GUIDE PRATIQUE ET NOTICES JURIDIQUES A DESTINATION DES COLLECTIVITES TERRITORIALES ET DE LEURS GROUPEMENTS

Les enjeux du big data territorial

Table des matières

Rappel des principales notions juridiques 4

Qu'est-ce que l'open data ? 5

Qu'est-ce que le big data ? 5

Qu'est-ce qu'une donnée personnelle ? 6

Que recouvre la notion de « traitement » de données à caractère personnel ? 6

Qui est le responsable de traitement ? 6

Que recouvre la nouvelle notion de « donnée de référence » au sens de la loi pour une République numérique ? 7

Guide à destination des collectivités territoriales 9

Que recouvre la notion de donnée publique ? 10

En quoi consiste l'ouverture des données publiques ? 10

Quand devrais-je mettre en ligne l'ensemble de mes données publiques ? 11

Quelles sont les responsabilités qui pèsent sur moi dans la gestion de mes données publiques ? 12

Notices juridiques 13

Chaine de valeur de la donnée : les principaux enjeux juridiques 14

L'accès aux données : 14

La collecte des données : 15

Le traitement, la réutilisation, l'archivage et le partage : 16

La responsabilité administrative et pénale liées à la protection des données personnelles 20

Conditions de licéité des traitements de données à caractère personnel 20

Conditions de mise en jeu de la responsabilité administrative et pénale des collectivités 21

Encadrement juridique des algorithmes 22

Rappels des enjeux juridiques 22

Le nouveau dispositif introduit par la loi pour une République numérique 22

Les enjeux liés à la notion de redevance 24

Principales dispositions des directives communautaires 24

La transposition de la directive 2013/37/UE par la loi VALTER 24

La cyberdéfense : nouvel enjeu de sécurité nationale 28

Présentation du programme PEPIC 28

Le cadre juridique national 29

L'insuffisante sensibilisation des collectivités territoriales en matière de sécurité informatique 31

Proposition de clausier type : éléments susceptibles d'être intégrés au sein des contrats de la commande publique 33
Eléments de contexte 33
Articulation du dispositif de protection des données personnelles avec celui institué dans le cadre des contrats de concession 33
Types de clauses susceptibles d'être insérées dans les contrats publics 34
Modalités d'ouverture et de mise à disposition des données à destination des administrés 34
Le régime de propriété des données 35
La responsabilité liée au traitement des données 36
Liste des principaux textes examinés dans le cadre du présent document 38
Textes communautaires : 38
Textes nationaux : 38
Glossaire 40

Rappel des principales notions juridiques

Qu’est-ce que l’open data ?

De manière littérale, le concept d’**open data** désigne une donnée numérique dont l'accès et l'usage sont laissés libres aux usagers. Cette donnée peut être d'origine publique ou privée, produite par l’Etat, une collectivité locale, un service public, ou encore une entreprise.

La donnée est diffusée de manière structurée, selon une méthode et une licence ouverte garantissant son libre accès et sa réutilisation par tous, sans restriction technique, juridique ou financière.

L’open data s'inscrit dans une tendance qui considère l'information publique comme un bien commun dont la diffusion est d'intérêt public et général.

L’open data représente à la fois un mouvement, une philosophie d'accès à l'information et une pratique de publication de données librement accessibles et exploitables.

Sous l’impulsion de l’Union Européenne, la mise à disposition des données et leur réutilisation se sont développées pour créer un vecteur de lisibilité de l’action publique, de développement économique et d’innovation, principes fondateurs de l’open data.

Depuis lors, la libéralisation des données publiques et le mouvement de mise à disposition est vivement engagé.

L'ouverture des données ou « open data » constitue aujourd’hui un véritable enjeu des politiques publiques comme nous le verrons ci-après.

Qu’est-ce que le big data ?

Le **big data** peut être entendu comme un concept permettant de stocker un très grand nombre d’informations sur une base numérique. Sa définition peut néanmoins varier selon que l’on se place du côté de l’usager ou du côté du fournisseur de services.

Littéralement, ces termes signifient « mégadonnées », grosses données ou encore données massives.

Le big data désigne un ensemble très volumineux de données qu’aucun outil classique de gestion de base de données ou de gestion de l’information ne peut traiter. Il se présente comme une solution dessinée pour permettre à tous d’accéder en temps réel à des bases de données géantes.

Le big data est aujourd’hui étudié comme un concept transdisciplinaire recouvrant une multiplicité de techniques et d’innovations relatives au stockage de données mais aussi à leur traitement.

Le phénomène de prolifération exponentielle, extrêmement rapide des données numériques classiques, en grande expansion ces dernières années, constitue un véritable enjeu pour les collectivités locales.

