CENTRE NATIONAL DE LA FONCTION PUBLIQUE TERRITORIALE

TEST D'ORIENTATION AUTOMNE 2017

CATÉGORIE A

PRINCIPAL

Durée : 3h00

CADRE RESERVE AU CNFPT
Note finale : ..... / 20
Appréciation du correcteur : .....
.....
.....
Décision d'orientation :
Accès direct en préparation ☐
Tremplin A module court (4 jours) ☐
Autre parcours ☐

Un examen de catégorie A exige un champ de connaissances élargi et une méthodologie de l'écrit rigoureuse. Ce test a pour but d'évaluer les acquis et compétences indispensables pour engager une préparation dans de bonnes conditions.

Compétences évaluées pour chaque séquence

Séquence 1 « analyse et reformulation » : être en mesure d'identifier les informations essentielles d'un texte et d'en analyser le contenu de manière fiable.

Séquence 2 « synthèse et développement » : effectuer des regroupements d'idées à partir d'un corpus de documents afin d'apporter une réponse structurée par un plan comportant des préconisations.

Séquence 3 « culture générale et territoriale » : témoigner d'une bonne connaissance des débats contemporains sur la société et des problématiques liées à l'action publique locale.

La maîtrise des codes de l'écrit sera évaluée tout au long du test. Un maximum de 2 points sera retranché du total obtenu si la copie du candidat comporte plus de 10 fautes.

Le candidat devra apporter des réponses entièrement rédigées et structurées. **Un candidat qui n'aborderait pas tous les exercices serait fortement pénalisé.**

Pour intégrer la préparation demandée, un candidat devra obtenir une note finale supérieure ou égale à 10/20.

NOMBRE PAGES : 27

SEQUENCE 1 : ANALYSE ET REFORMULATION (12 points)

Lire le texte suivant :

Et si on changeait tout ?

Quitter la ville

Le retour à la nature imprègne l'imaginaire d'une majorité de Français. Pour autant, est-il réellement la promesse d'un avenir meilleur ?

RÉGIS MEYRAN

Tout plaquer pour changer de vie en s'installant à la campagne : voilà, semble-t-il, le rêve secret partagé par 7 millions de citadins en France. Les Français qui se mettent au vert sont de plus en plus nombreux, au point de constituer un phénomène de société. En se mettant au travail à distance, en faisant des déplacements quotidiens vers les villes, ou même en exerçant pleinement leur activité à la campagne, les néoruraux cherchent à réaliser une utopie de liberté et d'épanouissement personnel qu'ils ne trouvaient pas en ville. Mais qu'y trouvent-ils réellement ?

Les faits sont là : selon un rapport remis au Sénat en 2008, l'espace rural français connaît un renouveau démographique. Depuis 1975, on assiste en effet à l'augmentation globale de la population rurale du pays. Avec un solde migratoire désormais positif, le taux de croissance de la population a atteint 1,3% en 2005 contre 0,5% en 1999 pour l'ensemble des communes de 2 000 habitants – soit trois fois plus que pour les communes urbaines (le taux de croissance de celles-ci étant passé de seulement 0,3 % à 0,5 % sur la même période). Ainsi, en 2003, on comptait 2 millions de migrants vers les campagnes, soit 4,2 % de la population française, et ce chiffre a augmenté depuis. Selon une enquête Ipsos de 2010, le nombre de ménages et leurs revenus, entre 2002 et 2007, ont même augmenté plus vite dans l'espace rural que dans les villes, ce qui est une nouveauté. Il s'agit certes d'une moyenne. En réalité, certaines zones à dominante rurale sont plus attractives, alors que d'autres, plus isolées, subissent un processus croissant de désertification (zones reculées de montagne, Bretagne centre…).

Qui sont ces néoruraux ? Tous les spécialistes soulignent l'aspect fluide et hétérogène de ce phénomène qui, toutefois, concerne avant tout des personnes jeunes d'origine citadine. D'après une enquête Ipsos (2003), 46 % d'entre eux ont entre 25 et 34 ans. Mais leurs profils sont en réalité variés et leur portrait reste à étudier plus finement (1). On trouve ainsi pêle-mêle d'anciens cadres ou des retraités qui montent une chambre d'hôte, des jeunes ménages de classe moyenne, des artistes qui veulent vivre de leur production – cela peut aller de l'artisanat local à la création musicale comme le groupe Aquaserge, qui a longtemps vécu dans une ferme-studio communautaire dans la campagne toulousaine. Ces derniers vivent d'ailleurs non loin de Tarnac, le quartier général du Comité invisible, ce groupe de philosophes néoruraux anonymes, auteurs du *best-seller* anticapitaliste *L'Insurrection qui vient* (2).

Une typologie des néoruraux à travers les âges

L'historienne Catherine Rouvière (3) s'est intéressée à ce phénomène, à partir du cas de l'Ardèche et en le généralisant ensuite à la France entière. Elle dresse une typologie générationnelle des néoruraux, dont certaines motivations sont restées les mêmes alors que d'autres évoluent au fil des décennies. La première vague (1969-1973) était constituée de hippies et de marginaux cherchant l'autarcie et voulant créer des « communautés », beaucoup d'entre eux sont repartis à la ville. Avec l'essor de l'écologie politique et la crise économique, la deuxième vague (1975-1985) ne voulait plus transformer la société mais remettait en cause la croissance comme but ultime, formulait un projet de vie agricole, et visait à s'installer dans la société autochtone. Une troisième génération (1985-1995) est venue à la campagne par souci d'un meilleur cadre de vie et d'une authenticité supposée génératrice d'identité et de liberté : elle était faite de travailleurs sociaux, d'employés, d'instituteurs, de jeunes couples avec enfants… La quatrième génération (1995-2000) serait plus précaire : des personnes touchant les *minima* sociaux, des femmes seules avec enfant, des jeunes au mode de vie nomade qui viennent chercher refuge et équilibre dans le monde rural. Enfin, la dernière vague (jusqu'à nos jours) serait constituée de nouveaux radicaux et libertaires (altermondialistes, zadistes, décroissants…) qui s'installent pour certains dans des yourtes ou des cabanes. Sur le terrain des valeurs en revanche, au-delà de la diversité des profils et des générations, on trouve plusieurs points communs : refus de la surconsommation, critique du capitalisme, souci de la production locale et de l'agriculture biologique, de l'entraide, respect de la nature… Ces néoruraux sont-ils les précurseurs d'un changement de civilisation ? Possible. Pour C. Rouvière, ils restent toutefois tributaires du vieux mythe agrarien né au 19e siècle. Malgré son aspect romantique, ce mythe reconduit un dualisme caricatural entre la mauvaise ville, artificielle, aliénante, capitaliste et soumise à un temps

Marie Nascimento/Rea

linéaire; et la bonne campagne, faite de gens simples et libres, obéissant aux lois cycliques de la nature, épanouissante, anticapitaliste.

