CYBERACTU'

LE MAGAZINE DU SERVICE PROTECTION DES DONNÉES DU CENTRE DE GESTION DU GARD

Juin 2026

IA et Collectivités

Un nouvel environnement numérique : vigilance et opportunités

Dossier page 14

L'actualité :
Les traceurs : pixels et cookies

Fiche pratique :
L'Installation des nouveaux élus

Archives :
Obligations et responsabilités des collectivités

CENTRE DE GESTION
DU GARD

Retrouvez toute notre actualité sur notre **site internet** et nos **réseaux sociaux** !

Nouveau site internet !

LinkedIn

Facebook

Instagram

SOMMAIRE

ÉDITO

Le pavillon change de main sur les flots de la protection des données

Né en 2018, dans le sillage de la grande marée du RGPD, le service de « Protection des données » a pris le large sous la garde vigilante de Pierre Bonanni. Capitaine droit et infatigable, il tint le cap durant de longues traversées, guidant collectivités territoriales et établissements publics gardois à travers récifs et brumes réglementaires, jusqu'à les mener vers des rivages plus sûrs.

Mais nul navire ne vogue éternellement sous le même gouvernail.

Après des années d'apprentissage et d'épreuves, Ana Vega se voit désormais confier le flambeau et s'apprête à tracer de nouvelles routes.

Elle sera votre Déléguée à la protection des données, poursuivant la quête de conformité, éveillant les consciences, et accompagnant chaque équipage face aux mystères et aux tempêtes juridiques.

Pierre BONANNI – Ana VEGA

Sarah ROMAN

Contact

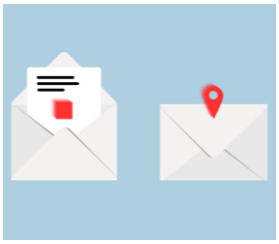
Service Protection des données

☎ : *04 66 38 86 86*

@ : *dpd@cdg30.fr*

Centre de gestion de la fonction publique territoriale du Gard

PIXELS DE SUIVI DANS LES COURRIELS : LA CNIL PRÉCISE LE CADRE D'UTILISATION



Face au développement croissant des pixels de suivi dans les courriels, la CNIL a récemment publié des recommandations visant à clarifier leur utilisation.

Une alternative aux cookies

Ces dispositifs, aussi appelés «pixels espions», consistent en de minuscules images intégrées dans un courriel, dont le chargement permet de savoir si un message a été ouvert. Ils constituent une alternative aux cookies et participent à des finalités variées telles que la mesure d'audience, l'amélioration de la délivrabilité ou encore la personnalisation des contenus.

Le courriel ne serait plus un espace personnel

Dans le contexte spécifique de la messagerie électronique, la CNIL souligne un enjeu majeur: le courriel est un espace personnel, associé à la consultation de contenus privés.

La multiplication des plaintes a ainsi conduit l'autorité à préciser le cadre juridique applicable, tant pour les organismes publics et privés que pour leurs prestataires, en complément des règles existantes sur les traceurs (article 82 de la loi Informatique et Libertés et recommandations «cookies et autres traceurs»).

Un accompagnement important

Ces nouvelles orientations visent à accompagner les acteurs dans l'identification de leurs obligations, notamment en distinguant les cas nécessitant le recueil du consentement de ceux pouvant bénéficier d'une exemption.

À ce titre, la CNIL admet une exemption pour certains usages strictement nécessaires, comme la mesure de la délivrabilité des courriels liés à un service expressément demandé par l'usager. Cette exception permet, d'identifier les destinataires inactifs afin de limiter les sollicitations inutiles.

Sont également concernés par ce cadre les «courriels transactionnels» tels que les confirmations de commande, notifications d'événements, alertes de sécurité ou l'obligation de Réinitialiser le mot de passe, dès lors qu'ils s'inscrivent dans un service attendu par l'utilisateur.

En revanche, pour les autres usages, notamment à des fins de suivi ou de communication, un consentement libre, éclairé et facilement révocable demeure requis.

Importance accrue

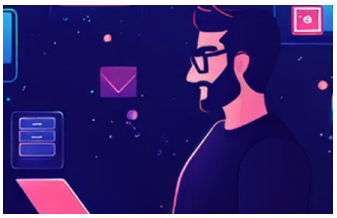
Pour les collectivités territoriales et établissements publics, ces recommandations invitent à renforcer les pratiques de transparence et d'information, tout en conciliant efficacité opérationnelle et respect des droits des usagers.

COOKIES ET TRACEURS : LA CNIL PUBLIE UNE FAQ POUR ACCOMPAGNER LA MISE EN CONFORMITÉ AU RGPD

La CNIL a mis en ligne une FAQ détaillée relative à ses lignes directrices modificatives et à sa recommandation « cookies et autres traceurs »

Un cadre juridique clarifié pour les traceurs

La FAQ apporte des précisions concrètes sur plusieurs thématiques clés : le champ d'application des règles, les différents types de traceurs, et les cas d'exemption. Elle détaille aussi les modalités de recueil du consentement et les conditions permettant aux usagers de refuser facilement ces dispositifs.



Les lignes directrices ont pour objectif de rappeler les obligations issues de l'article 82 de la loi Informatique et Libertés et d'en expliciter l'application. Elles sont complétées par la recommandation de la CNIL, qui propose des bonnes pratiques opérationnelles pour les acteurs publics et privés.

Un enjeu majeur pour les collectivités et établissements publics

Les sites internet constituant aujourd'hui un canal essentiel de communication avec les administrés, la conformité aux règles relatives aux cookies et traceurs est devenue incontournable. Cette responsabilité incombe non seulement aux responsables d'édition des sites, mais également à l'ensemble des partenaires impliqués, notamment les prestataires techniques en charge de leur gestion.

L'ACTUALITÉ DE LA PROTECTION DES DONNÉES

DURÉES DE CONSERVATION DES DONNÉES RH : UN NOUVEAU RÉFÉRENTIEL POUR ACCOMPAGNER LES COLLECTIVITÉS

Afin d'accompagner les organismes dans la définition de durées de conservation adaptées pour les traitements de gestion des ressources humaines, la CNIL a publié un référentiel dédié. Cet outil est applicable à la fonction publique territoriale sur la majorité des thématiques proposées, à l'exception de la gestion administrative du personnel.

