Repères

LES FRANÇAIS VEULENT ÊTRE RASSURÉS

- En 2016, 62 % des Français ont réalisé une démarche administrative dématérialisée – soit une augmentation de 24 % en quatre ans – mais seulement 40 % disent avoir confiance dans le numérique.
- 75 % des Français ont foi dans les sites de médias traditionnels, contre 64 % dans les moteurs de recherche, 64 % dans les blogs d'experts ou de journalistes, 63 % dans les portails d'information et 25 % dans les réseaux sociaux.
- 74 % des Français sont favorables à la numérisation des documents administratifs.
- 52 % seulement des Français ont confiance dans le paiement par empreinte digitale.
- 80 % des Français déplorent l'utilisation commerciale des données personnelles *via* les réseaux sociaux.
- 77 % des Français estiment qu'il est risqué d'enregistrer ses données bancaires en ligne.
- 67 % des Français n'ont pas confiance dans les réseaux sociaux pour garantir la protection des données personnelles.
- 65 % des Français se méfient des applications agrégeant les données de comptes bancaires.
- 62 % des Français sont inquiets du stockage sur Internet des données collectées.
- Les principales craintes des Français sont le piratage de leurs données, l'usurpation de leur identité et la consultation de leurs données par quelqu'un d'autre.

Selon une étude réalisée par Harris Interactive pour ACSEL (Association transversale pour professionnels), La Poste, Orange et la Caisse des dépôts, rendue publique le 18 décembre 2017.

UN GARDE-FOU POUR L'E-ADMINISTRATION

Le nouveau règlement européen sur la protection des données personnelles (RGPD) sera applicable à compter du 25 mai prochain. Sous peine de sanctions, les collectivités devront avoir pris toutes les mesures nécessaires, à commencer par la nomination d'un délégué (DPO : Data Protection Officer) chargé de vérifier la bonne application du nouveau texte et de faire remonter les manquements constatés. L'Union européenne avait déjà imposé cet objectif à travers la directive n° 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Aujourd'hui, la grande nouveauté est qu'elle se dote d'un texte qui servira de référence à tous les pays membres, notamment pour l'e-administration.

Un maire de montagne face à la nouvelle réglementation

« Faire les choses de manière pertinente et avec bon sens »

TANAONTE/STOCK.ADOBE.COM

D'après une enquête d'opinion pour la *Gazette des communes* du 10 juillet 2017, seulement 10 % des agents territoriaux estimaient que leur collectivité sera en conformité le 25 mai prochain avec le nouveau règlement européen destiné à mieux protéger les données à caractère personnel. Maire de Moûtiers (Savoie) depuis avril 2014, Fabrice Pannekoucke explique comment sa commune se prépare à appliquer le nouveau texte.

PLM : Comment avez-vous perçu la nouvelle réglementation européenne sur la protection des données personnelles (RGPD) ?

Fabrice Pannekoucke : Cela reste diffus. Dans les collectivités, on en a encore assez peu parlé. Pour l'instant, j'ai envie de dire qu'il y a une sorte de paradoxe. D'une part, nous sommes dans un système où, finalement, nous voulons être toujours plus connectés et bénéficier du partage d'informations. De l'autre, et dans le même temps, nous souhaitons toujours davantage de sécurité sur les données, ce qui est d'ailleurs très humain. Les élus des collectivités ne découvrent pas le problème. La protection des données, nous l'avons initiée depuis plusieurs années. Aujourd'hui, il nous faut la renforcer. Passer à l'étape suivante consiste d'abord à désigner un référent, ce fameux délégué à la protection des données à caractère personnel, le DPO[1].

PLM : Qu'en attendez-vous précisément ?

F.P. : La nouvelle réglementation nous oblige à avoir ce réflexe permanent de protéger les données personnelles. Pour cela, je compte sur le DPO en termes de conseils et de suivi. Ce référent sera une sorte de juge de paix qui nous rappellera à l'ordre si, d'aventure, nous nous éloignions un peu de la règle. Il pourra aussi labelliser tout nouveau dispositif de recueil d'informations. Et nous en mettons en place chaque année… Il aura donc clairement et systématiquement un regard sur tout ce qui touche au numérique, une mission très transversale de la collectivité.