La possibilité de fortes désillusions

Le rêve est une chose, mais que trouvent-ils réellement une fois le « retour à la nature » effectué ? En idéalisant ainsi le lieu où l'on veut habiter et changer de vie, ils semblent s'exposer à la possibilité de fortes désillusions, car l'entreprise se révèle souvent risquée. Certes, face à la crise économique, l'activité agricole peut jouer un rôle de refuge et d'insertion sociale. Mais ils s'exposent toutefois à un risque de déclassement. En migrant vers des territoires isolés, les néoruraux sont souvent contraints de s'adapter à l'offre locale, ce qui peut les amener à accepter des emplois moins qualifiés ou plus précaires (4). Ainsi, une étude effectuée dans le département de la Nièvre montre que les nouveaux arrivants sont plus diplômés que les Nivernais autochtones, mais qu'ils occupent moins souvent un emploi stable et connaissent régulièrement le chômage (5). Par ailleurs, de nombreux migrants sont des victimes de la ségrégation spatiale: ils s'exilent parce que la vie à la ville est trop chère. Les chômeurs ont ainsi un taux de migration deux fois plus élevé que les actifs et ils se retrouvent principalement dans le rural isolé, et les locataires ont un taux cinq fois supérieur à celui des propriétaires (6)! Enfin, le rêve d'harmonie peut se révéler plus compliqué que prévu à réaliser, sur le plan pratique: vivre dans un hameau ou dans un petit village constitue un véritable changement culturel (le silence, le calme, l'isolement, l'entre-soi…) et les néoruraux peuvent avoir quelques difficultés à se socialiser avec les locaux. Bref, si l'utopie néorurale fait de plus en plus d'adeptes, elle reste un pari risqué. ■

> Si l'utopie néorurale fait de plus en plus d'adeptes, elle reste un pari risqué.

(1) **Clothilde Roullier**, « Focus - Qui sont les néoruraux ? », *Informations sociales*, n° 164, 2011/2.
(2) **Comité invisible**, *L'Insurrection qui vient*, La Fabrique, 2007.
(3) **Catherine Rouvière**, *Retourner à la terre. L'utopie néorurale en Ardèche depuis les années 1960*, Presses universitaires de Rennes, 2015.
(4) **Ariac**, « Les pauvres en milieu rural, et notamment les jeunes ruraux et les néoruraux », rapport pour l'ONPES, novembre 2015.
(5) **Consulter** www.nievre.gouv.fr
(6) **Yannick Sencébé et Denis Lepicier**, « Migrations résidentielles de l'urbain vers le rural en France : différenciation sociale des profils et ségrégation spatiale », *EspacesTemps.net*, 2007.

Source : « Quitter la ville », extrait du magazine *Sciences Humaines*, n°288, janvier 2017

Exercice 1 (5 points)

Résumer ce texte, en une douzaine de lignes maximum. Vous prendrez soin d'approfondir le travail de connexion des idées entre elles et la finesse de l'expression.

Exercice 2 (1 point)

A l'aide des éléments d'information proposés par l'article ci-dessus, définissez « l'utopie néorurale ».

Exercice 3 (2 points)

Selon l'article de presse proposé, quelles sont les caractéristiques principales des néoruraux ?

Exercice 4 (4 points)

Qu'est-ce qu'être citadin aujourd'hui en France ?

Pour développer une réponse argumentée à la question, vous pourrez vous appuyer sur certaines informations du texte ci-dessus, mais avant tout sur vos connaissances personnelles.

SEQUENCE 2 : SYNTHESE ET DEVELOPPEMENT (14 points)

Lire les documents suivants :

DOSSIER

Sécurité informatique : comment se protéger ?

RÉALISÉ PAR PIERRE-ALEXANDRE CONTE

Confiance
Sur le net, les collectivités doivent tisser un lien de confiance avec les citoyens. Pour s'en assurer, il est indispensable de faire de la cybersécurité une priorité. Un incident peut rompre cette relation et avoir des conséquences en termes de réputation.

Souveraineté
Avec la dématérialisation croissante des données et la multiplication des outils numériques, la cybersécurité est aussi devenue un enjeu de souveraineté nationale. En témoigne la problématique récente entourant le stockage «en nuage».

Obligation
Si les collectivités sont sommées de veiller à ce que la protection des données soit assurée, la loi va évoluer vers des contraintes et des sanctions encore plus importantes. Prendre en compte la sécurité n'est pas une option, c'est une nécessité.

Les collectivités, des cibles potentielles sous surveillance

Si elles n'en ont pas toujours conscience, les collectivités territoriales peuvent bel et bien être victimes de cyberattaques. Et ce, pour de multiples raisons. En cas de faute avérée, les sanctions encourues peuvent devenir particulièrement difficiles à assumer.

DATE CLÉ

4 mai 2018
C'est la date à laquelle le règlement européen sur la protection des données personnelles entrera en application. Ses objectifs? Renforcer les droits des personnes, responsabiliser les acteurs traitant des données et crédibiliser la régulation. Les sanctions seront renforcées en cas de manquement à la loi. Les amendes pourront, par exemple, s'élever à 20 millions d'euros pour les collectivités.

Une République numérique. C'est ainsi qu'a été baptisée la loi portée par l'actuelle secrétaire d'Etat chargée du numérique, Axelle Lemaire, parue le 8 octobre 2016 au «Journal officiel». Un nom ô combien symbolique et révélateur de la profondeur de la transformation vécue par l'ensemble de la société. Celle-ci touche naturellement les collectivités territoriales, qui bénéficient des multiples avantages qu'elle génère, mais qui doivent, dans le même temps, composer avec de nouvelles obligations. Parmi elles, figure en tête de liste la sécurisation de leur système d'information.

En préambule de son rapport d'activité annuel paru en 2016 (*), l'Agence nationale de la sécurité des systèmes d'information (Anssi) introduisait le sujet comme suit: «Les technologies numériques procurent des gains de productivité et sont donc source de richesse et de compétitivité pour notre pays, mais elles induisent également des vulnérabilités nouvelles. La cybersécurité est devenue, de ce fait, une condition structurante, non seulement de la sauvegarde de notre patrimoine économique et intellectuel, mais aussi de la protection physique de nos concitoyens.» Des propos signés Louis Gautier, secrétaire général de la défense et de la sécurité nationale.

LES SITES WEB EN PREMIÈRE LIGNE

La première erreur en matière de sécurité informatique consiste à penser qu'une collectivité, quelle que soit sa nature, n'a aucune raison d'être la cible d'une attaque. C'est pourtant un raisonnement fréquemment rencontré au sein des petites et moyennes communes, qui considèrent parfois qu'elles ne détiennent rien qui puisse intéresser d'hypothétiques assaillants. «Comme tout un chacun qui dispose d'une visibilité sur internet, les collectivités territoriales peuvent faire partie des victimes d'une vague d'attaques, précise Guy Flament, référent de l'Anssi au sein de la région Nouvelle Aquitaine. Leur présence sur internet, notamment par le biais de leurs sites web, offre des surfaces pour les attaquants, qui peuvent leur permettre d'afficher des messages de revendication ou de propagande.