En effet, les durées de conservation des documents constituant le dossier individuel des agents publics relèvent d'un cadre spécifique fixé par l'arrêté du 21 décembre 2012 relatif à leur gestion sur support électronique.

Le référentiel couvre les traitements les plus fréquents dans le cadre de la gestion des ressources humaines :

•le recrutement ;
•la gestion des rémunérations ;
•la sécurisation des biens et des personnes ;
•la gestion des véhicules pro ;
•l'écoute des conversations téléphoniques sur le lieu de travail ;
•la gestion des relations collectives de travail ;
•la gestion des accidents du travail;
•la gestion du contentieux et du précontentieux ;
•la gestion des alertes professionnelles

Ce référentiel constitue un cadre de référence, mais ne couvre pas l'ensemble des situations.

Des obligations spécifiques peuvent s'appliquer selon les cas. Il est donc recommandé aux organismes de vérifier systématiquement les bases juridiques mentionnées afin de s'assurer de leur adéquation avec leurs propres traitements.

Enfin, les durées de conservation, exprimées en mois, peuvent être ajustées techniquement dans les outils numériques, notamment en les traduisant en jours.

CONFORMITÉ DES SITES WEB : TRACEURS ET COOKIES - LE GROUPE DE TRAVAIL AFCDP GARD/HÉRAULT FAIT LE POINT

Dans le cadre de son adhésion à l'Association française des correspondants à la protection des données (AFCDP), le service protection des données du CDG30 a récemment participé à une réunion du groupe Gard/Hérault

Cette réunion a été consacrée à la conformité des sites web, avec un focus sur les cookies et traceurs. Animée par une experte du sujet, cette session a permis de rappeler les fondamentaux réglementaires et d'en tirer des enseignements concrets pour les collectivités territoriales.

La réglementation applicable repose sur plusieurs textes structurants :

- la directive e-Privacy (2009/136/CE),
- l'article 82 de la loi Informatique et Libertés, ainsi que
- les lignes directrices et recommandations de la CNIL entrées en application en avril 2021.

Dans un contexte de contrôles renforcés, la bonne compréhension de ces règles est essentielle pour sécuriser les pratiques.

3 enjeux à retenir pour les collectivités

1. Nécessité de comprendre les cookies pour mieux les encadrer : Un cookie est un fichier déposé sur le terminal d'un utilisateur lors de sa navigation, permettant notamment de le reconnaître et d'analyser son comportement.

On distingue les cookies « first party », déposés par l'éditeur du site, et les cookies « third party », installés par des partenaires, sous la responsabilité de l'éditeur.

Par ailleurs, il est essentiel de différencier les cookies techniques, parfois exemptés de consentement sous conditions, et les cookies d'audience ou autres traceurs nécessitant une gestion conforme du consentement.

2. Responsabilités et vigilance des collectivités : Les collectivités, en tant qu'éditeurs de sites, doivent s'assurer que les traceurs soumis à consentement cessent effectivement de fonctionner en cas de refus de l'utilisateur. Cette exigence est centrale pour limiter les risques de non-conformité et de sanctions.

3. Contrôles et bonnes pratiques : La CNIL porte une attention particulière aux bandeaux cookies, à l'information délivrée aux usagers et à la documentation interne. Pour faciliter l'analyse des traceurs, le recours à l'intelligence artificielle est recommandé.

Ce retour d'expérience souligne l'importance, pour les collectivités territoriales, d'adopter une démarche proactive en matière de conformité numérique.

CYBERATTAQUE DE L'AGENCE NATIONALE DES TITRES SÉCURISÉS (ANTS)

L'Agence nationale des titres sécurisés (ANTS), interface majeure des démarches liées à l'obtention des titres d'identité, a annoncé via un communiqué sur son site officiel avoir été la cible d'une cyberattaque massive le mercredi 15 avril.

L'incident concerne environ 10 millions de comptes sur le portail ants.gouv.fr, ce qui en fait une atteinte particulièrement sensible au regard de la nature des informations détenues.

En effet, les données collectées par l'ANTS sont parmi les plus complètes et les plus fiables en matière d'identification. Elles constituent un profil civil presque exhaustif, pouvant être exploité à des fins malveillantes telles que l'usurpation d'identité ou les arnaques ciblées. L'incident touche à la fois des comptes professionnels et des comptes particuliers.

Pour les particuliers, les données personnelles potentiellement compromises incluent l'identifiant de connexion, la civilité, le nom, les prénoms, l'adresse électronique, la date de naissance ainsi qu'un identifiant unique du compte. Dans certains cas, d'autres informations peuvent également être concernées, telles que l'adresse postale, le lieu de naissance ou encore le numéro de téléphone.

Le ministère évoque un « accès non autorisé » à ces données, ce qui signifie qu'un individu a pu accéder de manière frauduleuse à un volume important d'informations. Le pirate à l'origine de l'attaque affirme avoir obtenu les données d'environ 18 millions de personnes et avoir identifié des failles de sécurité au sein du système. Il a publié un message provocateur sur le dark web, accompagné d'une partie des données volées. Les informations diffusées comprendraient notamment les noms, prénoms, identifiants, adresses, dates de naissance et numéros de téléphone. En revanche, aucune photo d'identité ni information relative aux liens de parenté ne serait concernée.

Cette situation expose les usagers à des risques accrus de tentatives d'hameçonnage. Ces attaques peuvent se présenter sous diverses formes, notamment par SMS, appels téléphoniques, courriels ou même courrier postal. Les victimes potentielles peuvent être incitées à communiquer des informations sensibles ou à cliquer sur des liens frauduleux. Dans ce contexte, il est vivement recommandé de modifier immédiatement les mots de passe des comptes liés.

La faille exploitée serait de type IDOR (Insecure Direct Object Reference). Ce type de vulnérabilité permet d'accéder aux données d'autres utilisateurs en modifiant simplement un identifiant dans les requêtes adressées à l'API, sans qu'un contrôle d'autorisation ne soit effectué côté serveur. Une telle faille est particulièrement préoccupante pour un site de la nature de l'ANTS, où les exigences en matière de sécurité devraient être extrêmement élevées.

