”La protection de données à caractère personnel : quels risques pour les collectivités territoriales ?”, JCP A - La Semaine juridique Administrations et Collectivités territoriales, LexisNexis, 2018, n° 42, 22 octobre, 2287

Jennifer Marchand

La protection de données à caractère personnel : quels risques pour les collectivités territoriales ?

JCP A n°42, 22 octobre 2018. 2287

Jennifer Marchand maître de conférences en droit public, université Clermont Auvergne - Centre Michel de l'Hospital, EA 4232

Les données à caractère personnel, moteur de nombreux services publics locaux. - La donnée à caractère personnel se définit comme toute information se rapportant à une personne physique identifiée ou identifiable notamment par référence à un nom, un numéro d'identification, une adresse IP ou par des éléments propres à son identité physique, physiologique, génétique, économique, culturelle ou sociale. Les collectivités territoriales traitent chaque jour de nombreuses données à caractère personnel tant dans le cadre de leur gestion interne (ressources humaines, contrôle d'accès par biométrie, géolocalisation des agents) que de la gestion des services publics (état civil, cadastre, aménagement, dispositifs de vidéo-protection). Les projets de *smart cities*[1] ou la problématique de l'*open data*[2] démontrent également l'intérêt des collectivités pour un accès et une utilisation accrue de données et notamment de données à caractère personnel. Le régime de protection des données à caractère personnel découle de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles pour assurer la mise en conformité du droit national avec le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (RGPD)[3].

La responsabilisation des collectivités territoriales en matière de protection des données à caractère personnel[4] -. Le RGPD met fin à la plupart des formalités préalables obligatoires auprès de la CNIL. En contrepartie, la responsabilité des collectivités territoriales est renforcée

[1] CNIL, Smart cities et données personnelles : quels enjeux de politiques publiques et de vie privée ?, 2017. – Ph. Mouron, La protection des données personnelles dans l'environnement urbain : RLDI 2017, n° 139.

[2] D. Da Palma, La mise en conformité du traitement des données personnelles dans l'Open Data au regard du RGPD. Quels enjeux pour les collectivités territoriales ?, JCP A 2017, 2213.

[3] Pour assurer la mise en conformité avec le RGPD, le choix a été fait de ne pas abroger la loi du 6 janvier 1978 mais de l'adapter. La date d'entrée en vigueur de la loi n° 2018-493 relative à la protection des données personnelles est rétroactive au 25 mai 2018 (date d'entrée en vigueur du RGDP dans l'ensemble de l'Union européenne).

[4] Le décret n° 2018-687 du 6 août 2018 contient diverses mesures d'application de la loi n° 2018-493 du 20 juin 2018 qui intéressent le secteur public.

au profit d'un principe d'*accountability*. Les collectivités sont désormais les garantes des données à caractère personnel qu'elles traitent. Pour ce faire, le RGPD consacre un nouveau mode de régulation proche des mécanismes de compliance. Il oblige les collectivités à internaliser les règles qu'il édicte et à mettre en œuvre les mesures techniques et organisationnelles appropriées afin d'être en mesure de démontrer que le traitement est effectué conformément au règlement.

Le RGPD et l'approche par les risques. Le RGPD consacre une approche basée sur le risque *privacy*. Il permet une gradation des mesures en fonction tant des risques pour les droits et libertés des personnes concernées que de la taille de la collectivité et de la nature des traitements. Une telle approche s'inscrit dans un processus itératif d'amélioration continue de la sécurité et de la protection des données à caractère personnel dès la conception et par défaut. De manière proactive, en tant que responsable de traitement, la collectivité représentée par son maire ou président devra évaluer les risques que comportent les traitements de données et concevoir les outils visant à prévenir la réalisation de ces risques (*privacy by design*). Les moyens mis en œuvre devront garantir que seules les données à caractère personnel nécessaires à la finalité du traitement seront traitées (*privacy by default*).

Après avoir exposé les nouvelles obligations incombant aux collectivités territoriales en matière de protection des données à caractère personnel (**1**), il conviendra de dresser un panorama des risques encourus par les collectivités territoriales (**2**).

1. Les nouvelles obligations incombant aux collectivités territoriales en matière de protection des données à caractère personnel

L'application du RGPD entraîne un changement de paradigme qui requiert des collectivités de prouver qu'elles sont en conformité avec le règlement avant (**A**) et pendant toute la durée de mise en œuvre des traitements de données à caractère personnel (**B**).