Il n'est cependant pas sans susciter des interrogations et difficultés de mise en œuvre.

En effet, il semblerait que les régimes de protection des données soient peu aptes à faire face aux défis inédits posés par les phénomènes de profilage et de personnalisation propres à la société numérisée.

Qu'est-ce qu'une donnée personnelle ?

Aux termes de l'article 2 de la loi CNIL, la notion de **donnée personnelle** est définie comme toute information relative à une personne physique :

- identifiée ou qui peut être identifiée,
- directement ou indirectement,
- par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.

Que recouvre la notion de « traitement » de données à caractère personnel ?

Aux termes de l'article 2 de la loi CNIL, le **traitement** concerne toute opération ou tout ensemble d'opérations portant sur de telles données à caractère personnel, quel que soit le procédé utilisé, et notamment :

- la collecte,
- l'enregistrement,
- l'organisation,
- la conservation,
- l'adaptation ou la modification,
- l'extraction,
- la consultation,
- l'utilisation,
- la communication par transmission, diffusion ou toute autre forme de mise à disposition,
- le rapprochement ou l'interconnexion,
- ainsi que le verrouillage, l'effacement ou la destruction.

Qui est le responsable de traitement ?

Aux termes de l'article 3 de la loi CNIL, le **responsable de traitement** est en principe la personne, l'autorité publique, le service ou l'organisme qui détermine les finalités et les moyens du traitement.
Le responsable de traitement met en œuvre le traitement dans son intérêt, en son propre nom et pour son propre compte.

C'est à lui de veiller au respect de la loi CNIL en déclarant les traitements sous sa responsabilité au correspondant informatique et libertés (ou à la CNIL si nécessaire) ainsi que leur modification ou suppression au risque de voir sa responsabilité civile et pénale engagée.

Le responsable de traitement ne doit pas être confondu avec :

- la personne concernée par le traitement ou le destinataire du traitement;

- le sous-traitant du responsable de traitement, qui, au terme de l'article 35 de la loi CNIL, est défini comme « *toute personne traitant des données à caractère personnel pour le compte du responsable des traitements* ». Etant précisé que lorsqu'un traitement est sous-traité, ledit sous-traitant ne devient pas le responsable du traitement, lequel conserve toute la responsabilité aux yeux de la loi.

- un « tiers autorisé » qui, au terme de l'article 3 de la loi CNIL vise les autorités habilitées par un texte de loi pour accéder aux contenus des traitements de données à caractère personnel. Tel est le cas par exemple de la **Commission Nationale de l'Informatique et des Libertés (CNIL).**

Que recouvre la nouvelle notion de « donnée de référence » au sens de la loi pour une République numérique ?

Aux termes de l'article 14 de la **loi n°2016-1321 du 7 octobre 2016 pour une République numérique,** sont des **données de référence**, les documents produits ou reçus par les administrations qui satisfont aux conditions suivantes :

- Elles constituent une référence commune pour nommer ou identifier des produits, des services, des territoires ou des personnes ;

- Elles sont réutilisées fréquemment par des personnes publiques ou privées autres que l'administration qui les détient ;

- Leur réutilisation nécessite qu'elles soient mises à disposition avec un niveau élevé de qualité.

La mise à disposition des données de référence en vue de faciliter leur réutilisation constitue une mission de service public relevant de l'Etat et à laquelle concourent l'ensemble des administrations publiques.

Guide à destination des collectivités territoriales

Que recouvre la notion de donnée publique ?

Traditionnellement, la notion de donnée publique a été rattachée dans la loi CADA, désormais codifiée au sein du code des relations entre le public et l'administration (CRPA) à celle de « **document administratif** ».

Or, la notion de document administratif revêt une acception très large et vise tout document produit ou reçu dans le cadre d'une **mission de service public** par une collectivité publique ou un organisme privé chargé d'une telle mission.

Ainsi, on comprend aisément que de très nombreux documents sont susceptibles de revêtir la qualité de donnée publique car rares sont les activités de l'administration qui ne sont pas exercées dans le cadre d'une mission de service public.

Et c'est justement l'un des principaux apports de la loi pour une République numérique qui ajoute à la catégorie des données publiques, l'ensemble des données produites et reçues par les administrations et **qui ne faisaient pas l'objet d'une diffusion publique** jusqu'alors.

Dès lors, sauf exception prévue par le législateur, la quasi-totalité des données détenues par les administrations devront être mises à la disposition du public.