Face à cet incident, l'ANTS a indiqué avoir informé les personnes concernées. Une déclaration a également été effectuée auprès de la Commission nationale de l'informatique et des libertés (CNIL). L'agence se veut rassurante en précisant que les informations permettant d'accéder aux comptes n'ont pas été compromises. Parallèlement, une enquête est en cours afin de déterminer l'origine exacte de l'attaque.

Les obligations légales ont été respectées, avec notamment une alerte transmise à l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et un signalement effectué auprès de la procureure de la République de Paris. Ces démarches visent à encadrer la gestion de la crise et à permettre l'identification des responsables.

En attendant les conclusions de l'enquête, les utilisateurs disposant d'un compte sur ants.gouv.fr doivent faire preuve d'une vigilance accrue. Il est essentiel de rester prudent face à toute communication prétendant provenir de l'ANTS et de ne jamais transmettre ses identifiants ou données personnelles en réponse à ce type de sollicitation.

CYBERATTAQUE DE L'AGENCE NATIONALE DES TITRES SÉCURISÉS : QUOI FAIRE SI VOUS ÊTES CONCERNÉS ?

Porter plainte rapidement afin d'assurer une protection en cas de litige

Si vous êtes concerné par cet incident, il est fortement recommandé de déposer plainte sans délai. En effet, il existe un risque que vos documents d'identité, comme votre carte d'identité ou votre passeport, soient exploités par des personnes malveillantes.

Un risque de fraude financière

Les données volées peuvent être utilisées pour des usurpations d'identité, notamment pour contracter des crédits à votre insu. Dans ce cas, vous pourriez être sollicité par un établissement bancaire pour rembourser des sommes que vous n'avez jamais perçues.

Le dépôt de plainte constitue un élément essentiel pour démontrer votre bonne foi. Il peut vous permettre, en cas de fraude avérée, de contester ces opérations et d'éviter d'avoir à rembourser un crédit contracté frauduleusement en votre nom.

CYBERATTAQUE DE L'AGENCE DU SERVICE CIVIQUE

L'organisme en charge de la mise en place et de l'encadrement du service civique a signalé un incident de cybersécurité affectant sa plateforme de formation, ayant conduit à une fuite de données personnelles.

Données concernées

Les informations compromises incluent :

- l'état civil (civilité, nom, prénom),
- les données de connexion (adresse email), ainsi que
- des données relatives aux structures telles que les numéros d'agrément et la raison sociale.

Pour certains comptes, des coordonnées supplémentaires ont également été exposées, notamment l'adresse postale complète et le numéro de téléphone.

Mesures prises et zones d'incertitude

Les personnes potentiellement concernées ont été informées, et une notification a été adressée à la CNIL.

Une enquête est actuellement en cours. À ce stade, plusieurs éléments restent inconnus, notamment le nombre exact de personnes touchées, l'origine de la faille ainsi que les raisons du délai entre la détection de l'incident et l'information des victimes.

CYBERATTAQUE DE LA PLATEFORME « E-CAMPUS » DE LA POLICE NATIONALE

La plateforme de formation en ligne de la police nationale, « e-campus », a été victime d'un piratage informatique les 17 et 18 mars

La Direction générale de la police nationale (DGPN) a confirmé que des données d'identification concernant des policiers actifs, administratifs et contractuels ont été consultées par un acteur malveillant, tout en précisant que ces informations ne proviennent pas de fichiers de police.

Une plateforme stratégique compromise

Cet outil constitue le principal dispositif de formation continue des agents de la police nationale. Gérée par un prestataire externe pour le compte du ministère de l'Intérieur, la plateforme centralise des informations sensibles telles que les parcours pédagogiques, les certifications professionnelles et les données d'identification des personnels.

Des risques accrus pour les agents

La compromission de ces données soulève des préoccupations importantes. Les informations géolocalisées peuvent permettre d'identifier les zones d'habitation des agents et de leurs familles, les exposant à des risques physiques ou à des opérations d'ingénierie sociale. De plus, les parcours de formation peuvent révéler les spécialisations, les compétences et les affectations potentielles, facilitant le ciblage par des acteurs malveillants.

Des conséquences opérationnelles

Ces données peuvent également être exploitées par des réseaux criminels afin d'adapter leurs stratégies, contourner les dispositifs de surveillance et mieux organiser leurs activités. L'atteinte à l'anonymat des agents constitue ainsi un enjeu majeur de sécurité.

Une externalisation qui interroge

La gestion de la plateforme par un prestataire privé soulève des questions sur les mesures de sécurité mises en place et sur le niveau de supervision exercé par les autorités.

Cet incident rappelle l'importance d'auditer rigoureusement les prestataires pour garantir la protection des informations sensibles.

Réaction et enjeux plus larges

Des mesures ont été prises pour contenir l'incident, sécuriser les accès et évaluer l'étendue de la compromission, sans que les causes précises du piratage ne soient encore connues. Plus largement, cette attaque illustre le fait que les entités stratégiques liées à l'identité numérique et aux infrastructures souveraines demeurent des cibles privilégiées pour la cybercriminalité.

