LES ESSENTIELS

Le RGPD dans les collectivités

Se mettre en conformité et le rester

2e édition

Laurent Charreyron
Consultant, expert en identité numérique et données personnelles

Chloé Hervochon
Juriste consultante RGPD, cabinet de conseils Lexagone

Paul-Amandin Petit
Juriste consultant RGPD, cabinet de conseils Lexagone

territorial éditions

Le RGPD dans les collectivités

Se mettre en conformité et le rester

Depuis le 25 mai 2018, toutes les collectivités doivent être en conformité avec le règlement sur la protection des données personnelles et la loi informatique et libertés modifiée.

Ce guide vous permettra d'en comprendre les dispositions essentielles et de découvrir les grandes étapes du projet de mise en conformité.

À la différence des nombreuses publications juridiques sur le sujet, il propose une approche synthétique et pratique qui s'adresse aussi bien aux élus locaux qu'aux équipes fonctionnelles. Basé sur l'expérience de plusieurs praticiens, c'est un outil irremplaçable de mise à niveau accélérée sur cette réglementation complexe, de sensibilisation des acteurs et de mise en place des fondations du projet.

Le RGPD s'inscrit dans la logique novatrice d'un nouveau service public de la donnée en collectivité. L'ambition de ce guide pratique est aussi de vous permettre de construire le socle solide de votre action de demain.

Laurent Charreyron est consultant sur les problématiques d'identité numérique et de protection des données personnelles. Praticien, de sensibilité à la fois juridique et technologique, il privilégie une approche pragmatique de la gestion des projets transversaux, axée sur les usages et la gouvernance. Coanimateur du diplôme « DPO en collectivité » de l'université de technologie de Troyes et du cycle « Identité numérique » de l'association Villes Internet, il publie régulièrement sur ces sujets dans le blog inuq.eu et participe à des conférences en France et à l'étranger.

Chloé Hervochon et **Paul-Amandin Petit** sont juristes consultants RGPD chez Lexagone, cabinet de conseils spécialisé en protection des données à caractère personnel. Ils sont tous les deux titulaires d'un Master 2 en Droit du numérique. Passionnés par le domaine du numérique en général et celui de la protection des données en particulier, ils accompagnent de multiples organismes dont des collectivités et des communes dans leurs mises en conformité au RGPD en tant que DPO externalisés.

LES ESSENTIELS

boutique.territorial.fr

ISSN : 2553-5803
ISBN : 978-2-8186-1970-4

© Urupong/adobeStock.com

territorial éditions

LES ESSENTIELS

Le RGPD dans les collectivités

Se mettre en conformité et le rester

2e édition

Laurent Charreyron
Consultant, expert en identité numérique et données personnelles

Chloé Hervochon
Juriste consultante RGPD, cabinet Lexagone

Paul-Amandin Petit
Juriste consultant RGPD, cabinet Lexagone

territorial éditions
Référence TBK 324A

Vous souhaitez nous contacter à propos de votre ouvrage ?

C'est simple !

Il vous suffit d'**envoyer un mail à :**
service-client-editions@territorial.fr
en précisant l'objet de votre demande.

Pour connaître l'ensemble de nos publications,
rendez-vous sur notre boutique en ligne
www.boutique.territorial.fr

Avertissement de l'éditeur :
La lecture de cet ouvrage ne peut en aucun cas dispenser le lecteur de recourir à un professionnel du droit.

Il est interdit de reproduire intégralement ou partiellement la présente publication sans autorisation du Centre Français d'exploitation du droit de Copie.
CFC
20, rue des Grands-Augustins
75006 Paris.
Tél. : 01 44 07 47 70

© Territorial, Voiron - CS 70215 - 38501 Voiron Cedex - Tél. : 04 76 65 87 17
ISBN : 978-2-8186-1970-4 – ISBN version numérique : 978-2-8186-1971-1
Imprimé par Reprotechnic, à Bourgoin-Jallieu (38) - Juin 2022
Dépôt légal à parution

Sommaire

Partie 3
Faire vivre le RGPD

Annexes

Avant-propos

Voici maintenant plus de vingt ans qu'Internet évolue et que le numérique en général prend une place tellement plus importante dans nos activités que certains évoquent cette période comme une mutation au moins aussi essentielle que celle qui jadis apporta l'électricité dans tous les foyers.

L'Internet, qui est en fait le principal outil mondial de communication, a été développé à partir de logiciels libres de droits. Le protocole IP ainsi réalisé et évolutif permet aux objets, aux hommes et aux femmes de se connecter. Une adresse de départ et une adresse d'arrivée du message, et voilà que l'information va vers sa destination. Le protocole IPv6 permet déjà de pouvoir connecter tout ce petit monde avec une adresse unique possible pour chaque individu, pour chaque objet sur notre planète. Alors, la tentation est grande d'associer nos identités avec ces adresses IP.