Demeurent non communicables, les documents administratifs dont la consultation ou la communication porterait atteinte :

- **à la sécurité publique** soit en particulier, au secret des délibérations du Gouvernement, au secret de la défense nationale, à la sûreté de l'Etat et tous autres secrets protégés par la loi ;

- **aux personnes** soit en particulier, à la protection de la vie privée, au secret médical :

- **au secret en matière commerciale et industrielle.**

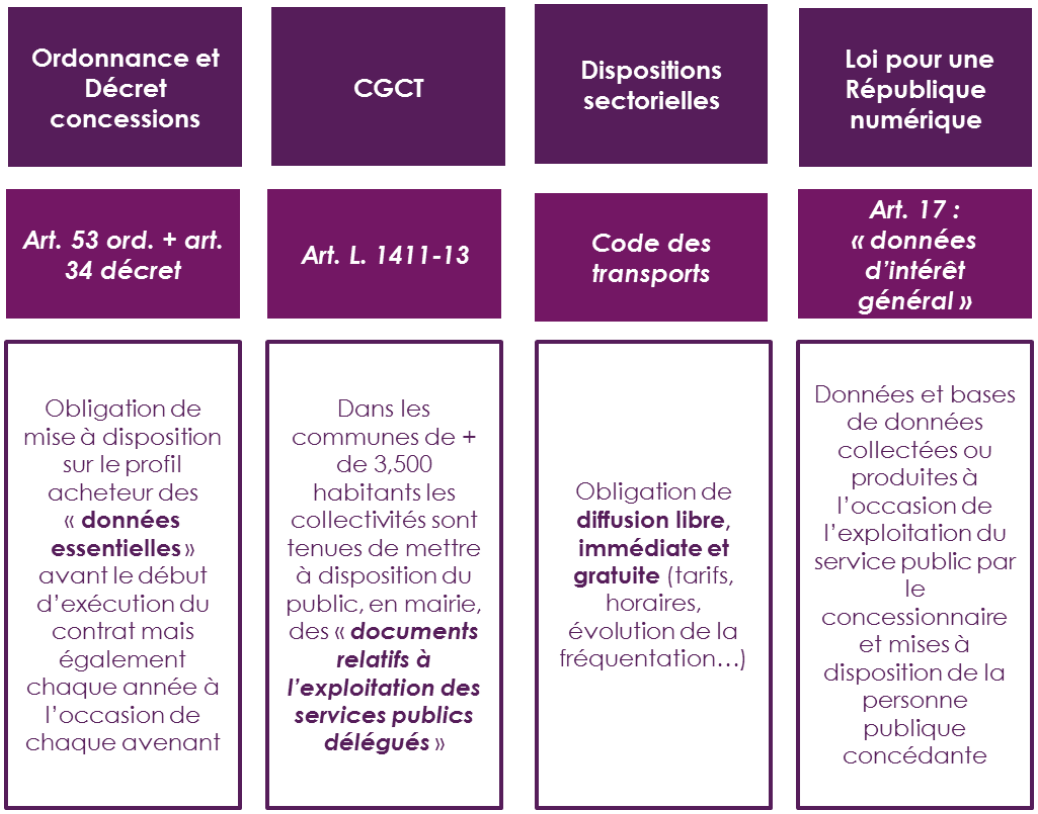
A cet égard, les nouvelles dispositions de la loi pour une République numérique obligent désormais l'administration à mettre à disposition du public les données personnelles qu'elle a en sa possession, après qu'elles aient fait l'objet d'un traitement permettant de rendre impossible l'identification de ces personnes.

En quoi consiste l'ouverture des données publiques ?

Le législateur s'est engagé ces dernières années, dans une politique volontariste d'ouverture des données publiques ou « politique d'open data » allant jusqu'à consacrer dans le cadre de la loi pour une République numérique, **l'obligation pour les administrations de mettre à disposition les données qu'elles détiennent.**

Cette obligation se trouve également renforcée dans le cadre des contrats publics et, en particulier, des contrats de concession sous l'impulsion des ordonnances et décrets de transposition des directives communautaire « concessions » et « marchés publics ».