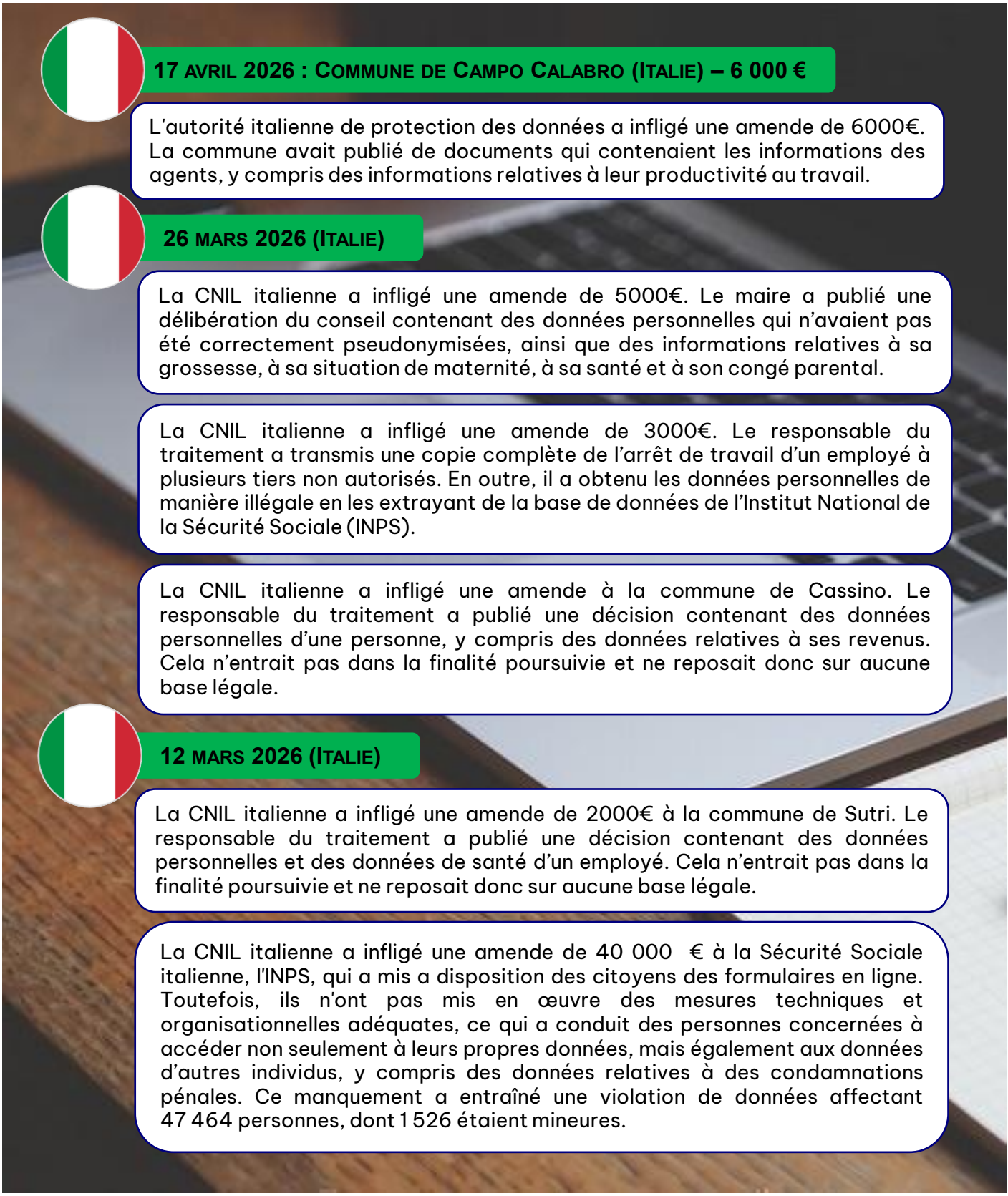
Une question de fond sur la cybersécurité publique

La succession d'incidents touchant des organismes publics manipulant des données sensibles pose une question essentielle : celle de la prise en compte réelle de la cybersécurité dans la gestion des plateformes étatiques.

Elle intervient dans un contexte marqué notamment par la montée des pratiques de double extorsion, combinant chiffrement et divulgation de données.

La montée des cyberattaques montre combien la souveraineté numérique est devenue essentielle pour la France. Le plan gouvernemental vise à mieux protéger les données sensibles, renforcer la sécurité des infrastructures et maîtriser les technologies critiques, afin de garantir la confiance et la résilience des services publics face aux menaces.

Les décisions des autorités chargées de la protection des données



17 avril 2026 : Commune de Campo Calabro (Italie) – 6 000 €

L'autorité italienne de protection des données a infligé une amende de 6000€. La commune avait publié de documents qui contenaient les informations des agents, y compris des informations relatives à leur productivité au travail.

26 mars 2026 (Italie)

La CNIL italienne a infligé une amende de 5000€. Le maire a publié une délibération du conseil contenant des données personnelles qui n'avaient pas été correctement pseudonymisées, ainsi que des informations relatives à sa grossesse, à sa situation de maternité, à sa santé et à son congé parental.

La CNIL italienne a infligé une amende de 3000€. Le responsable du traitement a transmis une copie complète de l'arrêt de travail d'un employé à plusieurs tiers non autorisés. En outre, il a obtenu les données personnelles de manière illégale en les extrayant de la base de données de l'Institut National de la Sécurité Sociale (INPS).

La CNIL italienne a infligé une amende à la commune de Cassino. Le responsable du traitement a publié une décision contenant des données personnelles d'une personne, y compris des données relatives à ses revenus. Cela n'entrait pas dans la finalité poursuivie et ne reposait donc sur aucune base légale.

12 mars 2026 (Italie)

La CNIL italienne a infligé une amende de 2000€ à la commune de Sutri. Le responsable du traitement a publié une décision contenant des données personnelles et des données de santé d'un employé. Cela n'entrait pas dans la finalité poursuivie et ne reposait donc sur aucune base légale.

La CNIL italienne a infligé une amende de 40 000 € à la Sécurité Sociale italienne, l'INPS, qui a mis a disposition des citoyens des formulaires en ligne. Toutefois, ils n'ont pas mis en œuvre des mesures techniques et organisationnelles adéquates, ce qui a conduit des personnes concernées à accéder non seulement à leurs propres données, mais également aux données d'autres individus, y compris des données relatives à des condamnations pénales. Ce manquement a entraîné une violation de données affectant 47 464 personnes, dont 1 526 étaient mineures.

12 mars 2026 (Italie)

Le lycée scientifique Morgagni di Roma a été sanctionné par la CNIL italienne d'une amende de 2 000€. Lors d'une « séance d'éducation affective et sexuelle », le responsable du traitement a distribué aux élèves des feuilles A4 découpées. Ces feuilles avaient déjà été utilisées à d'autres fins et contenaient des informations précises concernant le handicap d'élèves, ainsi que leurs noms complets.