Ensuite, les collectivités subissent des attaques par des "rançongiciels" qui prennent en otage leur système d'information et offrent de le libérer contre une rançon (lire p.35). En ce qui concerne les autres menaces informatiques que peuvent être le sabotage ou l'espionnage, elles ne sont pas, pour le moment, particulièrement visées. Mais elles pourraient le devenir, notamment à cause du nombre de données à caractère personnel qu'elles hébergent.» ↄOO

Les collectivités territoriales brassent en effet de plus en plus de données, dont certaines s'avèrent particulièrement sensibles. Elles sont au cœur de toutes les préoccupations, comme en témoignent les nombreux articles qui leur sont consacrés au sein de la loi pour une République numérique. Il convient donc de les protéger. «Les collectivités détiennent notamment l'état civil. Il ne faudrait pas qu'un jour ces fichiers puissent être modifiés par des attaquants. Les comptes de la commune intéressent aussi les gens et tout ce qui touche aux dossiers de consultation publique», lance Guy Flament.

50 %

Dans son rapport d'activité concernant l'année 2015, l'Anssi explique avoir reçu 4 000 signalements, soit 50 % de plus qu'en 2014. L'Agence a aussi dû traiter une vingtaine d'incidents de sécurité majeurs.

SANCTIONS PÉNALES

La protection des données du citoyen est garantie par la loi «informatique et libertés». C'est évidemment la Commission nationale de l'informatique et des libertés (Cnil) qui veille au respect de cette dernière. Ses compétences ont été élargies par la loi pour une République numérique. Sur le plan financier, les collectivités encourent une amende pouvant s'élever jusqu'à 3 millions d'euros; ce n'est pas rien! La Cnil peut aussi ordonner que l'organisme sanctionné informe à ses frais les victimes. La loi prévoit par ailleurs la possibilité de sanctionner pénalement les maires, les présidents de conseils régionaux et de conseils généraux en cas de manquement grave, comme le fait de ne pas prendre les mesures nécessaires pour garantir la confidentialité des informations ou l'utilisation de ces dernières à d'autres fins.

A partir du mois de mai 2018, les collectivités devront appliquer le règlement européen sur le sujet. Concernant ce dernier, selon Pierre Deprez, avocat du cabinet DS avocats dans le département «droit de la propriété intellectuelle, technologies numériques et data» (lire p.39), on parle d'un «changement de paradigme». Cela signifie le passage «d'un régime de déclaration et d'autorisation des traitements à un régime "d'accountability", "d'autoresponsabilité"». Les communes devront conserver «une trace des moyens techniques et organisationnels qu'elles auront mis en œuvre pour assurer la sécurité des données», dans le but de montrer patte blanche en cas de contrôle.

Mais les données ne sont pas l'unique préoccupation des collectivités. D'autres domaines requièrent leur attention, à l'image des objets connectés. Ce sont de formidables outils, mais ils peuvent aussi se retourner contre ceux qui les utilisent. «Les objets connectés, comme les smartphones il y a quelques années, représentent une augmentation de la surface d'attaque puisqu'ils sont, par nature, connectés à internet. Si ces objets ne sont pas correctement configurés et sécurisés, ils offrent une porte d'entrée à d'éventuels attaquants», précise Guy Flament.

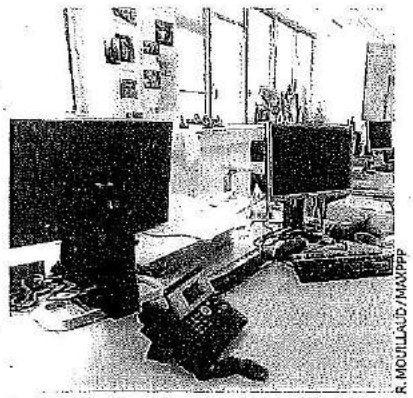
DES RISQUES DIVERS

«L'émergence des outils connectés implique de prendre ses précautions, déclare de son côté Olivier Fouqueau, directeur général des services d'Infocom94, syndicat intercommunal informatique du Val-de-Marne. Quand une direction générale des services techniques, voire un élu, décide que c'est super d'équiper toutes les places de parking d'un capteur pour permettre de savoir, à distance, par le biais de son téléphone portable, s'il y a une place pour se garer, mais qu'il n'y a pas de sécurité autour, cela peut très vite devenir difficile à gérer.» Les rapports affirmant que la cybercriminalité est en constante

L'expérience traumatisante d'une commune piratée

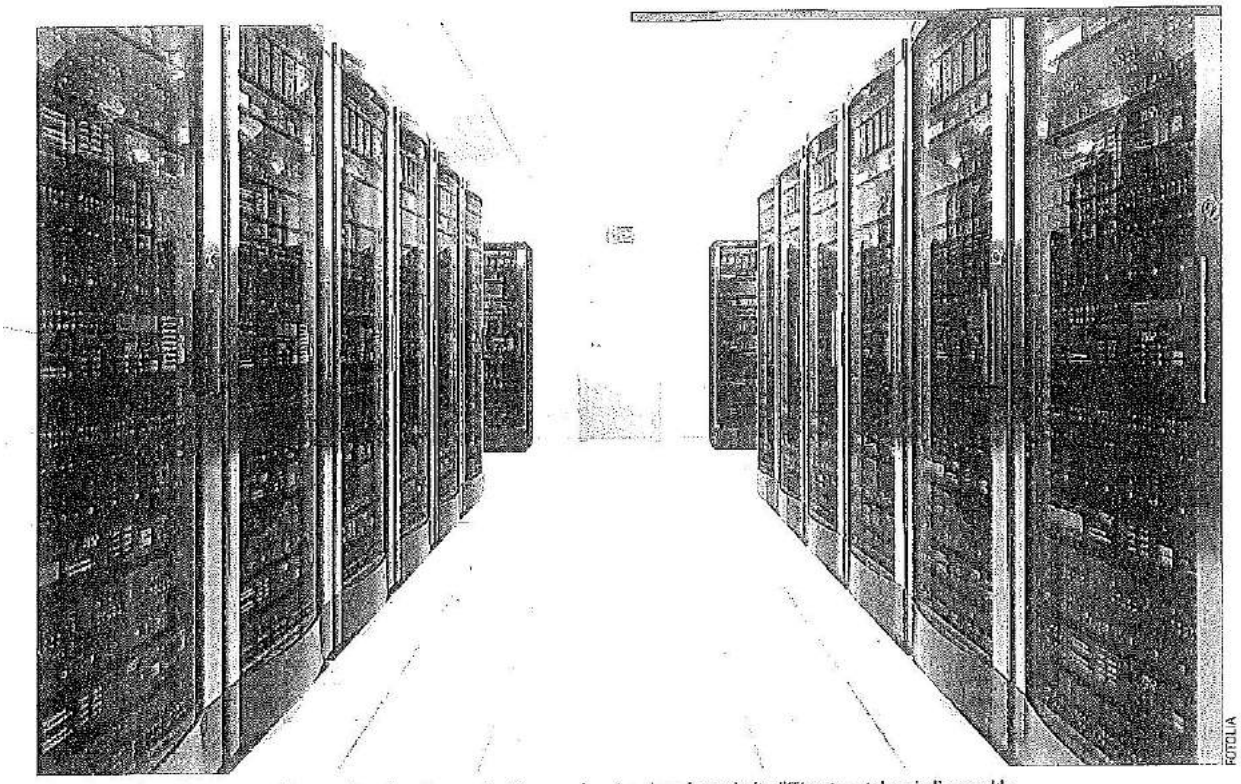
Choc Chaque jour ou presque, des collectivités découvrent qu'elles ont été victimes d'une attaque informatique. Mais difficile de témoigner à visage découvert. Voici ce qu'une victime raconte, sous couvert d'anonymat: «Nous sommes arrivés un matin et nos postes informatiques étaient bloqués, explique cette directrice générale des services. Impossible de travailler dans ces conditions. Sur les écrans était affiché un message énigmatique et surtout, une demande de rançon.»