Patrick McGoohan, l'acteur principal (numéro 6) de la célèbre série télévisée *Le prisonnier* y déclarait souvent comme un cri qu'il n'était pas un numéro mais un homme libre. L'identité est une notion qui s'est construite peu à peu depuis le début de l'humanité. Or, réduire sa propre humanité à un chiffre ou bien à quelques mots qui me caractérisent subjectivement, est inexorablement réducteur. Nous sommes des êtres complexes et multiples qui ne sauraient être réduits dans un tableur ou une base de données. Vous l'avez compris, nous touchons là à l'essentiel.

Le règlement général de protection des données (RGPD) issu d'un règlement européen a pour vocation de mettre en œuvre une sécurisation de nos données personnelles. En effet, nous vivons désormais dans un monde où des acteurs mondiaux sont susceptibles peut-être de nous connaître mieux que nous ne nous connaissons nous-mêmes. Il est heureux que l'Europe se préoccupe de ce sujet et que ses institutions construisent une souveraineté protectrice.

Pour l'heure, il nous faut mettre massivement en conformité nos actes avec nos pensées. Les collectivités locales doivent prendre leur part au chantier. La mutation numérique est en cours et va durer probablement encore quelques dizaines d'années. Pour autant, il est vital de ne pas se laisser déborder et de mettre en place les processus d'humanisation de nos organisations. L'action publique doit se renouveler et maîtriser la mutation en cours.

À ce titre, la gestion des données des citoyens devient désormais un enjeu national qui ne saurait être délégué aux forces du marché. Les collectivités locales doivent se positionner comme des tiers de confiance dans ces domaines. C'est là toute l'acuité du travail de Laurent Charreyron, Chloé Hervochon et Paul-Amandin Petit qui proposent un recueil très précis sur les obligations issues du RGPD à respecter et sur les étapes à suivre pour

les mettre en œuvre. C'est à n'en pas douter, pour les acteurs publics locaux, le début de l'appropriation de la gestion des données et de sa gouvernance. Si vous êtes dans cette démarche, cet ouvrage construit avec rigueur sera pour vous un compagnon précieux.

Jean-Luc SALLABERRY
Chef *du département numérique de la FNCCR*
www.fnccr.asso.fr

Préface

Données personnelles et propriété : question d'identité du citoyen

« *Je suis française, majeure et vaccinée.* »

Cette phrase prononcée la tête haute revendique une identité : je suis femme, émancipée et responsable. Je porte mon identité comme ma liberté. Simplement, ces quelques mots informent mes interlocuteurs sur mon pays d'origine, mon âge et ma santé. Pourtant, est-ce bien la vérité ? En France en 2022, pour le prouver je dois fournir des informations vérifiables par l'administration publique : lieu et date de naissance, numéro de Sécurité sociale ou attestation fiscale. Cette preuve de l'« état de civilité » d'une personne reste en 2022 à fournir sur support physique (papier ou numérique). Le plus souvent imprimées, lisibles et tenues en main, ces déclarations signées nous donnent accès à nos droits aux moments clés de nos histoires de vie : naissance, décès, élection, emménagement, études, soins vitaux... Ces données me permettent de renaître régulièrement dans l'espace public pour exercer mes droits et devoirs de citoyen. Et ces droits me sont « donnés » par celui qui détient l'autorité. Le propriétaire des supports matériels de ces « données » personnelles doit être « de confiance ».L'ordinateur[1] n'est qu'une machine intermédiaire des ordres qui lui sont donnés, en l'occurrence par l'État et ses administrations, centrales ou locales. Pour autant, mes droits me sont dus et personne ne doit en tirer un pouvoir commercial, idéologique ou politique.

Dématérialisation de l'identité : une révolution de la liberté ou du contrôle ?

Dans les années soixante, les scientifiques chercheurs en mathématiques et en informatique inventaient l'Internet. Sur ces réseaux numériques, une information est chiffrée puis découpée en morceaux dans un ordinateur[2] avant de circuler dans des câbles pour être reconstituée dans celui du destinataire. Une sécurité inédite pour la circulation de l'information, que les organisations internationales de défense ont immédiatement plébiscitée. On y voit l'outil du secret, clé de la victoire dans une guerre froide qui n'en finissait pas. Quelques philosophes français[3], à l'approche d'une autre révolution, de rue celle-là, ont exploré la part « copernicienne » de cette innovation technique.