26 février 2026 : Ministère de l'economie et des finances (Italie) – 12 000€

Le responsable du traitement organisait un « concours ouvert, sur épreuves, pour le recrutement ». Le concours comprenait une épreuve de présélection ainsi que des étapes ultérieures. En vertu de la loi, les personnes souffrant de certaines pathologies médicales pouvaient être dispensées de certaines épreuves. Après la présélection, le ministère a publié une liste des candidats admissibles à l'étape suivante, accessible à tous les candidats. Cette liste indiquait quels candidats avaient été dispensés de certaines épreuves, permettant ainsi de déduire des informations sur leur état de santé.

26 février 2026 : Ministère des entreprises et du Made in Italy – 30 000€

Le responsable du traitement a lancé un « concours ouvert, sur épreuves, pour pourvoir un total de 225 postes non dirigeants à temps plein et à durée indéterminée ». Ils ont eu recours à un sous-traitant pour publier la liste de classement, mais celui-ci n'a pas agi conformément au RGPD. Aucun contrat suffisamment encadré n'avait été conclu. Après la clôture du concours, la liste de classement des candidats était restée accessible et en ligne sur le site du ministère. Elle contenait des données personnelles des candidats. Par la suite d'une demande de suppression des données, le ministère a retiré la liste, mais celle-ci est réapparue ultérieurement sur le site d'un tiers.

26 février 2026 : Conservatoire (Italie) – 5 000€

Le responsable du traitement a envoyé un courriel à plus d'une centaine d'employés pour les informer qu'un ancien directeur administratif avait été licencié à la suite de mesures disciplinaires. Le message contenait également des détails supplémentaires sur les motifs du licenciement, notamment le fait que cet ancien employé avait auparavant fait l'objet de poursuites pénales.

20 février 2026 : Université de Szegzd (Hongrie) – 5 570 €

L'autorité hongroise a infligé une amende dans le cadre de la gestion par l'université des logements étudiants. Afin de déterminer quels étudiants pouvaient obtenir une place, l'université a traité les données personnelles des candidats, y compris des données de santé. Toutefois, l'université a procédé à un traitement excessif des données et d'informations sensibles par rapport à la finalité.

20 février 2026 : Etablissement de santé (Grèce) – 5 000 €

Une personne a demandé l'accès à des images captées par le système de vidéosurveillance du centre de santé. Celui-ci n'a répondu à la demande qu'après l'intervention de l'autorité, et de manière insuffisante, les images fournies étant incomplètes et altérées.

12 février 2026 (Italie)

La CNIL italienne a infligé une amende de 4000€ à la commune de Mazara del Vallo. La commune a utilisé un système de vidéosurveillance pour faire respecter le code de la route sans disposer d'une base légale suffisante. En outre, il a utilisé un système de caméras qui n'avait pas été homologué ni approuvé pour cette finalité spécifique. Par ailleurs, le responsable du traitement n'a pas réalisé d'analyse d'impact relative à la protection des données et n'a pas correctement informé les personnes concernées du traitement.

La commune de Monterotondo en Italie a été sanctionné d'une amende de 2000€. La commune utilisait la vidéosurveillance pour protéger des biens, mais a installé les caméras de manière à filmer des zones publiques, ce qui n'était pas nécessaire au regard de la finalité du traitement des données.

La commune italienne de Coccaglio a été sanctionnée de 6000 € pour un usage non conforme de la vidéosurveillance. Le dispositif, initialement installé pour protéger les biens, a été détourné pour une procédure disciplinaire visant un agent. De plus, la commune n'a pas informé correctement les agents et n'a pas effectué d'analyse d'impact.

La commune italienne de Velletri a été sanctionnée de 2000 € pour une application funéraire non conforme. Des données publiques ont été réutilisées à des fins sociales et commerciales. La commune n'a pas suffisamment contrôlé le sous-traitant. Les personnes concernées n'ont pas été correctement informées.

29 janvier 2026 Ministère de la culture (Italie) – 12 000 €

Le ministère utilisait un système de vidéosurveillance afin de protéger les biens de l'établissement. Cependant, il a également utilisé les images à des fins disciplinaires à l'encontre des agents. En outre, le responsable du traitement n'a pas correctement informé les personnes concernées du traitement des données.

29 janvier 2026 (Italie) – Institut Scolaire à Milan (Italie) – 12 000 €

L'établissement scolaire utilise un système de vidéosurveillance dans ses locaux. Pendant les heures de classe, un mineur a été impliqué dans un accident qui a été capté par une caméra de surveillance. Une vidéo de l'incident, diffusée sur l'écran d'un ordinateur, a ensuite été filmée à l'aide d'un téléphone portable et transmise à un détective privé travaillant pour la compagnie d'assurance auprès de laquelle les parents du mineur avaient demandé une indemnisation. Cependant, la vidéo n'avait pas été communiquée aux parents du mineur, qui n'avaient pas non plus été informés du traitement des données.

NÉCROLOGIE

LES DERNIÈRES VICTIMES DE CYBERATTAQUES

CC du Vexin Normand
11 mars 2026

CA Compiègne
14 avril 2026

Mairie de Paris
02 mars 2026

Mairie de Quiberon
03 mai 2026

Police Nationale (plateforme en ligne)
17 mars 2026

ANTS
15 avril 2026

Métropole Aix Marseille Provence
24 mars 2026

Ministère de l'éducation nationale
14 avril 2026

Vaucluse Provence Attractivité
mars 2026

Agence du Service Civique
06 mai 2026

Centre d'Urgence Cyber
0 800 71 13 13
Soutenu par
RÉPUBLIQUE FRANÇAISE
Numéro gratuit
Cyber'Occ délivre un service gratuit d'assistance, en cas de cyber-incident, aux TPE, PME, ETI, collectivités et associations d'Occitanie.
csirt@cyberocc.fr

IA ET COLLECTIVITÉS : UN NOUVEL ENVIRONNEMENT NUMÉRIQUE ENTRE VIGILANCE ET OPPORTUNITÉS

La transformation numérique s'impose aujourd'hui comme un levier incontournable pour moderniser l'organisation de la fonction publique territoriale. Face à la complexification des missions et aux attentes croissantes des citoyens, les collectivités doivent s'appuyer sur des outils innovants, notamment l'intelligence artificielle.