Si la police a rapidement été prévenue, la commune a dû se résoudre à trouver une solution au plus vite pour reprendre une activité normale. «Nous ne pouvions pas payer la somme, explique-t-elle. Nous avons appelé notre prestataire informatique qui a fait le déplacement et nous a indiqué qu'une grande partie de nos données, notamment les plus récentes, étaient perdues. Personne n'avait anticipé le problème. Cela a créé beaucoup de remous au sein de la collectivité, dans la mesure où nous ne savons pas qui est responsable de l'attaque. L'enquête est toujours en cours. Plusieurs pistes ont été évoquées, dont des personnes hostiles à certaines décisions locales. C'est une expérience qui reste encore assez traumatisante pour nous.» Si le prestataire informatique a fourni une solution d'appoint pour que les données soient plus fréquemment sauvegardées, aucun changement en profondeur, en termes de sécurité, n'a été apporté à ce jour.



R. MOUILLAUD/MAXPPP

Le vol de données peut mettre toute une activité au point mort. Une expérience qui s'avère très choquante pour les agents.



Nombre de collectivités sont touchées par des cyberattaques. Protéger ses données, dans des endroits différents, est donc indispensable.

augmentation sont rendus publics de manière quasi quotidienne. Pour autant, il n'est pas si évident de trouver une collectivité territoriale qui accepte de faire part d'une mauvaise expérience (lire p.34). La raison est simple: elle relève de la peur de voir son image se détériorer. C'est là l'un des principaux risques encourus, notamment par les villes. «Il ne se passe pas une journée sans qu'il y ait un site internet défiguré dans la région», déplore le référent de l'Anssi en Nouvelle Aquitaine. En cas de pertes de données et de responsabilité avérée, le règlement européen demandera également aux collectivités, en 2018, d'informer le public quant à ses failles de sécurité.

Si les communes sont concernées par leur image, elles doivent en plus composer avec l'inaccessibilité de leur site. Ce qui peut altérer de manière plus ou moins grave la mission de service public. La perte peut aussi être financière, notamment s'il y a demande de rançon, les sommes demandées étant, la plupart du temps, élevées. «Le sujet de la sécurité est souvent diabolisé, regrette Frank Mosser, expert dans le domaine de la cybersécurité et président de MGDIS, société éditrice de services logiciels de pilotage et de valorisation de l'action publique, basée à Vannes. Quand ça fait trop peur, on a tendance à mettre la tête dans le sac et à faire l'autruche. Il y a quelques années, ce n'était pas si grave que cela. Là, ça le devient un peu plus.» ●

(*) goo.gl/OdlYA7

Le «rançongiciel», fléau international en pleine expansion

Extorsion Tout le monde ou presque a entendu parler de Locky. Ce «ransomware» – «rançongiciel» en français – s'est rendu populaire en faisant de nombreuses victimes au cours de l'année passée. Une fois activé sur l'ordinateur de la personne visée, ce dernier chiffre les données et demande une somme d'argent en échange de leur restitution. S'il reste l'exemple le plus connu, Locky n'est pas un cas unique. Loin de là.

290 MILLIONS DE DOLLARS

Le FBI estime que durant le premier trimestre de l'année 2016, environ 209 millions de dollars ont été extorqués par le biais de «rançongiciels». Aux Etats-Unis, le Hollywood Presbyterian Medical Center a fait partie des victimes au mois de février 2016. Paralysé pendant plus d'une semaine, il avait fini par débourser la somme de 17000 dollars pour reprendre une activité normale. Et ce, après avoir dû envoyer de nombreux patients vers d'autres établissements. Une mésaventure similaire est arrivée trois mois plus tard au Kansas Heart Hospital. Mais cette fois, après avoir payé la rançon, l'hôpital n'a pas pu récupérer ses fichiers. Pire, une seconde somme d'argent lui a été demandée.

Fin janvier, c'est la police de Washington qui s'est aperçue que le réseau de vidéosurveillance de la ville ne fonctionnait plus correctement. Avant de prendre connaissance du problème: depuis le 12 janvier, un «ransomware» avait commencé à faire son œuvre, paralysant 123 des 187 caméras utilisées. En cherchant la source du dysfonctionnement, des enquêteurs sont tombés un peu plus tard sur un message les invitant à payer une somme. Ce qui n'a pas été fait. Le réseau a été réinstallé dans l'urgence. ●

Quelles solutions mettre en place pour une sécurité accrue ?

Il existe différentes méthodes permettant de faire face à la cybercriminalité : la formation pour éviter la faille humaine, la mutualisation pour partager savoirs et ressources, et des solutions avancées qui aident à protéger ses données.

Lorsqu'on les interroge sur la cybersécurité, nombreuses sont les collectivités territoriales qui nient encore l'importance du sujet. A l'inverse, certaines d'entre elles ont parfaitement conscience des enjeux, mais se montrent fatalistes au regard de la fréquence accrue des attaques, année après année. Pourtant, il existe de nombreuses solutions permettant de réduire nettement les risques, y compris pour les communes les plus modestes.

A travers son référentiel général de sécurité (RGS), l'Anssi a fixé un cadre réglementaire «permettant d'instaurer la confiance dans les échanges au sein de l'administration et avec les citoyens».

S'y conformer est aujourd'hui une nécessité pour les collectivités. L'agence a commencé à envoyer, à la fin de l'année 2015, un agent dans chacune des treize régions, pour gagner en proximité. Plus simplement, un guide contenant 42 règles d'hygiène informatique a été publié le 23 janvier 2017. «Le respect d'un certain nombre de règles couvre 80 % des risques, explique Guy Flament, référent de l'Anssi dans la région Nouvelle Aquitaine. Et là, on ne parle même pas d'investissement matériel ! L'investissement va passer par la formation et la sensibilisation du personnel», ajoute-t-il.

FORMATION

S'il est important de prendre en considération les failles techniques, les erreurs humaines sont extrêmement fréquentes lors d'attaques des systèmes d'information. La cybersécurité est l'affaire de tous et de chacun. Un simple clic innocent sur un lien présent dans un mail peut aujourd'hui paralyser l'ensemble des postes informatiques d'une collectivité. Aussi, la formation revêt-elle une grande importance pour prévenir les offensives.