1. Ordinateur : au XVIIe siècle, il s'agissait des religieux qui ordonnaient les règles de la vie commune et produisaient l'ordre social.
2. 1969 Réseau Arpanet : 4 laboratoires universitaires américains connectent 4 ordinateurs distants.
3. Les philosophes des processus : Michel Serres, Gilles Deleuze, Pierre Lévy.

Ils y ont vu son impact sociétal immense sur les démocraties, par définition instables. Très vite les chercheurs en droit[4] les ont suivis en exprimant la question fondamentale de l'appartenance.

« À qui appartient l'objet numérique ? » Les débats et les règles se percutent : droit de l'auteur, droit de l'hébergeur, droit de l'éditeur. On laisse à l'utilisateur le droit à l'oubli et à l'État une curieuse concurrence, la souveraineté numérique. Les lois sont publiées, les décrets pas toujours suivis. Les conseillers diplomatiques se font prospectivistes : « *Il est vraisemblable qu'on va assister à une victoire du droit privé sur le droit public, les réseaux correspondant plus au domaine du contrat privé qu'au domaine du contrat social. Ils accoucheront d'une société de marché. Le système judiciaire sera remplacé par des arbitres. Même le politique disparaîtra, puisque le contrat sera individuel et non plus social.* » [5]

Un enjeu européen

Le 25 mai 2018, c'est la naissance d'un règlement européen qui s'inscrit pour les Français dans l'histoire républicaine. Qu'en sera-t-il, outre un vaste marché de nouveaux experts ? Le début de la propriété des données par le citoyen ? Ou un meilleur outil de contrôle, marchés d'un côté, État de l'autre ? Ce règlement est un grand cadre dans lequel chaque élu, chaque décideur public doit peindre le tableau de ses responsabilités. Et pour le moins à haute voix exiger la transparence et la connaissance, car la complexité n'est pas synonyme d'ignorance pour les béotiens. Souhaitons que les nombreux délégués à la protection des données, rendus obligatoires par la Cnil, aient pour première mission l'éducation à la défense des droits numériques des citoyens. Remarquons que 4 ans après une systématisation de certaines règles cachent une application limitée de la loi.

Vigiles pour changer d'attitude

Au milieu du XVII[e] siècle, Spinoza a affirmé que si l'État veut se maintenir, il ne doit exercer aucun contrôle sur les pensées et les idées de ses habitants. Suivons ce grand guide et continuons de produire de la démocratie avec le respect des identités et des données qui en sont la preuve. S'éduquer pour protéger son identité et débattre pour en construire collectivement les défenses. Oui, Internet et les technologies sont sources d'émancipation des individus. Une source qui ne doit pas tarir quand on nous invite à redéfinir encore la vie privée.

La vigilance est un principe pour les élus et décideurs publics, membres de l'association Villes Internet. Vigiles pour saisir le meilleur de la technologie et savoir limiter ses excès, raisonnablement sans la diviniser, ni la diaboliser. Comme un produit desintelligences humaines dont les motivations diverses n'autorisent aucun évitement. Tout abus en matière d'identité abuse la société collectivement.

Commençons avec cet ouvrage, exercice délicat initié par Laurent Charreyron, co-concepteur des premiers débats ouverts sur ce sujet, le Cycle d'assises de l'identité numérique du citoyen que Villes Internet a produites de 2015 à 2016.

4. Lawrence Lessig : spécialiste en droit de la propriété intellectuelle, fondateur de l'organisation Creative Commons : « Nous sommes tellement obnubilés par l'idée que la liberté est intimement liée à celle de gouvernement que nous ne voyons pas la régulation qui s'opère dans ce nouvel espace, ni la menace qu'elle fait peser sur les libertés. »
5. Jacques Attali, Libération, juin 1998.

Consciente des controverses qui ne vont pas manquer d'émerger, des usages qui poseront de nouvelles questions, la seconde édition de cet ouvrage éclaire les opportunités pour les libertés personnelles. Il rappelle la genèse et décrit des méthodes, toujours soucieux de la place à protéger, celle du citoyen.

Il nous invite à « changer d'attitude ». Suivons-le...

Florence DURAND-TORNARE
Fondatrice *et déléguée générale de l'association Villes Internet*
https://www.villes-internet.net/site/

Introduction

Une nouvelle gouvernance de la donnée en collectivité

Attention
Par convention et facilité de lecture de cet ouvrage, nous utilisons le genre masculin comme un genre « neutre » pour parler des acteurs du RGPD.