Moderniser la fonction publique territoriale par l'innovation

Cette dynamique est déjà à l'œuvre dans de nombreux territoires. À Dijon, le projet « OnDijon » centralise les données urbaines pour piloter en temps réel l'éclairage, la circulation ou la propreté. À Nantes Métropole, des algorithmes permettent de prédire les besoins en restauration scolaire avec une précision de 98 %, limitant ainsi le gaspillage alimentaire. À Issy-les-Moulineaux, un chatbot basé sur l'IA générative traite des milliers de demandes d'usagers chaque année, améliorant la relation avec le public.

Dans des communes plus petites, l'innovation est également présente : détection de fuites d'eau par IA en Isère, caméras intelligentes pour prévenir les incendies dans les Alpes-Maritimes ou encore outils de détection de dépôts sauvages dans le Val-d'Oise.

Au niveau de l'État, les usages sont tout aussi structurants. France Travail utilise l'IA pour analyser les CV, détecter les offres frauduleuses et accompagner les demandeurs d'emploi, avec plus de 27 cas d'usage déployés à grande échelle.

De son côté, la Direction interministérielle de la transformation publique mobilise des outils d'IA pour analyser les avis des citoyens sur les services publics et améliorer en continu les politiques publiques.

Enfin, le développement d'un modèle souverain comme «Albert», déployé dans plusieurs ministères, illustre la volonté de l'État de structurer une IA publique maîtrisée.

Ces exemples montrent que l'IA transforme déjà en profondeur l'action publique. Toutefois, cette évolution suppose une vigilance accrue en matière de protection des données et de cybersécurité.

Encadrer l'usage de l'IA : une gouvernance structurée et responsable

L'intégration de l'IA dans les collectivités nécessite un cadre organisationnel solide. Les chartes d'utilisation de l'IA permettent de formaliser les bonnes pratiques et de garantir le respect du RGPD.

Les autorités territoriales doivent impulser une stratégie claire. Le manifeste du CIG de la Grande Couronne s'inscrit dans cette logique en promouvant une IA éthique, responsable et souveraine, au service des agents et des usagers. Ce besoin d'encadrement est d'autant plus important que les usages se développent rapidement.

Anticiper avant de déployer : réflexion stratégique et qualité des données

Avant tout déploiement, les collectivités doivent identifier leurs besoins et vérifier la pertinence de l'IA.

L'expérience des collectivités montre que les applications les plus fréquentes concernent la gestion administrative, la relation usagers et l'analyse documentaire.

Des outils comme la retranscription automatique des réunions à Suresnes ou l'aide à la rédaction d'actes administratifs illustrent ces gains de productivité.

Cependant, l'efficacité de ces outils repose sur la qualité des données. Sans bases fiables, l'intelligence artificielle peut produire des résultats erronés ou biaisés.

Souveraineté numérique : un enjeu stratégique

Le recours à l'IA soulève des enjeux majeurs de souveraineté. Le développement de solutions nationales, comme le modèle «Albert», ou l'orientation vers des infrastructures françaises, permet de mieux contrôler les données publiques.

Cette question est au cœur des politiques publiques, notamment dans le cadre du renforcement de la stratégie nationale en matière d'IA et de cybersécurité.

Former pour mieux protéger : une priorité

La formation des élus et des agents est essentielle. Aujourd'hui, une large part des agents publics utilise déjà des outils d'IA, souvent sans cadre formel ni formation adaptée.

Une meilleure formation permettrait de prévenir les risques liés aux données personnelles, en particulier les données sensibles au sens du RGPD. Leur divulgation peut avoir des conséquences graves pour les personnes concernées et exposer les collectivités à des cyberattaques ciblées.

Santé mentale, risques psychosociaux et exigence d'une IA éthique

L'intégration rapide de l'intelligence artificielle dans les collectivités territoriales et les établissements publics ne se limite pas à des enjeux techniques, juridiques ou organisationnels. Elle a également un impact direct sur les individus, qu'il s'agisse des agents publics, des usagers ou plus largement des citoyens, en particulier les jeunes générations.

L'un des premiers effets observés concerne la transformation des conditions de travail. L'automatisation de certaines tâches peut être perçue comme une opportunité, mais également comme une source d'inquiétude. La crainte d'une déqualification ou d'une substitution par la machine peut générer : stress, perte de repères professionnels, sentiment d'isolement ou pression accrue.

Chez les agents, l'introduction d'outils d'IA peut aussi modifier les responsabilités. Lorsque la décision est assistée, voire influencée par un algorithme, la question de la responsabilité individuelle devient plus complexe. Ce déplacement du rôle humain peut créer une tension entre efficacité attendue et responsabilité morale, nourrissant un malaise professionnel si ces évolutions ne sont pas accompagnées.

Les jeunes usagers, quant à eux, sont particulièrement exposés. Habitués aux outils numériques, ils développent des interactions quotidiennes avec des systèmes automatisés, parfois sans en percevoir pleinement les limites. Le recours à des agents conversationnels ou à des outils prédictifs peut influencer leur rapport à l'information, à la décision et à la relation humaine. Il existe un risque d'appauvrissement du sens critique, mais aussi de dépendance à des systèmes qui orientent subtilement les comportements.

Dans ce contexte, l'usage de l'IA ne peut se réduire à une logique de performance ou d'optimisation. Il doit s'inscrire dans une réflexion plus large sur la place de l'humain dans les organisations.

Cela implique de préserver plusieurs équilibres fondamentaux :

- Maintenir la primauté de la décision humaine, en particulier dans les situations sensibles
- Garantir la compréhension des outils utilisés, afin d'éviter une dépendance opaque aux algorithmes
- Protéger la dignité et l'autonomie des individus face aux systèmes automatisés

Une approche éthique de l'IA suppose également de reconnaître que toute innovation porte en elle une responsabilité collective. Les collectivités doivent veiller à ne pas déshumaniser la relation au service public. Le progrès véritable ne se mesure pas uniquement en gains de productivité, mais aussi en capacité à renforcer la confiance, la cohésion sociale et le respect des personnes.

Dans cette perspective, la formation des agents et la sensibilisation des élus doivent intégrer ces dimensions humaines. L'accompagnement au changement devient un enjeu central pour prévenir les risques psychosociaux et construire un environnement numérique équilibré.