Selon Guy Flament, il existe «un manque de sensibilisation au risque informatique» dans les collectivités. Ce dernier précise par ailleurs que la formation s'oriente souvent «vers les responsables informatiques des collectivités, qui sont déjà un peu mieux formés». L'accent doit donc être mis sur «la sensibilisation du personnel, de tous les personnels». René-Yves Labranche, directeur des systèmes d'information mutualisés entre la communauté urbaine et la ville de Dunkerque (lire p.38), prend le problème très au sérieux : «Une fois par an, au minimum, nous lançons une information auprès des organisations syndicales lors d'un comité technique. Nous organisons également des formations sur la sécurité auprès des agents. Les nouveaux arrivants doivent valider la charte informatique et s'engager à en avoir pris connaissance.»

MUTUALISATION

Les collectivités locales de taille plus modeste ont tendance à se sentir démunies devant l'ampleur du problème. Elles n'ont souvent ni les moyens, ni les compétences pour faire face aux cyberattaques.

«La solution, c'est la mutualisation, lance Frank Mosser, expert en cybersécurité et président de la société MGDIS. On sait aujourd'hui que pour un maire, respecter les réglementations, ça devient compliqué. Un expert en sécurité, une petite commune ne peut pas s'en payer un.»

Olivier Fouqueau est le directeur des services du syndicat intercommunal Infocom94, dans le Val-de-Marne. Celui-ci compte 19 adhérents principaux comprenant notamment des collectivités de tailles différentes, dont une commune de 2500 habitants. «En cumulant territoires et villes, nous couvrons environ 800 000 habitants, lance-t-il. Cela nous donne du poids dans nos relations avec les éditeurs. A la fois en termes de prix et de capacité à obtenir des mobilisations.» Avant de renchérir:

L'EXPERT

FRANK MOSSER, président de la société MGDIS

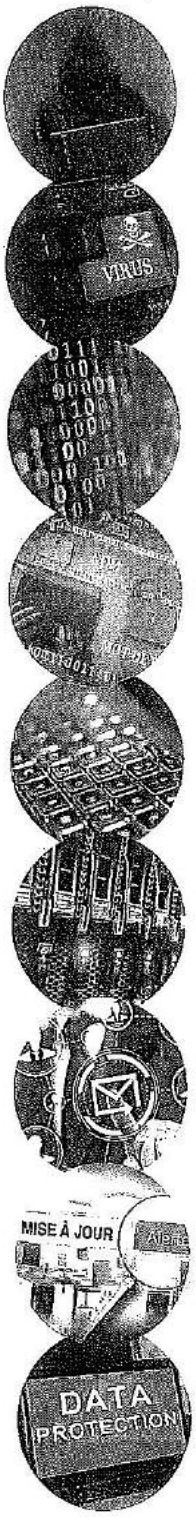
«Un temps doit être consacré à la sécurité dans l'appel d'offres»

«Par rapport aux appels d'offres auxquels on répond, la cybersécurité est un sujet que l'on met souvent en avant, mais qui n'est pas toujours mentionné au niveau de la demande, et qui n'est pas toujours un critère technique important dans le choix du prestataire. Au cours de la conception d'un logiciel, si vous enlevez le volet "sécurité", cela coûte moins cher à développer. Il faut en avoir conscience. Si l'on parle d'objets connectés, de "smart cities", de nouveaux services, il y a un temps qui doit être consacré à la sécurité dans l'appel d'offres. Cela doit faire partie des exigences de tout cahier des charges. Et il faut s'adjoindre les compétences pour pouvoir ensuite valider cette dimension sécuritaire.»

9

C'est le nombre d'étapes que contient le guide d'homologation des systèmes d'information produit par l'Anssi à destination des collectivités territoriales. Le tout se présente sous forme de questions qui permettent à l'Agence d'émettre un avis, dans le but de faire prendre conscience du danger encouru et de trouver un équilibre entre risques et coûts de sécurisation.

Les dix chapitres du guide d'hygiène informatique de l'Anssi



01 Sensibiliser et former. L'Agence nationale de la sécurité des systèmes d'information (Anssi) recommande de sensibiliser les utilisateurs aux bonnes pratiques en termes de sécurité informatique, mais aussi de former les équipes opérationnelles pour éviter les erreurs générant des failles. Maîtriser les risques de l'infogérance en se posant les bonnes questions en amont est également important.

02 Connaître le système d'information (SI). Protéger efficacement les données sensibles nécessite de les identifier. Cela permet ensuite de localiser les postes à risque. Il faut aussi disposer d'un inventaire complet des comptes bénéficiant de droits étendus, veiller aux départs, aux arrivées et aux changements de fonctions. Enfin, les équipements qui s'y connectent doivent être maîtrisés.

03 Authentifier et contrôler les accès. L'Anssi incite à prêter attention au rôle de chaque personne, à attribuer les bons droits sur les ressources sensibles. Concernant l'accès au SI, les mots de passe doivent être correctement dimensionnés et, si besoin, stockés dans un endroit sécurisé. Lorsque cela est possible, l'authentification la plus forte doit être privilégiée.

04 Sécuriser les postes. Cette mesure implique de mettre en place un niveau de sécurité minimal sur l'ensemble du parc informatique, de configurer un pare-feu avec précaution, de chiffrer les données sensibles transmises par internet, de proscrire l'utilisation de supports amovibles tels que les clés USB et d'homogénéiser les politiques de sécurité.

05 Sécuriser le réseau. Outre le fait de protéger l'accès physique aux serveurs et aux locaux techniques, l'Anssi recommande de veiller à segmenter et à cloisonner le réseau pour éviter que toutes les machines soient liées entre elles. Utiliser des protocoles réseaux sécurisés, protéger la messagerie professionnelle, font partie des autres conseils.

06 Sécuriser l'administration. La navigation sur internet comporte de nombreux risques. Il convient donc d'interdire l'accès au web depuis les postes ou serveurs utilisés pour l'administration du SI. L'utilisation d'un réseau dédié et cloisonné est encouragée. Par ailleurs, il faut limiter au strict besoin opérationnel les droits d'administration.

07 Gérer le nomadisme. Il faut prendre des mesures de sécurisation physique, mais aussi chiffrer les données sensibles en cas de perte du matériel nomade. S'assurer de la sécurisation de la connexion de l'appareil au réseau du SI est aussi crucial. Plus globalement, adopter des politiques de sécurité dédiées aux terminaux mobiles apparaît indispensable.

08 Maintenir le système d'information à jour. Les failles contenues dans les logiciels sont particulièrement dangereuses. Mais elles sont progressivement corrigées. Aussi, il est important de s'équiper des versions les plus récentes des différents outils pour minimiser les risques. Anticiper la fin de leur maintenance est également essentiel.

09 Superviser, auditer, réagir. L'Anssi préconise, si possible, de désigner un RSSI, mais aussi de procéder régulièrement à des contrôles et audits de sécurité. Il convient également de mettre en place une politique de sauvegarde des composants critiques. En cas d'incident, disposer d'une procédure de gestion s'avère essentiel pour éviter de commettre des erreurs.

10 Privilégier l'usage des produits et services qualifiés par l'Anssi. L'agence propose une liste de produits et de prestataires qualifiés par ses soins. Elle encourage l'utilisation de ces derniers pour toute entité, car elle estime qu'il s'agit du seul gage d'une étude sérieuse et approfondie du fonctionnement technique de la solution et de son écosystème.