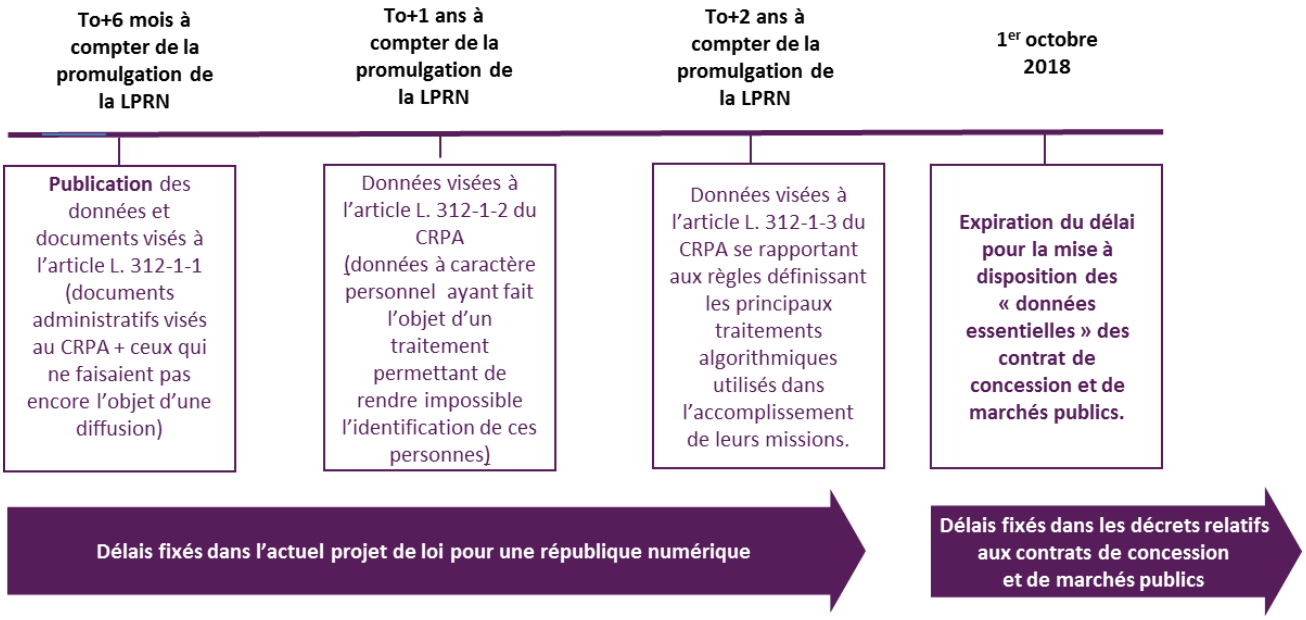
Or, l'étude approfondie des différents textes fait ressortir pour un même contrat de concession, un **empilement des différentes obligations d'open data**, tel que résumé dans le schéma ci-dessous :



Outre cet empilement des textes, d'une façon générale, il appartiendra aux collectivités territoriales de s'interroger sur les modalités de mise en œuvre des nouvelles obligations d'open data qui ont été mises à leur charge d'autant plus que, souvent, les différents échelons de collectivités territoriales n'ont pas tous appréhendé de la même manière ces nouvelles obligations.

Quand devrais-je mettre en ligne l'ensemble de mes données publiques ?

Les nouvelles obligations introduites par les textes susvisés entreront rapidement en vigueur, comme rappelé sur la frise ci-dessous :



Quelles sont les responsabilités qui pèsent sur moi dans la gestion de mes données publiques ?

La responsabilité d'une collectivité publique dans la gestion de ses données peut être mise en jeu à un double titre :

- ***au titre des obligations d'open data***, car, en cas de refus de communication de documents par l'administration, la **Commission d'Accès aux Documents Administratifs (CADA)** peut être saisie dans un délai de deux mois à compter de la notification du refus ou de l'intervention du refus tacite. Dès lors qu'elle est saisie, la CADA émet un avis sur le refus de communication ouvrant la voie à la saisine du juge administratif ;

- ***au titre de la gestion des données,*** la collectivité peut mettre en jeu sa responsabilité administrative et pénale en cas de violation des dispositions de la loi CNIL, lesquelles viendront à être profondément modifiées à la suite de l'entrée en vigueur du règlement communautaire relatif à la protection des données personnelles, adopté le 14 avril 2016 par le Parlement européen et dont la mise en œuvre effective est en principe programmée pour 2018.

Notices juridiques

Chaine de valeur de la donnée : les principaux enjeux juridiques

Si les enjeux pour les collectivités territoriales et les acteurs privés dans le processus de gestion de la donnée sont nombreux – et ont été renforcés dans le cadre de la loi pour une République numérique – ils ne sont pas les mêmes selon que l'on se situe au stade :

- de l'accès aux données (ou « open data ») ;
- de la collecte des données ;
- du traitement, de la réutilisation, de l'archivage et du partage.

L'accès aux données :

Du côté des acteurs publics

Le législateur s'est engagé dans une politique volontariste d'ouverture des données publiques.

La plupart des lois récentes incitent l'administration à mettre à disposition du public les données qu'elles détiennent.

Outre les nombreux textes « sectoriels », des textes généraux, tels que la loi NOTRe, sont venus imposer de nouvelles obligations de mise à disposition des données aux collectivités.