A. - Les obligations de conformité ex ante des collectivités territoriales en matière de protection des données à caractère personnel

1° **La désignation obligatoire d'un délégué à la protection des données**

Du CIL au DPD[5]. La désignation d'un délégué à la protection des données (DPD) est obligatoire lorsque le traitement est effectué par une autorité publique ou un organisme public. Le délégué remplace le Correspondant informatique et libertés (CIL) dont la désignation était jusqu'alors facultative. Le choix du DPD doit se faire en fonction de son expertise juridique et sa connaissance approfondie du RGPD. Il doit permettre à la collectivité de maîtriser les risques de non-conformité au règlement. Pilote de la conformité interne, le DPD doit disposer d'une autonomie et de ressources suffisantes pour s'acquitter efficacement de ses missions qu'il exerce en toute indépendance. Associé dès le stade le plus précoce aux questions relatives à la protection des données, il devra bénéficier d'un positionnement stratégique au sein de la structure en étant rattaché à la direction générale des services. Son rôle est de contrôler le respect du RGPD, de conseiller le responsable de traitement et de coopérer avec l'autorité de contrôle. La fonction de DPD peut être externalisée sur la base d'un contrat de service ou être mutualisée entre EPCI et communes membres compte tenu de leur taille et structure organisationnelle. En cas de violation du règlement, le DPD n'est pas pénalement responsable. En désignant un délégué, le responsable de traitement n'échappe à aucune de ses responsabilités.

2° **Cartographie et analyse d'impact relative à la protection des données**

Analyse des risques, compliance et RGPD. Le règlement présente un certain nombre de dispositions qui relèvent d'une démarche de compliance permettant d'anticiper plutôt que d'intervenir en réaction lorsqu'une violation des règles se révèle. Les collectivités territoriales vont devoir établir une cartographie de tous leurs traitements de données à caractère personnel et recenser les objectifs poursuivis par les opérations de traitement de données ; les acteurs qui traitent ces données et les flux en indiquant l'origine et la destination des données.

L'analyse d'impact[6], élément structurel de la conformité au règlement, consacre une approche par les risques. Elle n'est requise que lorsque le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques tel que l'évaluation/*scoring* (y compris le profilage) ; une décision automatique avec effet légal ; la surveillance systématique ; la collecte de données sensibles ou encore le croisement de données. Les collectivités territoriales devront par exemple réaliser une analyse d'impact en cas d'utilisation d'un réseau de caméras

[5] Article 70-17 de la loi n° 78-17 du 6 janvier 1978 crée par la loi n° 2018-493 du 20 juin 2018.
[6] Article 70-4 de la loi n° 78-17 du 6 janvier 1978 crée par la loi n° 2018-493 du 20 juin 2018.

avec reconnaissance automatique des plaques d'immatriculation, de surveillance des agents ou de collecte de données dans un but de notation ou d'évaluation[7]Note 7. La responsabilité de l'analyse d'impact incombe au responsable de traitement après avoir obligatoirement consulté le DPD. En cas de doute quant à la nécessité d'effectuer une analyse d'impact, il est recommandé d'en effectuer une malgré tout. Elle doit contenir *a minima* une description systématique des opérations de traitement envisagées et les finalités du traitement ; une évaluation de la nécessité et de la proportionnalité des opérations de traitement ; une évaluation des risques sur les droits et libertés des personnes concernées et les mesures envisagées pour faire face aux risques.

B. - **Les obligations de conformité ex post des collectivités territoriales en matière de protection des données à caractère personnel**

1° **La certification et le respect de code de conduite**

Les outils de la conformité. Le RGPD prévoit de nouvelles méthodologies à destination des responsables de traitements et des sous-traitants pour démontrer la conformité de leurs traitements en matière de protection des données à caractère personnel. Ces méthodologies prennent notamment la forme de certifications et de codes de bonne conduite. Ces outils peuvent servir d'éléments pour prouver le respect des obligations incombant au responsable du traitement telles que l'*accountability* ; la protection des données dès la conception et par défaut ou encore le respect de l'obligation de sécurité. La mise en œuvre d'actions conformes à ces outils pourra être prise en compte par l'autorité de contrôle en cas de procédure contentieuse. La certification est volontaire et accessible via un processus transparent. Elle sera délivrée soit par un organisme agréé, soit par l'autorité de contrôle – en France, la CNIL – soit par le Comité européen à la protection des données. L'assurance du respect des différentes obligations peut également se faire par l'application d'un code de bonne conduite. Il sera élaboré, modifié ou prorogé par les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants. Le projet de code sera soumis pour avis. S'il offre des garanties appropriées suffisantes, il sera approuvé, enregistré et publié par la CNIL.