«Un responsable de la sécurité des systèmes d'information (RSSI), on n'en trouve pas dans les villes petites ou moyennes. Ce sont des gens qui ont une stature, des réflexes, une vraie épaisseur en matière technique. La mutualisation nous permet d'obtenir des compétences que l'on peut se payer à plusieurs et que l'on peut partager pour faire de l'audit, des conseils, voire pour être proactif sur des problématiques de sécurité.» Du côté de l'Anssi, Guy Flament «invite toutes les collectivités à se tourner vers les syndicats informatiques qui ont un contact privilégié avec l'agence».

ANTICIPATION

Faire appel à des prestataires de confiance, considérer la sécurité comme un sujet important en cas d'appel d'offres sont des mesures de bon sens. Mais parfois, l'urgence rend la prise de décision plus compliquée. Depuis plusieurs mois, les collectivités sont victimes de «rançongiciels». La paralysie de leur système d'information peut s'avérer extrêmement dommageable. Pour éviter de se retrouver dans une situation critique, il faut anticiper le problème et veiller à ce que ses données soient sauvegardées dans plusieurs endroits différents. Et pas uniquement dans deux salles d'un même bâtiment, par exemple. Des plans de continuité ou de reprise d'activité permettent, dans les deux cas, le retour plus ou moins rapide à une activité normale.

Pour autant, aussi frustrant soit ce constat, il faut aussi prendre conscience du fait que l'intégralité des risques informatiques ne sera jamais couverte. «Le risque zéro en matière de cybersécurité n'existe pas, conclut Guy Flament. Ou alors à des niveaux de contrainte qui ne sont pas supportables par une collectivité territoriale. L'important, c'est d'éviter l'intégralité des attaques les plus fréquentes.»

«Cloud» et souveraineté : le débat fait rage

Une note ministérielle du 5 avril 2016 affirme l'obligation pour les collectivités d'avoir recours à un «cloud souverain». Mais l'offre répondant à cette injonction ne donne pas satisfaction à toutes les collectivités, qui se trouvent dans une position inconfortable.

Le «cloud» est une solution adoptée ou envisagée par un nombre important de collectivités. Elles voient dans ce système de stockage «dans le nuage», une solution adaptée à leurs besoins de modernisation. Le 5 avril 2016, une note informative émanant du ministère de l'Intérieur et du ministère de la Culture et de la communication est toutefois venue jeter le trouble.

Celle-ci explique que les collectivités doivent impérativement souscrire une offre de «cloud souverain». La démarche inverse est qualifiée «d'illégale, pour toute institution produisant des archives publiques» du fait de la nécessité de s'assurer que les données sont stockées et traitées sur le territoire national.

LES AMÉRICAINS DANS LE VISEUR

A l'évidence, la note, qui a été signée par le directeur général des collectivités locales, Bruno Delsol, et par le directeur chargé des archives de France, Hervé Lemoine, vise les offres provenant de sociétés américaines.

De Microsoft à Google, en passant par Amazon, les entreprises proposant leurs services sont nombreuses. Elles disposent en effet de moyens colossaux et ont investi depuis longtemps dans ce système de stockage. A ce jour, ces acteurs sont nettement en avance sur leurs concurrents français et se taillent la part du lion sur le marché international et hexagonal. Pour autant, adopter une solution émanant d'entreprises américaines comporte un risque. Et pas des moindres. Car ces dernières ont l'habitude de conserver des «backdoors», c'est-à-dire des portes dérobées dont les utilisateurs n'ont pas connaissance, qui leur permettent d'avoir un accès au logiciel. Or en vertu des lois en vigueur aux Etats-Unis, le gouvernement peut avoir accès aux données personnelles hébergées sur le sol américain ou détenues par une société américaine à tout moment, sans autorisation judiciaire. Ce qui pose un problème évident pour les collectivités.

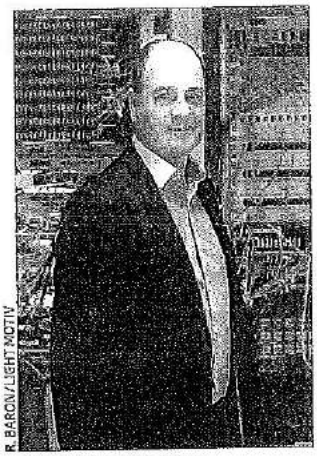
OFFRE ÉTRANGÈRE

Si la note informative du 5 avril 2016 donne des consignes assez fermes, elle n'est, pour autant, pas un texte de loi. Aussi, malgré les risques encourus, les collectivités peuvent encore se tourner vers une offre de «cloud» étrangère. D'autant que plusieurs sociétés américaines, à l'instar d'Amazon et de Microsoft, ont annoncé qu'elles allaient ouvrir des «data centers» en France. Leurs systèmes de stockage «en nuage» deviendront alors, de fait, souverains. Mais rien ne permet d'affirmer pour autant que les données détenues par ces entreprises ne tomberont jamais dans les mains de l'administration du pays dans lequel est établie leur maison mère (lire p.39).

Les collectivités territoriales qui abordent la question du «cloud» se doivent donc d'être conscientes des conséquences induites par le choix de leur prestataire. Certaines d'entre elles vont ainsi privilégier l'efficacité du service en veillant à ne pas stocker de données sensibles, tandis que d'autres vont choisir la solution la plus sécurisée... Cette question n'a, de toute évidence, pas fini de faire parler.●

Communauté urbaine de Dunkerque (Nord) 21 communes - 201 400 hab.

Une orientation vers une offre de Microsoft pour remplacer la messagerie actuelle



R. BARON/LIGHT MOTIV

RENÉ-YVES LABRANCHE, directeur des systèmes d'information

La cybersécurité fait partie des préoccupations principales de la communauté urbaine et de la ville de Dunkerque. Pour autant, en dépit de la note informative du 5 avril 2016, elle s'oriente vers une offre «cloud» de Microsoft pour remplacer sa messagerie actuelle sous Lotus notes. Un choix assumé par son directeur des systèmes d'information, René-Yves Labranche: «Une annonce de Microsoft nous a signalé que la société implanterait des "data centers" en France dès 2017. Et Office 365 semble être la solution adaptée à notre besoin, tout en respectant au maximum la sécurité», lance-t-il.
Avant d'expliquer en profondeur la démarche: «Il y a une antinomie entre la notion de "cloud souverain" et la nécessité de transformation et de modernisation des systèmes d'information dans les collectivités. Si on applique cette note à la lettre, on fait marche arrière sur la totalité de la transformation qu'on a déjà opérée et pour laquelle nous sommes en conformité avec le référentiel général de sécurité. Nous avons un RSSI et avons beaucoup investi en termes humains et financiers pour améliorer la sécurité de notre système d'information.»

ARNAUD TESSALONIKOS • PIERRE DEPREZ

«Google et Amazon ont annoncé la création de "data centers" en France»

Pour Arnaud Tessalonikos et Pierre Deprez, avocats en «propriété intellectuelle, technologies numériques et data» au sein du cabinet DS avocats, utiliser un «cloud souverain» est une nécessité, même s'il n'existe pas vraiment de cadre législatif établi.

