne citer que les principaux textes applicables : le référentiel général de sécurité (1) [2] et le règlement eIDAS (2) [3] pour la mise en œuvre des téléservices locaux (demande de permis de construire, demande de logement social…), le RGPD (3) [4] et la loi « informatique et libertés» [5] (4) [6] concernant la protection des données personnelles et, plus récemment, la directive NIS2 [7] (5) [8].

Même si l'adoption du texte officiel se fait attendre, le sort des collectivités locales ne va pas s'arranger puisque le projet de loi « résilience » [9] (6) [10] – qui vise notamment à transposer NIS2 en droit interne – prévoit d'inclure près de 1 500 collectivités dans son périmètre. Les collectivités concernées seront soumises à des obligations variables, selon qu'elles sont considérées comme des entités « essentielles » (régions, départements, centres de gestion, services départementaux d'incendie et de secours, communes de plus de 30 000 habitants…) ou « importantes » (communautés d'agglomération ne comprenant pas de commune de 30 000 habitants…).

Quoi qu'il en soit, le cadre juridique actuellement en vigueur est déjà porteur d'une obligation générale de sécurité. L'article 32 du RGPD [11] impose la mise en œuvre de « mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque ». Il faut être clair : protéger les données personnelles est indissociable d'une politique de cybersécurité robuste.

La tenue d'un registre des traitements, la désignation d'un délégué à la protection des données, la conduite d'analyses d'impact et la notification des violations de données sont autant d'instruments qui, correctement déployés, structurent le premier volet de cette gouvernance.

Mettre en œuvre des bonnes pratiques « d'hygiène numérique »

Au nombre des nouvelles obligations imposées par la directive NIS2 figure la mise en place de mesures de « cyberhygiène ». Si la formule peut prêter à sourire, son contenu est pourtant très concret. La sécurisation des SI repose, avant tout, sur des mesures techniques et organisationnelles d'apparence simple – mais dont le respect est, en pratique, encore trop souvent un vœu pieux…

Schématiquement, il s'agit avant tout :

- de mettre à jour les mots de passe régulièrement ;
- de déployer des solutions d'authentification multifacteurs (MFA) lorsque nécessaire ;
- de limiter les droits d'accès au strict « besoin d'en connaître » ;
- de revoir régulièrement les habilitations ;
- de mettre à jour systématiquement les logiciels et les systèmes d'exploitation ;
- de mettre en place des sauvegardes régulières déconnectées du réseau principal ;
- de cloisonner les usages professionnels et personnels ;
- de chiffrer les actifs sensibles.

Pour être appliquées, ces mesures doivent se décliner en politiques internes : charte informatique, politique de sécurité, procédures de gestion des incidents, – véritable – politique d'archivage et de destruction des données… Sans celles-ci, la sécurité restera un catalogue de bonnes intentions.

Précisons néanmoins que dans ce domaine, comme dans de nombreux autres, la faille la plus courante est humaine. Autrement dit, ces mesures techniques resteront lettre morte sans une véritable politique de formation et de sensibilisation des agents aux risques et bonnes pratiques en matière de cybersécurité. Il faut insister : ce n'est pas d'expertise que l'on parle, mais d'hygiène élémentaire, appliquée à la sécurité des données.

Penser au contenu de ses contrats

Le contrat, encore le contrat, toujours le contrat. Chaque externalisation crée une nouvelle dépendance technique, et donc un nouveau risque. La cybersécurité doit se déployer tout au long de la « chaîne

d'approvisionnement », ce qui inclut nécessairement les relations contractuelles avec les fournisseurs. La première exigence est celle du choix du prestataire. Les acheteurs publics doivent veiller à ce que les critères de sélection et les clauses des marchés reflètent le sérieux du monde local. Des référentiels et certifications reconnus (HDS, SecNumCloud, ISO 27001, SOC2 Type II…) peuvent être utilisés comme indicateurs du niveau de maturité du fournisseur et intégrés dans les critères de sélection des candidatures et des offres.

Surtout, il faut en finir avec les clauses génériques du type « le prestataire s'engage à assurer la cybersécurité du système », bien trop souvent constatées. Outre le fait que ces clauses sont juridiquement insuffisantes, elles entretiennent le risque en donnant l'illusion d'une protection qui n'existe pas.

Les contrats doivent comporter des engagements précis et vérifiables : référentiels de sécurité applicables, objectifs de certification (éventuellement assortis de délais), exigences techniques précises portant sur le chiffrement des données, la gestion des accès et les habilitations. Le contrat doit également prévoir des mécanismes de contrôle (éventuels audits et tests d'intrusion), des procédures de notification des incidents de sécurité et, bien entendu, des conséquences contractuelles en cas de manquement (par exemple, des pénalités croissantes allant jusqu'à une résiliation pour faute).

Sur le terrain de la protection des données personnelles, les contrats doivent intégrer les clauses imposées par l'article 28 du RGPD [12]. Il ne s'agit pas seulement d'en faire une annexe qui ne sera ni lue ni appliquée, mais d'encadrer strictement les traitements par des instructions documentées, d'imposer des obligations de confidentialité, de prévoir des mesures de sécurité appropriées, d'encadrer la sous-traitance « ultérieure » (« en cascade ») et, enfin, de régler ce qui est bien trop souvent oublié : le sort des données au terme du contrat.

Se préparer au pire

Aucune mesure de prévention n'élimine totalement le risque. L'expérience des dernières années le démontre, et même des collectivités (très) bien équipées ont été touchées par des attaques d'ampleur. La question n'est plus de savoir si un incident surviendra, mais quand. La réponse appropriée consiste en la mise en place d'un plan de continuité d'activité (PCA) ; un outil trop peu connu des acteurs locaux – même si certains ne cessent de rappeler son importance (7) [13].

De quoi s'agit-il ? En substance, le « PCA-cyber » est le document qui répond, à l'avance, aux questions que les collectivités n'ont plus le temps de se poser le jour d'un cyberincident : quels sont les services prioritaires à rétablir ? Quelles sont les procédures de fonctionnement en mode dégradé (y compris le retour au papier) ? Qui a la charge de quoi au sein de la cellule de crise ? C'est aussi dans ce plan que doivent être intégrées les procédures de notification, dont les délais impératifs (et courts) résultent des textes précités.

Le PCA est un document vivant : après chaque incident, un retour d'expérience doit permettre d'identifier les vulnérabilités exploitées, d'évaluer l'efficacité de la réponse et de mettre à jour le plan en conséquence. C'est aussi l'occasion de vérifier la conformité des prestataires à leurs engagements contractuels et, le cas échéant, d'en tirer les conséquences.

POUR ALLER PLUS LOIN

- Les collectivités territoriales dans l'expectative après le dévoilement de la nouvelle stratégie nationale de cybersécurité
- Cybersécurité : l'isolement, le premier risque dans les petites communes