Ainsi, l'article 106 de la loi NOTRe, intitulé « **Transparence des données des collectivités territoriales »** précise que :

> « *les collectivités territoriales de plus de 3 500 habitants ainsi que les EPCI à fiscalité propre auxquels elles appartiennent rendent accessibles en ligne les* ***informations publiques mentionnées à l'article 10 de la loi n° 78-753 du 17 juillet 1978 lorsque ces informations se rapportent à leur territoire et sont disponibles sous forme électronique.*** *Ces informations publiques sont offertes à la* ***réutilisation*** *dans les conditions prévues au chapitre II du titre Ier de la même loi.* »

Outre le caractère particulièrement général d'une telle disposition, force est de constater qu'elle préfigurait déjà les nouvelles obligations que le législateur allait mettre à la charge des collectivités dans le cadre de la loi pour une République numérique.

En effet, le législateur a estimé nécessaire de modifier encore davantage le cadre juridique de l'ouverture des données publiques pour passer de l'incitation à **l'obligation pour les administrations de mettre à disposition les données qu'elles détiennent.**

Toutefois, la législation d'ores et déjà en vigueur distinguait déjà trois cas d'ouverture des données publiques, lesquels étaient soumis à des conditions de mise en œuvre différentes :

- la communication,
- la publication,
- la réutilisation.

La loi pour une République numérique se propose donc d'introduire davantage de continuité entre ces trois phases en généralisant la mise à disposition des données par les administrations qui les détiennent.

Du côté des acteurs privés

De leur côté, les acteurs privés ont également été soumis, ces dernières années, à davantage d'obligations de mise à disposition d'informations qu'ils détiennent.

Ces obligations sont bien évidemment renforcées lorsque l'on se situe dans le champ des contrats publics et, en particulier des délégations de service public, nouvelles conventions de concession (dans le cadre de la réforme des contrats et marchés publics), thématique ayant occupé une large partie des débats parlementaires relatifs au projet de loi pour une République numérique.

En effet, la loi propose de créer un nouveau dispositif d'ouverture des données **pour renforcer l'information des personnes publiques sur les services qu'elles décident de déléguer à des acteurs privés.**

Enfin, les conventions de concession de certains secteurs jugés « sensibles » devront désormais être soumises à des obligations renforcées de mise à disposition d'informations.

A titre d'illustration, dans le secteur des transports publics, les entreprises concessionnaires doivent, conformément aux dispositions de l'article L. 1115-1 du code des transports, diffuser certaines données « *librement, immédiatement et gratuitement en vue d'informer les usagers et de fournir le meilleur service* » comme les tarifs, les horaires, l'évolution de la fréquentation, etc.

La collecte des données :

Du côté des acteurs publics

Il n'est pas toujours aisé pour les collectivités territoriales d'obtenir, de la part de leurs partenaires privés, l'ensemble des informations relatives aux services qu'elles délèguent, lesquelles ne sont, en général, pas accessibles « en ligne ».

Or, l'exploitation d'un contrat public donne aujourd'hui lieu à la **production d'un volume croissant de données**, en particulier dans les domaines de l'eau ou encore des transports, par exemple.

Il est plus qu'indispensable pour la collectivité de pouvoir disposer de ces données, d'une part, afin d'en assurer leur **mise à disposition**, et, d'autre part afin de pouvoir assurer efficacement le **suivi**, **l'évolution** mais surtout le **renouvellement du contrat** en cause.

Du côté des acteurs privés

De leur côté, les partenaires privés des collectivités territoriales détiennent, dans le cadre de l'exécution des missions de service public qui leur ont été déléguées, des informations de natures diverses et potentiellement sensibles :

- informations commerciales,
- informations personnelles,
- savoir-faire industriel,
- cyber-sécurité.

Aujourd'hui, certains concessionnaires ou détenteurs de droits exclusifs tels qu'ERDF, par exemple, masquent les données commercialement sensibles ou comportant des données à caractère personnel.

En effet, ces derniers tendent à se retrancher derrière la **responsabilité civile et pénale** qui est la leur aux termes des dispositions de la loi CNIL, comme exposé au sein de la fiche consacrée à la responsabilité CNIL.

Le traitement, la réutilisation, l'archivage et le partage :

Du côté des acteurs publics

De nombreuses incertitudes persistent à l'heure actuelle, compte tenu des différentes problématiques que suscite chacune de ces tâches que sont :

- Le traitement,
- La réutilisation,
- Et l'archivage de la donnée.

Les conditions de réutilisation des données publiques :

De récentes modifications ont été apportées par le législateur aux conditions de réutilisation des informations publiques.