[7] G29, Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD), 4 oct. 2017.

2° **L'obligation technique de sécurisation des données**

Cybersécurité et collectivités territoriales. Le responsable du traitement doit mettre en œuvre des mesures techniques et organisationnelles appropriées pour préserver la sécurité des données à caractère personnel telles que la pseudonymisation et le chiffrement des données à caractère personnel ; le rétablissement de la disponibilité et de l'accès aux données personnelles dans des délais appropriés en cas d'incident physique ou technique et la mise en œuvre de procédures visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures assurant la sécurité du traitement. La destruction, la perte, l'altération, la divulgation et l'accès non autorisés, accidentels ou illicites sont constitutifs d'une faille de sécurité. Le règlement généralise l'obligation de notification de ces failles à l'autorité de contrôle compétente dans un délai de 72h et impose une nouvelle obligation de communication aux personnes concernées par une violation de leurs données. Ces obligations s'appliquent à tous les responsables de traitement qui seront tenus d'informer l'autorité de contrôle de la nature de la violation et, si possible, des catégories et du nombre approximatif de personnes concernées par la violation ; du nom et des coordonnées DPD ; des conséquences probables de la violation et des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, les mesures pour en atténuer les éventuelles conséquences négatives.

2. **Panorama des risques encourus par les collectivités territoriales en matière de protection des données à caractère personnel**

Une cartographie exhaustive des traitements et des données à caractère personnel doit permettre d'identifier les éléments pouvant générer de multiples risques juridiques pour les collectivités territoriales : le risque fonctionnel, réputationnel (**A**), financier et pénal[8] (**B**).

[8] Cette typologie reprend les risques exposés par F. Mattatia dans son étude « la mise en œuvre du RGPD au prisme du risque juridique » : RDLI 2017, n° 140.

A. - **Le risque fonctionnel et réputationnel**

1° **Le risque fonctionnel**

L'atteinte au fonctionnement des services publics. Le RGPD consacre des principes généraux de protection[9] tels que la légalité, la finalité, la légitimité et la proportionnalité du traitement ; de manière plus novatrice, la transparence, la limitation des finalités, la minimisation et la garantie de sécurité des données ; la licéité du traitement ; les conditions applicables au consentement ou celles entourant les traitements de données sensibles ou relatifs aux condamnations pénales et aux infractions. S'ils ne sont pas respectés, ils peuvent altérer le fonctionnement des collectivités et celui de certains services publics. Ce risque fonctionnel peut amener l'autorité de contrôle à interdire temporairement ou définitivement le traitement en cas de mise en demeure restée infructueuse. Une telle décision peut affecter lourdement la mise en œuvre du service public local privé de sa ressource principale. Par exemple, pour ne pas voir leur responsabilité mise en jeu, les collectivités devront assurer la maîtrise des données dans les contrats de marché ou de concession en y insérant des clauses au titre de l'accès aux données à caractère personnel ou au titre de la responsabilité du traitement[10]. Le règlement impose des obligations spécifiques aux sous-traitants qui doivent notamment aider les responsables de traitement dans leur démarche permanente de mise en conformité. Si le responsable de traitement est tenu de s'assurer que ses sous-traitants offrent les garanties nécessaires pour mettre en œuvre un traitement respectueux du RGPD, ce dernier consacre la notion de responsabilité conjointe qui pourra être organisée par le contrat.

2° **Le risque réputationnel**

Atteinte à l'autorité politique de la collectivité. Le RGPD renforce et précise les droits fondamentaux des personnes physiques[11] à l'égard des traitements de données les concernant tels que le droit d'accès ; le droit de rectification, le droit à l'effacement ; le droit à la limitation

---

[9] Article 6 de la loi n° 78-17 du 6 janvier 1978.

[10] https ://droit-des-contrats-publics.efe.fr/2018/09/27/comment-adapter-la-commande-publique-au-rgpd : « Que ce soit pour un dossier de candidature (CV, photo, date de naissance) ou au cours de l'exécution ou de la résiliation d'un achat public, les données sensibles des personnes physiques sont traitées par les acheteurs publics. Ils devront à l'avenir réduire le nombre de renseignements exigés dans le cadre de la passation, pour qu'ils aient un lien direct avec l'objet du contrat. Certains avocats encouragent les acheteurs publics à intégrer une clause relative à l'exploitation limitée des informations récoltées dans le cadre d'un contrat de la commande publique. »

[11] Article 70-18 de la loi n° 78-17 du 6 janvier 1978 crée par la loi n° 2018-493 du 20 juin 2018.