Saisir l'opportunité avec responsabilité

L'intelligence artificielle constitue une opportunité majeure pour transformer l'action publique locale. Elle permet d'améliorer l'efficacité des services, de soutenir les agents et de renforcer la qualité de la relation avec les citoyens.

Néanmoins, cette transformation exige une vigilance constante, notamment en matière de protection des données et de cybersécurité. Les élus locaux ont un rôle déterminant pour encadrer ces usages et garantir une IA éthique et souveraine.

Dans les collectivités gardoises comme ailleurs, s'emparer dès aujourd'hui de ces enjeux, c'est préparer un service public plus performant, plus sécurisé et résolument tourné vers l'avenir.

Fiche - Installation des nouveaux élus municipaux

Dans le cadre de leur mandat, les élus auront à traiter de nombreuses données personnelles. Les règles en matière de protection des données leur seront donc applicables.

Mettre en place des outils adaptés à leurs fonctions

Afin de pouvoir communiquer de manière sécurisée, il convient de créer une adresse électronique professionnelle pour chaque élu qui ne doit pas se servir de son adresse personnelle pour réaliser ses missions d'élu. Il convient également d'encadrer l'usage des outils informatiques et téléphoniques mis à leur disposition aux moyens d'une charte informatique ou d'un règlement intérieur dédié.

L'accès des élus aux fichiers de la population, que ce soient des dossiers papier ou informatisés, doit être encadré afin qu'il corresponde aux compétences déléguées aux élus. Dans le cadre des missions attribuées aux élus, il sera nécessaire d'établir un arrêté de délégation. Celui-ci permettra aux élus de formaliser leur accès aux différents fichiers relatifs à la population. En l'absence des délégations correspondantes, l'accès et la transmission de ces fichiers demeurent strictement interdits.

Assurer la sécurisation des outils et supports mis à disposition des élus lors de leur installation

- Créer des moyens d'identification et des droits d'accès au réseau selon les fonctions (maire, adjoint, conseillers) et changer les mots de passe en cas de besoin.
- Fournir des adresses électroniques professionnelles et vérifier la configuration des équipements (smartphone, PC, etc.).
- Contrôler les habilitations sur les logiciels et supprimer les accès des élus sortants.
- Vérifier la configuration des équipements (smartphone, tablette, PC).
- Interdire le stockage sur des supports non sécurisés (clé USB personnelle, cloud privé).
- Mettre en place un registre de suivi recensant l'ensemble des élus détenteurs des clés et des codes d'accès aux bâtiments municipaux. Assurer la mise à jour régulière de ce registre et procéder au changement périodique des codes d'accès, a minima à chaque renouvellement de mandat.

Protéger les données personnelles des élus

Les élus, en qualité de citoyens français, disposent également de droits liés à leurs propres données personnelles. Il convient de ne pas afficher de liste des élus avec leurs coordonnées personnelles à destination du public. Traiter de ces données en interne, dans un souci d'assurer le bon fonctionnement des institutions de l'administration reste tout à fait possible.

Collecter les données personnelles et pièces justificatives nécessaires des élus en respectant le RGPD implique d'informer les élus de l'usage qui sera fait de leurs données. Ainsi, toute fiche des renseignements des élus devra avoir les mentions d'information correspondantes et être signée. De même, avant de pouvoir diffuser leurs coordonnées (professionnelles), il est nécessaire de s'assurer de recueillir leur consentement à cette fin. Cela peut, par exemple, être réalisé via un simple formulaire signé par l'élu et à conserver pour la durée du mandat.

Le droit à l'image des élus

Le droit à l'image est protégé par l'article 9 du Code Civil qui garantit le respect de la vie privée. Les élus municipaux, lorsqu'ils exercent leurs fonctions en situation publique sont soumis à un régime particulier.

- Dans l'exercice du mandat (séances publiques, actes publics) : l'accord des élus n'est pas requis pour ces captations et diffusions, car ils s'expriment dans le cadre de leur mandat.

- En dehors de leurs fonctions ou dans un cadre privé : leur consentement demeure nécessaire. Les élus conservent un droit à l'image dans d'autres contextes : dans un contexte privé, dans un cadre professionnel sans lien avec leur mandat. Même dans l'espace public, si l'élu n'intervient pas dans l'exercice de son mandat, sont accord peut rester nécessaire selon la finalité de l'image ou l'usage envisagé.

Former rapidement les élus aux pratiques numériques

Une session d'installation devrait inclure un module permettant de communiquer les règles d'hygiène informatique afin de prévenir les risques, notamment à propos de :

- La gestion des échanges par mail,
- La manipulation des dossiers de population. Seuls les dossiers strictement nécessaires à l'accomplissement du mandat peuvent être transmis aux élus (exemples sensibles : état civil, listes électorales, dossiers sociaux, données RH, contentieux).
- La non-conservation des dossiers dans des messageries personnelles ou stockages privés.
- L'utilisation des réseaux sociaux dans un cadre institutionnel, il faut veiller à éviter l'usage de réseaux sociaux pour diffuser des données personnelles.
- Le DPO doit être sollicité avant signature d'un nouveau contrat sensible vis-à-vis de tout prestataire accédant à des données.

Prévoir une procédure claire de gestion des incidents

Communiquer aux élus la procédure interne à suivre en cas :

- De perte d'un téléphone ou ordinateur,
- D'envoi de mail à la mauvaise personne/de divulgation accidentelle d'un document,
- De réception d'un message suspect (phishing) et de suspicion de cyber attaque.

Le réflexe immédiat : prévenir la direction et le DPO dans le but de réaliser les déclarations nécessaires auprès de la Commission nationale de l'informatique et des libertés (CNIL).

Informer les élus des droits et obligations liées au RGPD

Les élus nouvellement installés doivent être informés de la politique de mise en conformité au RGPD de la commune, de la désignation du DPO et des situations dans lesquelles le solliciter. Le DPO est le point de référence pour tout nouveau projet impliquant des données, la gestion d'incidents de sécurité, la mise en conformité des documents et l'accompagnement des services dans leurs pratiques quotidiennes.

Il sera nécessaire d'informer les élus concernant le registre des traitements de la commune ainsi que sur les procédures à suivre en cas de violations des données, de contrôle de la CNIL et d'exercice des droits des personnes.