Existe-t-il un cadre juridique particulier entourant l'utilisation du «cloud» par les collectivités?

A. T.: En tant que tel, non, pas véritablement. Il y a la note d'information du 5 avril 2016 relative à l'informatique «en nuage» qui s'apparente à une circulaire. Elle précise le cadre dans lequel la loi doit être comprise et interprétée, mais elle n'est pas un acte créateur de droit.

La première question qui se pose pour la collectivité territoriale est de savoir si elle a recours ou non à un opérateur de «cloud souverain». La réponse est évidemment oui! Est-ce que cela règle pour autant tous les problèmes? Pas forcément. Au-delà de l'endroit où se trouve l'opérateur de «cloud computing» [information «en nuage»] avec lequel je vais travailler, la question du niveau de sécurité sur lequel se situer pour formuler ses exigences se pose.

Est-ce qu'une filiale d'une société américaine possédant des serveurs en France peut rentrer dans ce cadre?

P. D.: Google et Amazon ont récemment annoncé la création et la construction de «data centers» en France. Si l'on suit la définition du «cloud souverain» telle qu'elle a été formulée dans la note d'information, à savoir que cette dernière parle d'entités de droit français et que ces «clouds» sont gérés par Google France ou Amazon France, qui seraient bien entendu des entités de droit français, ils seraient a priori souverains. Mais le problème qui est inhérent à toute société américaine s'appliquerait malgré tout. C'est-à-dire que les autorités américaines auront la possibilité, en vertu de l'ensemble de leurs lois de sécurité intérieure et de contre-espionnage, d'avoir accès aux données hébergées dans les serveurs en France, mais possédés par des sociétés dont la maison mère est américaine. Il y a donc un risque.

A. T.

> *«Les collectivités doivent avoir recours à un opérateur de "cloud souverain".»*
> Arnaud Tessalonikos, avocat

Quels conseils donneriez-vous dans ce cas?

A. T.: Il faut se poser la question au cas par cas. Il faut définir comment on fonctionne, quand déclencher une archive, avec qui on travaille, à quel moment on va renégocier ses contrats informatiques...

Cela peut être l'occasion, in concreto, de réviser ses plans, de voir comment se conformer à cette nouvelle règle, quelle incidence cela aura sur l'organisation et comment faire progresser, dans un principe d'amélioration continue, la qualité de ses systèmes d'information. Parce que cela va devenir l'élément le plus stratégique de toute activité humaine.●

À CONSULTER

Les référents de l'Anssi en région

Depuis la fin de l'année 2015, l'Anssi a commencé à mettre en place des agents relais au niveau local dans les treize régions métropolitaines. Ce document compile les noms et emails des différents experts. Attention, certaines régions ne sont pas encore couvertes; elles le seront dans le courant du premier semestre 2017.

http://goo.gl/TJ8jwg

SUR LE WEB

Le guide d'hygiène informatique de l'Anssi

L'Anssi a publié sur son site, le 23 janvier, un guide d'hygiène informatique qui s'adresse à toutes les organisations, dont les collectivités. Il contient 42 mesures distinctes réparties dans dix chapitres. Elles sont «la transcription dans le monde numérique de règles élémentaires de sécurité sanitaire».

http://goo.gl/7j8TPJ

Règlement européen sur la protection des données: ce qui change pour les professionnels

Le nouveau règlement européen sur la protection des données personnelles entrera en application en 2018. Les collectivités territoriales sont évidemment directement concernées par son contenu. Pour se préparer au mieux à ces exigences, la Cnil propose un article résumant les principaux changements en quelques points.

http://goo.gl/btG8gT

la Gazette.fr

Pour aller plus loin

Former et sensibiliser les agents à la sécurité informatique pour réduire les risques
www.lagazette.fr/461392

Sécurité informatique: les petites communes à la traîne
www.lagazette.fr/446735

la gazette.fr

Adresse de l'article http://www.lagazettedescommunes.com/507657/donnees-personnelles-les-collectivites-vont-devoir-se-lancer-dans-une-demarche-de-mise-en-conformite/

NUMÉRIQUE

Données personnelles : « les collectivités vont devoir se lancer dans une démarche de mise en conformité »

Gabriel Zignani | Actu juridique | France | Publié le 24/05/2017 | Mis à jour le 27/06/2017

A un an de l'entrée en vigueur du règlement européen sur la protection des données, Alice de La Mure, juriste au service Correspondants informatiques et libertés de la CNIL, revient sur les nouvelles obligations qui concernent largement les collectivités territoriales.

CNIL
Commission Nationale de l'Informatique et des Libertés

Le règlement général sur la protection des données (RGPD), adopté par le Parlement européen le 14 avril 2016, sera directement applicable dans les Etats membres le 25 mai 2018. Il sera alors le texte de référence concernant la protection des données à caractère personnel. Il consolide, voire renforce, les grands principes de la loi Informatique et Libertés [1].

Divers axes s'en dégagent, dont plusieurs concernent directement les collectivités territoriales :

- la responsabilisation globale de l'ensemble des acteurs ;
- le renforcement des droits des personnes, avec notamment l'avènement du droit à la portabilité et du droit à la limitation du traitement ;
- l'augmentation du montant des sanctions susceptibles d'être prononcées par la CNIL : la loi du 7 octobre 2016 pour une République numérique [2] avait fait passer ces sanctions maximales à 3 millions d'euros d'amende. Avec le règlement, le nouveau plafond est de 20 millions d'euros. Le non-respect des dispositions relatives aux délégués est bien évidement passible de sanctions.

Ce texte européen s'appliquera à tous les organismes, publics ou privés, traitant des données à caractère personnel. A un an de l'entrée en application de ce règlement européen, Alice de La Mure, juriste au service Correspondants informatiques et libertés de la CNIL, revient sur le contenu du texte.

- La Cnil insiste sur l'urgence d'une nouvelle loi Informatique et Libertés [3]
- Protection des données : le législateur appelé à intervenir rapidement [4]

Le règlement européen s'appliquera à compter du 25 mai 2018. Pour quels changements par rapport au cadre juridique actuel ?

Le règlement général sur la protection des données (RGPD) amène un véritable changement de paradigme. On passe d'une logique de contrôle a priori, avec des démarches administratives extrêmement lourdes pour l'ensemble des organismes gérant des données à caractère personnel, à une logique de contrôle a posteriori, d'autocontrôle dynamique et permanent par les organismes, sous le regard et avec l'accompagnement de la CNIL.

En vertu de cette logique de responsabilisation des acteurs, les organismes concernés – dont les collectivités territoriales – vont devoir s'inscrire dans une posture de mise en conformité dynamique aux règles d'or de la protection des données. La question ne sera plus tant de savoir s'il faut remplir telle ou telle formalité, mais davantage de savoir si l'organisme assure en permanence une protection optimale aux données personnelles qu'il traite.

Cette logique de contrôle a posteriori impose toutefois aux organismes d'internaliser la compétence. C'est pour cela que le règlement établit l'obligation d'instituer un délégué à la protection des données (DPO) dans tous les organismes publics qui gèrent des données à caractère personnel. Chaque collectivité devra donc être pourvue d'un tel délégué. Celui-ci incarne cette logique de responsabilisation, d'autocontrôle interne.