En effet, il ressort du nouvel article L321-1 du CRPA que :

> « *Les informations figurant dans des documents produits ou reçus par les administrations mentionnées à l'article L. 300-2, quel que soit le support, peuvent être utilisées par toute personne qui le souhaite à d'autres fins que celles de la mission de service public pour les besoins de laquelle les documents ont été produits ou reçus.*

Lorsqu'elles sont mises à disposition sous forme électronique, ces informations le sont, si possible, dans un standard ouvert et aisément réutilisable, c'est-à-dire lisible par une machine. »

Cette disposition définit la réutilisation d'informations comme **leur utilisation à d'autres fins que celles de la mission de service public pour les besoins de laquelle ces informations ont été produites ou reçues.**

Etant précisé que, aux termes des dispositions de l'article L. 322-2 du même code et conformément aux prescriptions de la loi CNIL, les informations publiques comportant des données à caractère personnel peuvent faire l'objet d'une réutilisation, soit lorsque la personne intéressée y a consenti, soit si l'autorité détentrice est en mesure de les rendre anonymes ou, à défaut d'anonymisation, si une disposition législative ou réglementaire le permet.

Enfin, si elle ne l'a pas rendue obligatoire, la loi VALTER du 28 décembre 2015 (relative à la gratuité et aux modalités de réutilisation des informations du secteur public) a affirmé la faculté pour les administrations de soumettre à **licence de réutilisation**, les informations publiques **à titre gratuit.**

Une licence de réutilisation a pour objet de fixer les conditions spécifiques de réutilisation des informations publiques, désormais codifiées dans le CRPA.

Ces nouvelles dispositions ont ouvert un nouveau champ d'action aux collectivités territoriales, lequel ne sera pas sans générer des incertitudes quant à ses modalités de mise en œuvre.

L'archivage des données publiques :

L'ensemble du régime juridique applicable à l'archivage figure au sein du code du patrimoine, lequel régit, notamment, la définition et la justification des archives, le réseau des archives de l'État, l'exercice du contrôle scientifique et technique de l'État sur les archives publiques, les modalités de collaboration entre les services producteurs et les services d'archives, les versements dans les services publics d'archives, l'accès aux archives et régime de communication des archives ainsi que les sanctions pénales.

Par ailleurs, deux nouvelles instances dédiées à la problématique de l'archivage ont été créées : **le délégué et le comité interministériel aux archives de France dont le directeur, chargé des Archives de France assure le secrétariat.**

Les archives sont définies comme :

- Les documents qui procèdent de l'activité, dans le cadre de leur mission de service public, de l'Etat, des collectivités territoriales, des établissements publics et des autres personnes morales de droit public ou des personnes de droit privé chargées d'une telle mission ;
- Les minutes et répertoires des officiers publics ou ministériels.

Les collectivités territoriales et leurs groupements sont « propriétaires de leurs archives ». Elles en assurent elles-mêmes la conservation et la mise en valeur.

Toutefois, les régions peuvent également confier la conservation de leurs archives, par convention, respectivement au service d'archives du département où se trouve le chef-lieu de la région.
Les groupements de collectivités peuvent, quant à eux, les déposer au service départemental d'archives compétent.

Le régime de communicabilité des archives publiques et notamment les délais de communication, est différent selon la nature de ces archives.

Le régime de réutilisation des informations publiques figurant dans ces archives mériterait cependant d'être clarifié.

À défaut d'interdiction ou d'encadrement de la réutilisation des informations publiques contenues dans les archives publiques, le principe est celui de la **liberté de réutilisation**, dans le respect de la loi CNIL.

Le code du patrimoine prévoit un certain nombre d'infractions pénales réprimant la violation des règles régissant les archives.

Du côté des acteurs privés

Dans l'hypothèse où une entreprise produit de la donnée, cette activité doit entrer dans le champ concurrentiel : son traitement doit être valorisé et les modalités de réutilisation et de partage commercialisées.

Le schéma ci-après, présente, en synthèse, les différents enjeux liés à la donnée, selon que l'on se place au stade de **l'accès**, de **la collecte** ou **du traitement** d'une part, et selon que l'on se place côté acteurs publics ou acteurs privés :