PLM : Pouvez-vous nous donner un exemple concret de ce que ce référent peut changer dans l'administration de votre commune ?

F.P. : À Moûtiers, le référent n'est pas encore désigné mais j'ai une idée de ses compétences. C'est quelqu'un qui suit les questions numériques de la com-mune et qui sera associé à chaque étape de l'évolution de nos outils, à chaque fois que l'on mettra en place de nouveaux formulaires ou de nouvelles manières de collecter les données. Un exemple : nous réfléchissons actuellement à la mise en place d'une carte du territoire. Ce support, à la fois physique et numérique, permettra à l'usager d'être identifié et reconnu sur la totalité de notre secteur : la cantine, la garderie, l'école de musique, etc.

DR

Fabrice Pannekoucke :
« Le numérique peut être une contribution formidable mais il peut aussi être une arme dangereuse s'il est mal utilisé. »

PLM : À l'autre bout de la chaîne, qu'apporte cette carte du territoire à votre commune ?

F.P. : Grâce à cet outil, les habitants de Moûtiers pourront se réapproprier leur espace de vie mais il sera également une véritable force de frappe pour la commune qui, du coup, disposera d'innombrables données permettant d'informer les usagers dans toutes sortes de cas. Ainsi, dans l'hypothèse d'un plan communal de sauvegarde, nous aurons toutes les informations. Et, en cas de besoin d'hébergement d'urgence dans nos communes, cette carte permettra de demander à de nombreux administrés s'ils peuvent nous aider. Si nous mettons en place cette carte du territoire, le référent y sera naturellement associé car il aura cette culture du numérique et il pourra faire en sorte que nous prenions les bonnes précautions. Il ne faut, en effet, jamais oublier que le numérique peut être une contribution formidable mais qu'il peut aussi être une arme dangereuse s'il est mal utilisé.

PLM : De nombreuses communes pourraient faire appel à des délégués communs à la protection des données, qu'en pensez-vous ?

F.P. : Toute politique publique peut être partagée mais chaque situation est spécifique. C'est donc une question de pertinence. Dans notre communauté de communes, Moûtiers et Saint-Martin-de-Belleville sont particulièrement concernées par la protection des données personnelles car elles ont beaucoup de services et d'activités. Leurs dispositifs serviront d'éclaireurs aux autres communes. Ensuite, au regard des premières leçons que nous tirerons, celles-ci pourront peut-être mutualiser.

PLM : Moûtiers sera-t-elle prête le 25 mai prochain ?

F.P. : Je le répète : nous ne partons pas de rien et nous ferons en sorte d'être prêts. Nommer le référent, ce sera fait. Adapter quelques dispositifs de prudence, également. Après, est-ce que toutes les cases seront cochées ? À ce jour, je suis incapable de le dire parce que nous ne savons pas encore quelle sera la déclinaison française du texte *in fine*.

PLM : Quels conseils donneriez-vous à vos collègues maires qui sont peut-être un peu moins bien préparés que vous ?

F.P. : Le maître mot, l'objectif, reste les services que nous devons apporter à nos administrés. Alors, je conseille simplement de faire les choses de manière pertinente et avec bon sens.

(1) Le DPO (Data Protection Officer) sera le nouveau délégué chargé de la protection des données numériques.

L'avis d'un juriste

« Cette sécurisation est vraiment indispensable »

Avocat titulaire d'un DEA en droit public et d'un DESS en administration publique, Yann Landot est spécialiste des problématiques liées à l'intercommunalité, au droit des services publics locaux et au droit de l'environnement. Il explique aux communes que la nouvelle réglementation européenne est une belle occasion de se poser les bonnes questions et de mettre en place les bonnes procédures.

PLM : Cette nouvelle règle européenne de protection des données personnelles était-elle réellement indispensable ?