Assurer la continuité du secrétariat municipal

Il est nécessaire d'assurer la continuité de la gestion de la mairie dans cette période particulière. Ainsi, la destruction d'informations doit être soigneusement encadrée. Aucun document ne peut être détruit sans laisser une trace ou sans consulter le prestataire informatique ou l'archiviste. Les identifiants, les mots de passe, les comptes et les dossiers informatiques font partie des archives municipaux et sont des données qui appartiennent à la commune.

Les messages figurant dans la boîte aux lettres doivent s'apprécier au cas par cas, selon les informations contenues dans les documents et les messages électroniques : informations librement communicables, informations qui relèvent du secret relatif à la vie privée, informations relatives à la sécurité publique, et les informations relatives au secret médical.

Fiche - Obligations et responsabilités (avec liens pratiques)

Rappel : dans le Gard, en 2026, le récolement règlementaire doit se faire sur la plateforme nationale Démarches Numériques via le lien envoyé par la préfecture le 5 mars 2026. Vous trouverez les notices méthodologiques et recommandations relatives au récolement des archives communales et intercommunales à effectuer suite aux élections municipales et communautaires des 15 et 22 mars 2026 sur le site France Archives via le lien suivant :

https://francearchives.gouv.fr/fr/circulaire/DGPA_SIAF_2025_011

Les responsabilités de la collectivité

Conserver tous les documents : "*Les archives sont l'ensemble des documents, y compris les données, quels que soient leur date, leur lieu de conservation, leur forme et leur support produits ou reçus par toute personne physique ou morale et par tout service ou organisme public ou privé dans l'exercice de leur activité.* "Article L2111-1 du Code du Patrimoine ;

Constituer les registres de délibérations et des arrêtés selon la règlementation en vigueur ;

S'assurer du respect du secret et de la communicabilité, qu'ils s'agissent des délais règlementaires ou du règlement RGPD ;

Assurer la conservation dans des conditions sécurisées (protection contre les dégâts et les vols).

Et attention :

Interdiction de destruction sans visa de la Direction des Archives Départementales qui exerce le contrôle scientifique et technique sur les archives publiques de tout le département ;

Interdiction de cession ou appropriation, les archives sont des biens publics inaliénables et imprescriptibles.

Les responsabilités des élus

Une responsabilité immédiate personnelle civile et pénale dès la prise de fonction ;

Une obligation de surveillance, de récolement et d'alerte concernant toutes les archives quelques soient leurs formes et leurs supports (papier, numérique, objets, œuvres, cadeaux reçus, diplômes, médailles...).

"*La conservation des archives est organisée dans l'intérêt public tant pour les besoins de la gestion et de la justification des droits des personnes physiques ou morales, publiques ou privées, que pour la documentation historique de la recherche.* "Article L.211-2 du Code du patrimoine

Sans oublier que, qu'ils s'agissent de documents numériques ou papiers *« Les dossiers traités par un élu dans l'exercice de ses fonctions publiques [...] appartiennent à la collectivité [...] et doivent [...] être versés au service d'archives. »* (Voir les Règles de gestion et de sélection des archives)

Une conservation assurée par une bonne gestion (conseils et procédures des Archives Départementales du Gard) et des conditions climatiques précises :

- 16-22 °C
- 40-55 % d'humidité relative
- Pas, peu de variations de températures et d'humidité
- Pas d'éclairage naturel
- Respect de la norme ISO 11799 :2024

Lors de l'aménagement d'un local archives (travaux, construction) ou d'un déménagement, il ne faut pas oublier d'en informer les Archives Départementales.

La conservation des archives est une dépense obligatoire du budget, article 2321-1 du Code Général des collectivités territoriales. Le département du Gard et le Ministère de la culture proposent des subventions pour la restauration et la protection incendie de vos archives publiques, n'hésitez pas à vous renseigner !

Liens vers les subventions : dispositif national et le dispositif départemental.

À consulter : Règles générales en matière de propriété, conservation et mise en valeur (Articles R1421-1 à R1421-8)

CAS PRATIQUE : La gestion des archives en fin de mandat et lors des alternances politiques

Présentation de l'affaire de référence

- **Les faits :** À la suite d'une alternance politique lors des élections municipales de 2020 dans la commune de Villeneuve-sur-Yonne, la nouvelle équipe constate la disparition de nombreux documents officiels essentiels à la continuité du service public. Une enquête permet de découvrir que des dizaines de cartons d'archives administratives ont été délibérément enterrés sur un terrain municipal, les rendant totalement inexploitables à cause de l'humidité.

- **La procédure :** Une plainte pénale est déposée par la nouvelle municipalité. L'enquête judiciaire mène l'ancien maire et son ancienne Directrice Générale des Services (DGS) devant le Tribunal correctionnel pour *"destruction illégale d'archives publiques"*.

- **La conclusion juridique (2023) :** L'ancien maire est relaxé au bénéfice du doute, la preuve formelle d'un ordre direct de sa part n'ayant pas pu être légalement établie.

- **La condamnation :** C'est la Directrice Générale des Services (DGS) de l'époque qui a été reconnue coupable et condamnée pénalement pour avoir matériellement organisé et exécuté la destruction de ces pièces.

Analyse des risques

Ce cas met en lumière une réalité souvent méconnue : la responsabilité pénale des agents et des élus en matière de gestion documentaire.

1. Risque juridique et pénal

Les archives publiques (qu'elles soient sur papier ou numériques) sont protégées par le Code du patrimoine (Article L. 214-3).

Le délit : Le fait de détruire, détériorer ou détourner des archives publiques est puni de 3 ans d'emprisonnement et de 45 000 € d'amende. Comme le montre cette jurisprudence, l'administration (DGS, agents) peut être condamnée, même si l'impulsion initiale est politique.

2. Risque RGPD et Cybersécurité

Si l'affaire de Villeneuve-sur-Yonne concernait des archives physiques, la même logique s'applique au numérique (e-mails professionnels, bases de données des administrés, serveurs de fichiers). Au sens du RGPD, l'effacement non autorisé ou la perte de disponibilité de données personnelles constitue une violation de données. Elle doit être notifiée à la CNIL dans les 72 heures.