La protection des données personnelles est un enjeu fondamental de la société de demain. Il concerne chacun de nous, dans toutes nos capacités : individu, citoyen, agent ou partenaire des collectivités. Il est aussi perçu comme une dimension économique importante face aux excès de la mondialisation. C'est pourquoi rarement législation européenne n'aura bénéficié d'un tel consensus.

Pour autant, ce n'est pas une révolution : l'essentiel des principes que le RGPD affirme était déjà défini en France dans la loi informatique et libertés de 1978.

Il faut aussi se replacer dans le mouvement actuel de régulation du monde virtuel et la modernisation de l'action publique, avec la loi pour une République numérique, la loi NOTRe, le Code des relations entre le public et l'administration, la loi Sapin, la loi sur la modernisation de la justice, les textes sur la sécurisation des infrastructures informatiques, sur la signature électronique, *etc*.

Derrière des affirmations de principe parfois monolithiques, le RGPD contient une cinquantaine d'exceptions, qui renvoient au droit national. La loi Informatique et Libertés modifiée (par la loi du 20 juin 2018, l'ordonnance du 12 décembre 2018, le décret d'application du 29 mai 2019).

Voyez le RGPD comme une nouvelle règle du jeu. Un jeu très sophistiqué ! Ses dispositions sont souvent sujettes à interprétation. Elles sont parfois contradictoires avec d'autres législations. En attendant l'inévitable jurisprudence, les autorités nationales réunies au sein du Comité européen à la protection des données (CEDP, ex-« G29 ») publient des « lignes de conduite » et des avis permettant de clarifier certains points. En France, le rôle de la Cnil est déterminant et il faudra toujours se référer à elle en cas de doute.

Elle a notamment publié des référentiels ces dernières années qui doivent être pris en considération par tous les acteurs qui traitent des données personnelles.

Les enjeux de la donnée

Dans un monde presque entièrement informatisé, où le virtuel fusionne à grande vitesse avec le réel, la maîtrise des données est devenue essentielle pour le bon fonctionnement de nos sociétés.

L'Internet et les infrastructures informatiques normalisées sont désormais capables de capturer et d'analyser des masses énormes de données en temps réel, dans tous les domaines.

Le big data et la mobilité ouvrent tous les jours des horizons nouveaux sur nos modes de fonctionnement. D'où l'engouement pour le concept de la « ville intelligente ».

Les données sont devenues le nerf de la guerre des grandes économies financières modernes. Les entreprises qui font l'objet des plus importantes valorisations boursières sont celles dont le cœur de métier est de traiter l'information. La donnée est désormais considérée comme un actif financier, au même titre que les infrastructures traditionnelles.

La donnée générée sur le territoire a une valeur d'usage très concrète pour les citoyens, les acteurs locaux, et pour l'attractivité économique du territoire.

Mais cette valeur est aussi l'objet de toutes les convoitises, ce qui soulève la question fondamentale de la protection des données et des systèmes informatiques dans lesquels elles « vivent ».

C'est un changement de paradigme, qui remet aussi en cause les rôles et les missions traditionnels de tous les acteurs économiques et sociaux, privés et publics.

Le défi des données pour la collectivité

Le territoire est un lieu stratégique de production de l'information. S'y imbriquent les nombreuses infrastructures physiques vitales (eau, électricité, télécommunications, assainissement, transports, voirie, *etc*.) qui permettent à la collectivité de fonctionner, et celles-ci génèrent en permanence des flux de données d'usage ou de performance.

Une fois que l'organisation de l'espace physique est assurée, l'essentiel des activités des collectivités est de fournir des services qui sont autant de flux d'informations à traiter, permettant à nos sociétés complexes de fonctionner.

Le croisement des données d'infrastructure et des données d'organisation et d'usage représente un enjeu majeur pour leur avenir. C'est un des challenges de la ville intelligente et d'un nouvel urbanisme.

Améliorer les outils de pilotage

Dans un contexte économique tendu, il est vital de pouvoir collecter et analyser les données afin d'optimiser la valeur d'usage des infrastructures et d'améliorer le service rendu aux citoyens.

Le mode de gouvernance des collectivités va ainsi évoluer, passant d'une gouvernance patrimoniale (axée sur le développement des infrastructures physiques), à une gouvernance de services (où c'est la capacité de délivrer rapidement des services aux utilisateurs qui prime). Cette nouvelle orientation s'inscrit par ailleurs dans une logique de développement durable, qui souhaite minimiser l'impact écologique.

Elle implique de capturer toutes les interactions pour comprendre finement les comportements des utilisateurs afin de :
- mieux modéliser les investissements et anticiper les évolutions ;
- optimiser l'usage des infrastructures existantes ;
- mutualiser les services et simplifier les organisations ;
- réagir rapidement aux situations de crise et assurer la sécurité.