Yann Landot : Si on tire les conséquences de toutes les dérives apparues ces dernières années, on ne peut répondre que par l'affirmative. Par conséquent, plutôt que de vivre la nouvelle réglementation comme une contrainte, il vaudrait mieux la prendre comme une opportunité. L'utilisation de plus en plus fréquente des smartphones, des ordinateurs, des tablettes, des boîtes mails et des moteurs de recherche oblige, en effet, à se poser cette question essentielle : toutes les informations rentrées sont-elles bien protégées ? À l'évidence, ce n'est pas le cas. Les données peuvent fuiter et la cybercriminalité est toujours plus performante. En outre, si l'on recherche quelque chose sur Internet avec un mot-clé, cela ressort ensuite pratiquement à chaque fois que vous ouvrez votre ordinateur. C'est déjà du traitement de données…

PLM : En quoi les collectivités sont-elles concernées ?

Y.L. : Les collectivités hébergent aussi des données sur le cloud. C'est très commode pour pouvoir travailler depuis n'importe où mais cela crée des dangers en termes de sécurité et, en définitive, les risques sont énormes. Pour les collectivités, il est encore plus indispensable de mieux sécuriser les données personnelles, d'autant que la plupart des élus et des agents n'ont pas la culture du numérique et de la mise à jour. Cette nouvelle réglementation est précisément l'occasion de sortir le nez du guidon, de se poser les bonnes questions et de mettre en place les bonnes procédures.

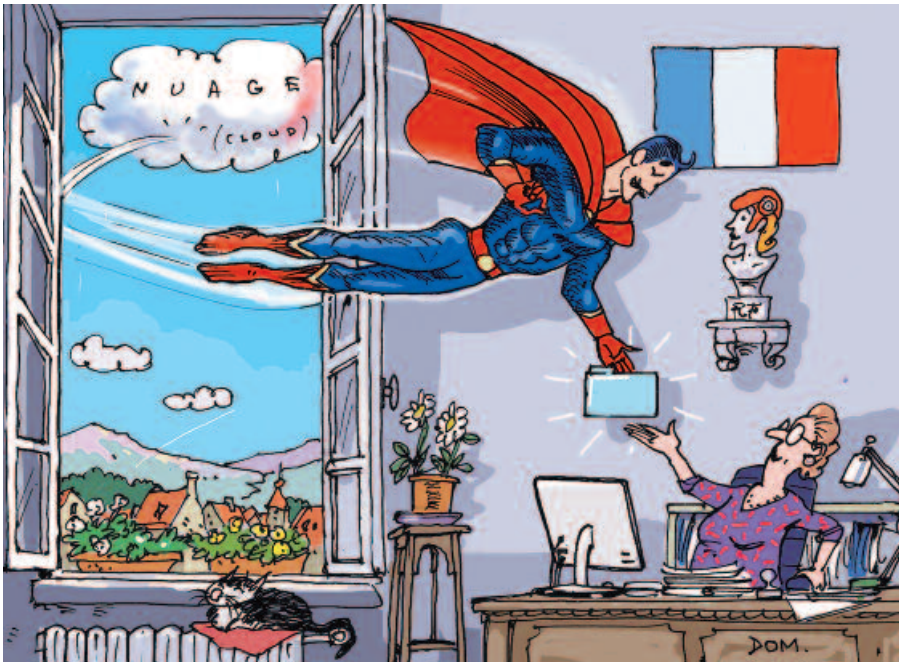
PLM : Que risque-t-il de se passer pour les collectivités qui ne seront pas en conformité le 25 mai prochain ?