du traitement et notamment la limitation du profilage par algorithmes ; le droit à la portabilité des données et le droit d'opposition. Afin de préserver la confiance des personnes dans le traitement de leurs données, les collectivités territoriales devront être particulièrement vigilantes. Toute méconnaissance de ces droits aura une résonance forte auprès des usagers de nature à affecter la réputation des collectivités territoriales. Les cyber-attaques peuvent également générer un fort risque réputationnel et un déficit d'image. Les applications ou fichiers utilisés par les collectivités recensent de nombreuses informations sur les administrés et usagers (état civil, justificatifs de domicile, données fiscales...). Leur divulgation ou leur mauvaise utilisation est donc susceptible de porter atteinte aux droits et libertés des personnes concernées. Compte tenu du degré d'exposition aux risques, les collectivités territoriales sont donc non seulement tenues de mettre en œuvre des mesures destinées à sécuriser leur système d'information – en se basant sur le Référentiel général de sécurité – mais elles ont également intérêt à développer en leur sein une véritable culture de la sécurité informatique et de la protection des données à caractère personnel.

B. **Le risque financier et pénal**

1° **Le risque financier**

L'augmentation des sanctions financières. Lorsque le responsable du traitement ou le sous-traitant ne respecte pas les obligations résultant du RGPD, le président de la CNIL peut saisir la formation restreinte dans le but de prononcer, après procédure contradictoire, un rappel à l'ordre ; une injonction de mise en conformité du traitement ; la limitation temporaire ou définitive du traitement ; le retrait d'une certification ou une amende administrative[12]. Sur ce point, le RGPD a considérablement renforcé leur montant. La CNIL devra veiller à ce que les amendes administratives soient effectives, proportionnées et dissuasives. En cas de violation notamment des dispositions relatives à la *protection by design* et *by default* ; à la sécurité du traitement et notification des failles de sécurité ; à l'analyse d'impact ; au DPD ou encore à la certification, l'amende s'élèvera à 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial pour une entreprise. L'amende pourra atteindre 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial en cas de violation des principes de base des traitements et des droits dont bénéficient les personnes concernées.

[12] Article 45 de la loi n° 78-17 du 6 janvier 1978 crée par la loi n° 2018-493 du 20 juin 2018.

2° **Le risque pénal et contentieux**[13]

Responsabilité pénale et action de groupe. Les maires et présidents sont responsables des traitements informatiques et de la sécurité des données à caractère personnel qu'ils contiennent. Leur responsabilité civile et pénale peut être engagée. Le Code pénal punit notamment le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite ; le fait de mettre ou de conserver en mémoire informatisée des données à caractère personnel sans le consentement exprès de l'intéressé ou le fait de procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne à des fins de prospection commerciale ou à des fins de recherche dans le domaine de la santé ; le fait de détourner des informations à caractère personnel de leur finalité et le fait de porter à la connaissance de tiers n'ayant pas qualité pour recevoir des données à caractère personnel, des données dont la divulgation porterait atteinte à la considération de l'intéressé ou à sa vie privée *(C. pén., art. 226-16 à 226-24)*. Au-delà des responsabilités individuelles, les collectivités territoriales peuvent également être reconnues responsables, dans les conditions prévues à l'article 121-2 du Code pénal.

Il faut également ajouter le risque découlant de la nouvelle action de groupe en matière de protection des données à caractère personnel consacrée par la loi du 18 novembre 2016 de modernisation de la justice du XXIe siècle. Cette action de groupe a pour objet la cessation du manquement à la législation et non l'indemnisation des préjudices subis. En l'absence de réparation possible pour les personnes concernées, le champ d'application de cette action de groupe est limité. Le RGPD permet toutefois aux personnes concernées de mandater des organismes, organisations ou associations afin d'introduire une réclamation en leur nom devant l'autorité de contrôle pour obtenir réparation des préjudices moraux liés à une atteinte injustifiée au droit à la vie privée.

Le RGPD fonde une approche reposant sur la gestion des risques en matière de protection des données à caractère personnel. Il crée de nombreuses obligations pour les collectivités territoriales. Si sa mise en œuvre avait nécessairement un coût financier pour les collectivités, la mise en conformité assurera non seulement la sécurité juridique mais représentera aussi un

[13] S. Bonenfant, L'environnement « informatique et liberté » des collectivités territoriales, une source de contentieux : AJCT 2017, p. 13.

investissement en terme de valorisation du patrimoine informationnel et de confiance entre les collectivités et leurs usagers.