Les collectivités doivent percevoir cette nouvelle réglementation comme une avancée, non comme une contrainte. La conformité au cadre de la protection des données personnelles permet par exemple de créer de la confiance, et donc de favoriser l'innovation.

- Données à caractère personnel : « Les citoyens demandent des règles claires et précises » [5]

Le délégué est l'une des pièces maîtresses de ce nouveau paradigme ?

Dans ce nouvel écosystème juridique de responsabilisation des acteurs, les organismes concernés vont devoir recourir à divers outils de conformité.

Le délégué à la protection des données est l'un d'entre eux, et il est essentiel. Ce délégué est le successeur du correspondant informatique et libertés (CIL) actuel.

Quelles sont les différences entre le DPD et le CIL ? Quel rôle pour le délégué à la protection des données ?

Entre le délégué à la protection des données et son prédécesseur, il y a un changement d'échelle, mais pas de nature. Le délégué, c'est un super CIL, un CIL 2.0.

Au niveau du statut comme des missions, ces deux entités sont similaires :

- ils exercent leurs missions auprès du responsable de traitement ;
- ils doivent être à l'abri des conflits d'intérêts ;
- leur rôle est de veiller à la bonne application et à la bonne prise en compte des règles d'or de la protection des données.

Mais il y a un véritable changement d'échelle. Le RGPD renforce le niveau d'expertise requis : on passe d'une fonction à un métier. Le RGPD indique expressément que le délégué est désigné sur la base de ses qualités professionnelles, et en particulier de ses connaissances spécialisées du droit et des pratiques en matière de protection des données. En outre, le RGPD précise et renforce les moyens dont dispose le délégué.

Quels seront ses moyens d'action ?

Le règlement européen indique expressément que l'organisme devra aider le délégué à exercer ses missions en lui fournissant toutes les ressources nécessaires, en lui donnant un accès à l'ensemble des données traitées et à l'ensemble des opérations de traitement, et en lui permettant d'entretenir ses connaissances spécialisées (grâce à la formation continue).

Il est également prévu que le délégué puisse mener des audits. Il doit aussi sensibiliser l'ensemble de ses collaborateurs sur les obligations en matière de protection des données, avec un objectif de diffusion d'une culture informatique et libertés. Enfin, il a un rôle de contrôle et coopère avec l'autorité de contrôle (la CNIL), auprès de laquelle il joue le rôle d'interlocuteur privilégié.

Le délégué est donc le chef d'orchestre de la conformité de demain. Il a un rôle de pilote de la conformité. Il est l'interface entre l'organisme et les personnes concernées.

- Bilan 2016 de la Cnil : ce qui intéresse les collectivités territoriales [6]

Il faut également noter que le RGPD prévoit la possibilité de mutualiser cette fonction. Dans le cadre normatif actuel, cette possibilité existe déjà. Et certains syndicats mixtes, spécialisés dans l'e-administration, proposent ainsi une prestation de CIL mutualisé aux communes qui en sont membres.

Quatre centres de gestion de la fonction publique territoriale proposent un service de CIL mutualisé. De même, il arrive que la même personne occupe la fonction de CIL pour une métropole et sa ville centre, ce qui est par exemple le cas à Nantes.

Que peuvent faire les collectivités afin d'être prêtes le 25 mai 2018 ?

La CNIL travaille et accompagne les collectivités dans ce sens. Différents outils sont disponibles sur le site www.cnil.fr [7] pour aider les collectivités à se préparer. Le RGPD y est décrypté et des fiches pratiques sont disponibles :

- Règlement européen : se préparer en 6 étapes [8]
- Règlement européen : questions-réponses [9]
- Devenir délégué à la protection des données [10]

De plus, des courriers seront prochainement envoyés à toutes les collectivités territoriales, afin de les sensibiliser sur le sujet.

Une démarche intéressante est en cours dans région Aquitaine : tous les départements ont mutualisé leurs démarches de mise en conformité. Ils ont désigné un département pilote et ont mis en place un plan d'action pour que tous les départements de la région soient prêts le 25 mai 2018. Les collectivités peuvent ainsi se préparer de manière collective et se répartir les tâches.

- Un label de gouvernance des données pour rassurer les usagers et les agents [11]

REFERENCES

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

POUR ALLER PLUS LOIN

- L'indispensable anonymisation des données personnelles des passants
- Campagne électorale : quelles règles pour l'utilisation des données privées ?

Pour cette séquence, les textes suivants ont été sélectionnés :

- « Sécurité informatique : comment se protéger ? », dossier extrait de « la Gazette » du 13 février 2017 ;

- « Données personnelles : les collectivités vont devoir se lancer dans une démarche de mise en conformité » », article issu du site internet de « la Gazette ».

Exercice 1 (5 points)

Vous êtes directeur du service en charge des systèmes informatiques de l'intercommunalité de Smartcity, 260 000 habitants. Celle-ci est composée d'une ville centre de 120 000 habitants et 15 autres communes membres de l'EPCI. Votre collectivité, ainsi que la ville centre et plusieurs autres communes s'interrogent sur leurs obligations en matière de sécurité informatique et les modalités de mise en œuvre d'une démarche de cybersécurité partagée.

À partir des documents proposés ci-dessus et de vos connaissances opérationnelles, proposez le plan de ce rapport avec propositions, **sans en rédiger le contenu, en attribuant à chaque partie et sous-partie un titre évocateur.**

Exercice 2 (4 points)

Rédiger l'introduction de ce rapport avec propositions à l'appui des informations contenues dans le mini-dossier et du plan déjà élaboré.

Exercice 3 (5 points)

Rédiger au choix l'une des sous-parties **relatives aux propositions opérationnelles**, en vous basant sur les différents documents proposés et vos connaissances personnelles.

SEQUENCE 3 : CULTURE GENERALE ET TERRITORIALE (14 points)

Exercice 1 (3 points)

Quels sont les avantages et les limites du télétravail dans la fonction publique territoriale ? Après avoir introduit cette notion, vous développerez successivement deux paragraphes permettant d'argumenter les deux facettes du sujet.

Exercice 2 (3 points)

Qu'est-ce qu'une collectivité territoriale ? Après en avoir donné une définition, vous rappellerez au moins une compétence de chaque niveau de collectivité territoriale.

OU

Quelles sont les étapes de la procédure budgétaire dans une collectivité territoriale ? Vous rappellerez successivement celles-ci et en soulèverez les principaux enjeux.

Exercice 3 (4 points)

Définissez les notions suivantes, en deux phrases maximum pour chacune d'entre elles :

- Le sourcing
- L'agenda d'accessibilité programmée
- La hiérarchie des normes
- PPCR

OU

Définissez les notions suivantes, en deux phrases maximum pour chacune d'entre elles :

- Le service civique
- RIFSEEP
- CHSCT
- Le détachement

Exercice 4 (4 points)

Dans quelle mesure les outils numériques changent-ils nos manières de communiquer et de travailler ?

Vous répondrez à cette question en prenant soin de proposer un raisonnement argumenté explorant différentes facettes du sujet et en vous appuyant sur vos connaissances personnelles.