Y.L. : En théorie, elles pourraient faire l'objet de sanctions mais je pense qu'il y aura une période de tolérance. J'imagine que, jusqu'à la fin de l'année 2018, on leur laissera le temps de se mettre en conformité avec ce nouveau règlement européen. D'autant que, pour le moment, aucune commune n'est vraiment prête et il y a gros à parier que ce sera encore le cas le 25 mai prochain. À la limite, les territoires qui seront à jour le 25 mai seront soit très forts, soit ils auront bâclé le travail. Dans ces conditions, je conseille déjà aux élus de désigner leur fameux DPO et de lancer leur procédure afin de démontrer que leurs communes ont engagé le mouvement. En commençant, par exemple, par l'actualisation des documents-types de la collectivité. La mutualisation des moyens avec d'autres communes peut aussi être envisagée et engagée. Et puis soyons pragmatiques : à l'impossible, nul n'est tenu. En conclusion, il ne faut pas s'affoler mais ne pas non plus repousser au lendemain ces mises à jour et ces mises à niveau, sinon il y aura clairement un risque de mise en cause de la responsabilité des collectivités.

YB/STOCK.ADOBE.COM

Yann Landot :
« Pour les collectivités, il est encore plus indispensable de mieux sécuriser les données personnelles. Cette nouvelle réglementation est l'occasion de se poser les bonnes questions et de mettre en place les bonnes procédures. »

La CNIL veillera à la protection optimale des données traitées



À compter du 25 mai, le correspondant informatique et libertés (CIL) sera remplacé par le délégué à la protection des données (DPO). Celui-ci exercera ses missions sous le contrôle de la Commission nationale informatique et libertés (CNIL).

Les missions du DPO sont principalement d'informer et de conseiller la collectivité, notamment le responsable du traitement des données ou le sous-traitant. Ce délégué veillera également au respect de la réglementation, il conseillera la collectivité sur la réalisation d'une analyse d'impact relative à la protection des données et vérifiera son exécution. Il servira d'interface avec la CNIL.
Celle-ci prévient que, « dans l'exercice de ces missions, le délégué devra être à l'abri des conflits d'intérêts, rendre compte directement au niveau le plus élevé de la hiérarchie et bénéficier d'une liberté certaine dans les actions qu'il décidera d'entreprendre. »
« Les collectivités seront appelées à tenir un

La Poste et la transformation de l'action publique territoriale

125 collectivités de toutes les tailles, représentatives de la diversité des territoires, se sont engagées avec La Poste dans une démarche inédite de coconstruction d'une plateforme omnicanal de services pour les citoyens, se félicite le président du Groupe La Poste, Philippe Wahl, dans un Livre blanc.

Simplifier la vie des citoyens et contribuer à la transformation de l'action publique territoriale, DOCAPOST – Solutions publiques se veut une réponse aux enjeux du XXIe siècle. Son but est de « permettre aux collectivités territoriales d'inventer et de proposer les nouveaux services numériques utiles à leurs administrations et aux citoyens. » Que l'on soit une collectivité ou un acteur historique au service de l'intérêt général comme La Poste, la révolution digitale incite en définitive à s'interroger en premier lieu sur soi et sur les rapports que l'on entretient avec les usagers, peut-on lire en introduction du Livre blanc.
« Si la distinction entre la sécurité des données et la sécurité des systèmes d'information pouvait se résumer à un principe, ce serait celui-ci : ce n'est pas parce qu'une exploitation des données est sans danger pour soi qu'elle l'est aussi pour toutes les parties prenantes », relève Thierry Deniau, directeur de la direction de l'ingénierie et des systèmes d'information et des télécommunications (DISIT) du Groupe La Poste.
Le nouveau règlement européen sur la sécurité des données (RGPD) institue ainsi un principe de responsabilité inédit, ajoute-t-il. Celui qui effectue le traitement des données doit aussi être garant des droits de celui qui en est le propriétaire. Et cette contrainte doit être intégrée non seulement dès la conception de services nouveaux, mais aussi à l'ensemble des services existants.