ENJEU N°1: **ACCES AUX DONNEES**	Côté acteurs publics	Vers la généralisation massive de la diffusion et de la mise à disposition de données publiques collectées. Passage d'une logique de demande d'accès à une offre d'accès
	Côté acteurs privés	Obligation de fournir aux collectivités, les données collectées et produites à l'occasion d'un service public : Loi pour une République numérique / Loi TECV / Loi NOTRe / Ordonnances concessions et marchés publics
ENJEU N°2: **COLLECTE DES DONNEES**	Côté acteurs publics	Difficultés pour les collectivités d'obtenir auprès de leurs partenaires privés des informations nécessaires au fonctionnement des services publics.
	Côté acteurs privés	Contraintes particulières liées à la préservation et à l'anonymisation des données personnelles ou commercialement sensibles et, notamment, à l'obtention, en temps réel des données de consommation.
ENJEU N°3: **TRAITEMENT, REUTILISATION, ARCHIVAGE**	Côté acteurs publics	Incertitudes liées aux conditions de réutilisation des données publiques, notamment dans le cadre de licence de réutilisation ou encore au stade de l'archivage des données.
	Côté acteurs privés	Dans l'hypothèse où une entreprise produit de la donnée, cette activité entrera dans le champ concurrentiel : son traitement sera valorisé et les modalités de réutilisation et de partage commercialisées.

La responsabilité administrative et pénale liées à la protection des données personnelles

Le respect, par les collectivités locales, des règles de protection des données à caractère personnel est un **facteur de transparence et de confiance** à l'égard des usagers. C'est aussi un **gage de sécurité juridique** pour les élus qui, responsables des fichiers mis en œuvre, doivent veiller à ce que la finalité de chaque traitement informatique et les éventuelles transmissions d'informations soient clairement définies, les dispositifs de sécurité informatique précisément déterminés et les mesures d'information des administrés appliquées.

Conditions de licéité des traitements de données à caractère personnel

Les conditions de licéité des traitements de données à caractère personnel peuvent être synthétisées autour des cinq notions clefs suivantes :

- **La finalité** : les données doivent être collectées pour des finalités « *déterminées, explicites et légitimes* » et ne doivent pas être traitées ultérieurement « *de manière incompatible avec ces finalités* » ;

- **La pertinence** : seules doivent être collectées les données « *adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs* » ;

- **La conservation** : les données doivent être conservées « *pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées.* » ;

- **Le respect des droits des personnes** : un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée ou satisfaire à l'une des conditions suivantes :

    - le respect d'une obligation légale incombant au responsable du traitement ;
    - la sauvegarde de la vie de la personne concernée ;
    - l'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ;
    - l'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci ;
    - la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée.

- **La sécurité :** le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

Conditions de mise en jeu de la responsabilité administrative et pénale des collectivités

La CNIL, dès lors qu'elle est compétente, dispose d'un pouvoir large de sanction en cas de réutilisation des données à caractère personnel contraire à la loi et notamment en cas d'atteinte aux droits de la personne résultant des fichiers ou des traitements informatiques.

A cet égard, les collectivités territoriales et leurs groupements ne sont responsables pénalement que des infractions commises dans l'exercice d'activités susceptibles de faire l'objet de conventions de concession, comme cela est rappelé par l'article 121-2 du code pénal.

Cette responsabilité n'exclut pas toutefois la responsabilité pénale des personnes physiques auteurs ou complices des mêmes faits (art. 121-2 du code pénal, par renvoi de l'art. 226-24).

Les principales infractions réprimées par le code pénal peuvent être résumées de la manière suivante :

AU STADE DE LA COLLECTE	**5 ans de prison / 300 000 € d'amende**	• Fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite (art. 226-18).
AU STADE DE LA CONSERVATION	**5 ans de prison / 300 000 € d'amende**	• Conservation en mémoire informatisée, non prévue par la loi, ou non autorisée par l'intéressé, de données à caractère personnel concernant notamment les origines raciales, ethniques, opinions politiques…les infractions, condamnations, mesures de sûreté (art. 226-19). • Conservation au-delà de la durée prévue par la loi (art. 226-20).
AU STADE DU TRAITEMENT, DE LA REUTILISATION, DU TRANSFERT	**5 ans de prison / 300 000 € d'amende** **3 ans de prison / 100 000 € d'amende pour la divulgation prévue à l'art. 226-22**	• Traitement de données à caractère personnel sans le consentement des personnes concernées ou malgré leur opposition, à des fins de prospection notamment commerciale (art. 226-18-1) ou dans le domaine de la santé (art. 226-19-1); • Détournement des informations à caractère personnel de leur finalité lors de leur enregistrement, classement, transmission ou toute autre forme de traitement (art. 226-21); • Fait de porter à la connaissance de tiers n'ayant pas qualité pour recevoir les données à caractère personnel, des données dont la divulgation porterait atteinte à la considération de l'intéressé ou à sa vie privée (art. 226-22); • Transfert de données à caractère personnel faisant l'objet ou destinées à faire l'objet d'un traitement vers un Etat hors UE (art. 226-22-1).