C'est toute la difficulté de la transformation numérique, qui impose de décloisonner et de croiser les données pour affiner les outils de pilotage et d'aide à la décision.

Créer de la valeur pour tous

Dans la logique du service public, la mise en valeur et l'exploitation des données générées par le territoire doivent se faire au bénéfice de tous.

Cela implique :
- d'ouvrir l'accès aux données (open data) ;
- de garder la maîtrise sur les conditions d'exploitation, notamment dans les relations avec les exploitants des infrastructures matérielles, ou les sous-traitants ;
- de gérer activement ce nouveau patrimoine en le partageant avec les acteurs des autres dimensions territoriales.

La collectivité doit s'emparer de cette nouvelle mission, notamment pour favoriser l'attractivité économique et jouer son rôle d'aménagement du territoire numérique.

Il s'agit d'un nouveau « service public de la donnée » visant à garantir l'accès des données à tous, et à s'assurer que la donnée est collectée, traitée et conservée dans le respect des obligations légales de chaque activité.

Cette valorisation de la donnée implique la mise en place de toute une chaîne de services et d'applications informatiques (stockage, sécurité, traçabilité, conformité, *etc.*), c'est pourquoi on parle de plus en plus de la collectivité comme d'une « plate-forme » de services, à l'usage de tous les acteurs du territoire.

Attention
L'open data est devenue une obligation réglementaire :
- c'est une obligation pour les collectivités de plus de 3 500 habitants : loi NOTRe, loi Valter, loi Macron, loi pour une République numérique, qui emploient plus de 50 agents (en équivalent temps plein) ;
- depuis le 7 octobre 2018, les données essentielles de la commande publique : doivent être mises à disposition ;
- depuis le 1er août 2017, les données essentielles des conventions de subvention sont rendues publiques.

Exploiter et partager les données

Exploiter la donnée territoriale, c'est créer des entrepôts de données, monter des systèmes d'information géographique, mettre en place des outils analytiques et de visualisation, affiner les outils décisionnels et les tableaux de bord.

Il s'agira de gérer activement les données dans le système d'information :
- savoir où elles résident, faire des cartographies ;
- s'assurer de leur qualité : comment sont-elles saisies, sont-elles correctement décrites ?

- en organiser le cycle de vie : collecte, anonymisation, suppression, backup, archivage ;
- puis penser la mise à disposition des informations via des portails dédiés (plate-forme d'information géographique, portails thématiques, *etc.*), des applications mobiles ou des API[6] documentées ;
- enfin organiser l'utilisation et le partage des connaissances en interne via le réseau social d'entreprise.

Attention
La coordination de l'information géographique est une compétence régionale (loi NOTRe).

Protéger les données

La mission de protection des données est fondamentale. La collectivité doit s'imposer comme un tiers de confiance impartial et être le garant de la qualité de cette « matière première numérique » auprès des usagers et des partenaires. Il y va de sa légitimité politique.

Elle devra donc :
- vérifier la conformité juridique et technique des traitements, dans une démarche d'amélioration continue ;
- s'assurer régulièrement de la sécurité à tous les niveaux de l'infrastructure informatique et des applications, en conformité avec le RGS[7] et les réglementations sectorielles ;
- porter une attention particulière à l'application du RGPD pour la protection des données à caractère personnel.

Les deux derniers points impliquent de passer à un mode de gestion « par les risques », c'est-à-dire de tenter d'avoir une vue analytique sur l'activité, afin d'anticiper et de se concentrer sur les informations sensibles.

En parallèle, il faudra assurer la traçabilité exhaustive des opérations afin de pouvoir réagir rapidement en cas de fuite de données, et justifier à tout moment des mesures prises auprès des autorités de contrôle.

Tout le monde est partie prenante

Avec l'informatique, c'est bien tous les acteurs gravitant autour de la collectivité qui sont concernés, car tous contribuent à produire l'information.

On sait, par ailleurs, que l'essentiel des attaques informatiques pourrait être évité par de simples mesures comportementales. En interne, il sera donc indispensable de mener immédiatement des actions de sensibilisation et d'éducation des agents à la sécurité des données. C'est une des missions prioritaires de la très active ANSSI[8] (voir son MOOC : www.secnumacademie.gouv.fr).

6. Application Programing Interface : ce sont les briques du lego applicatif qui permettent d'accéder directement aux fonctions des applications.
7. Le référentiel général de sécurité (RGS) est le cadre réglementaire permettant d'instaurer la confiance dans les échanges au sein de l'administration et avec les citoyens.
8. Agence nationale de la sécurité des systèmes d'information.