« Pour La Poste, la gouvernance des données doit être envisagée comme une activité stratégique. »

« En matière de sécurité, il est évident que le risque zéro n'existe pas. En revanche, les collectivités peuvent développer de bonnes pratiques de résilience en s'appuyant sur des spécialistes de la sécurité », observe Thierry Deniau. Il s'agit pour elles de se préparer aux attaques de la même manière qu'elles préviennent les risques d'atteinte à la sécurité des personnes dans leurs locaux. La question à se poser n'est pas « ai-je pensé à


BAZ STUDIO/STOCK.ADOBE.COM

registre de leurs activités de traitement, à encadrer les opérations sous-traitées dans les contrats de prestation de services, à formaliser des politiques de confidentialité des données et des procédures relatives à la gestion des demandes d'exercice des droits, à adhérer à des codes de conduite ou encore à certifier des traitements. Dans certains cas, pour les traitements à risques, elles devront effectuer des analyses d'impact sur la vie privée et notifier à la CNIL, voire aux personnes concernées, les violations de données personnelles », précise encore la CNIL qui peut décider de sanctions administratives en cas de manquement.

Toutes les collectivités ne sont pas sur un pied d'égalité pour faire évoluer les pratiques. La CNIL leur recommande la mutualisation du délégué à la protection des données comme une solution pour les plus petites d'entre elles ou celles en grande difficulté financière. « Cela permet de limiter les coûts tout en bénéficiant de professionnels disposant des compétences et de la disponibilité nécessaires à un bon pilotage. »

tout ? », mais comment réagir efficacement en cas de problème. Cette réaction repose sur une connaissance exhaustive des circuits empruntés normalement par les données personnelles dans les systèmes d'information et sur l'état de sécurité des systèmes impliqués. « En matière de sécurité des données, il ne s'agit pas de courir plus vite que le tigre mais plus vite que son voisin. »

Pour le Livre blanc de La Poste, la gouvernance des données doit être envisagée comme une activité stratégique. Il s'agit de définir et de contrôler l'application de leurs règles d'utilisation, mais également la capacité d'intelligence qui peut découler de leur analyse et de leur agrégation. « C'est cette information signifiante qui recèle le plus fort potentiel de valeur ajoutée pour la collectivité et l'expose le plus au risque d'image en cas de violation ou de détournement d'usage. »

Au final, la véritable urgence consisterait à rompre ce cercle vicieux : plus les collectivités se concentrent sur les risques et les difficultés de la transformation numérique, plus elles hésitent à s'appuyer sur les compétences extérieures qui leur permettraient d'en saisir les opportunités à moindre coût, regrette La Poste. Au demeurant, celle-ci propose également des solutions qui intègrent les obligations liées au SVE et au SVA (lire ci-contre).

Les modalités de la saisine par voie électronique

Depuis le 7 novembre 2016, les collectivités territoriales sont tenues d'offrir aux usagers les moyens de les saisir par voie électronique (SVE), et doivent s'organiser pour traiter leurs demandes dans des délais réduits (SVA).

Moins de deux semaines avant l'extension aux collectivités territoriales du droit des usagers à saisir l'administration par voie électronique (SVE), un décret en a précisé les termes. Il les place dans l'obligation d'informer le public des téléservices qu'elles mettent en place afin que l'usager puisse exercer son droit de saisir l'administration. L'accusé de réception électronique devra comporter la date de réception de l'envoi électronique, le nom du service chargé du dossier, son adresse électronique ou postale et son numéro de téléphone.

Le silence gardé pendant plus de deux mois sur une demande ou une démarche d'un administré vaudra accord (SVA), à moins que des circonstances particulières soient retenues.

Dans ce cadre, l'accusé de réception du SVE devra aussi indiquer si la demande est susceptible d'être acceptée ou rejetée, ainsi que la date à laquelle celle-ci sera réputée acceptée ou rejetée à défaut d'une décision expresse et sous réserve que la demande soit complète. Dans le premier cas, l'accusé de réception mentionnera la possibilité offerte au demandeur de recevoir l'attestation prévue à l'article L. 232-3 du Code des relations entre le public et l'administration (CRPA). Dans le second cas, il mentionnera les délais et les voies de recours à l'encontre de la décision.

Les collectivités qui ne prennent pas de dispositions particulières en matière de dématérialisation des échanges sont tenues d'accepter n'importe quel canal électronique utilisé par l'usager (e-mail, Facebook, Twitter, etc.).