Encadrement juridique des algorithmes

Rappels des enjeux juridiques

Comme le relevait le Conseil d'Etat dans son étude annuelle 2014 consacrée au numérique et aux droits fondamentaux, il devient aujourd'hui essentiel de prendre la mesure du rôle d'intermédiation joué par les algorithmes et de concevoir leur encadrement juridique et leur utilisation.

En effet, si l'utilité des algorithmes pour optimiser un certain nombre de services n'est pas discutable, ils présentent cependant des sources de risques liés notamment à une exploitation toujours plus fine des données à caractère personnel notamment.

Des outils de régulation de l'utilisation des algorithmes doivent dès lors être mis en place.

A cet égard, dans son rapport, le Conseil d'Etat préconisait trois méthodes d'encadrement :

- Assurer l'effectivité de l'intervention humaine dans la prise de décision au moyen d'algorithmes,
- Mettre en place des garanties de procédure et de transparence lorsque les algorithmes sont utilisés pour prendre des décisions à l'égard d'une personne,
- Développer le contrôle des résultats produits par les algorithmes, notamment pour détecter l'existence de discriminations illicites.

Or, aujourd'hui de nombreuses décisions individuelles sont prises par l'administration assistée de **traitements algorithmiques**, c'est-à-dire d'outils soumettant les données entrées par l'administration à une suite d'opérations ou d'instructions permettant d'aboutir à un résultat.

De tels instruments sont, en particulier, utilisés pour gérer de grandes masses de données, faisant intervenir de multiples facteurs à prendre en compte comme des listes de vœux ou des critères à croiser, afin d'optimiser les solutions.

Comme le relevait la CNIL dans son avis sur le projet de loi pour une République numérique[1], la loi CNIL, apporte déjà certaines garanties, au titre notamment de son article 10, lequel interdit qu'une « *décision produisant des effets juridiques à l'égard d'une personne physique* » puisse résulter de la seule mise en œuvre d'un traitement de données « *destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité* », sans intervention humaine.

Toutefois, ce dispositif demeure limité aux traitements de données à caractère personnel.

Le nouveau dispositif introduit par la loi pour une République numérique

[1] CNIL, délibération n° 2015-414 du 19 novembre 2015 portant avis sur un projet de loi pour une République numérique.

La loi pour une République numérique a entendu permettre aux usagers, ayant fait l'objet d'une décision individuelle prise sur le fondement d'un traitement algorithmique, de disposer d'un **droit d'accès** aux règles définissant le traitement algorithmique, ainsi qu'aux principales caractéristiques de sa mise en œuvre.

L'article 4 de la loi a ainsi introduit un nouvel article L. 311-3-1 au sein du CRPA, intitulé « *Droit d'accès aux règles et caractéristiques de l'algorithme intervenu dans la prise d'une décision individuelle* », prévoyant que toute décision individuelle prise sur le fondement d'un traitement algorithmique doit comporter une mention explicite en informant l'intéressé.

Ce nouveau dispositif devrait s'étendre à toutes les personnes, physiques ou morales, ainsi qu'à toutes les décisions administratives individuelles prises sur le fondement d'un traitement algorithmique.

En outre, a également été ajouté au CRPA, un nouvel article visant à la publication des règles définissant les principaux traitements algorithmiques utilisés dans l'accomplissement de leurs missions lorsqu'ils fondent des décisions individuelles.

Les enjeux liés à la notion de redevance

La directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public (dite « **directive PSI** ») avait été transposée par l'ordonnance n° 2005-650 du 6 juin 2005 relative à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques.

Afin de préciser le champ d'application de la directive PSI, d'encadrer le traitement des demandes de réutilisation des informations publiques, ainsi que la mise en place de redevances ou la conclusion d'accords d'exclusivité, la directive 2013/37/UE du Parlement européen et du Conseil a été adoptée par le Parlement européen et le Conseil le 26 juin 2013.

Cette Directive a été transposée par la **loi VALTER** dont la mise en œuvre suscitera des interrogations.

Principales dispositions des directives communautaires

La directive PSI n'a entendu créer aucune obligation pour les États membres d'autoriser la réutilisation de documents et n'a fait que créer des règles minimales s'appliquant lorsque la réutilisation est autorisée. Les redevances pouvant être perçues étaient alors encadrées par la directive.

Le total des recettes provenant de la fourniture et des autorisations de réutilisation des documents ne pouvait alors dépasser les coûts de collecte, de production, de reproduction et de diffusion, tout en permettant un retour sur investissement raisonnable.

La directive 2013/37/UE a entendu modifier ce principe : **désormais lorsqu'une réutilisation est soumise à redevance, cette dernière doit être basée uniquement sur les coûts marginaux de reproduction, de mise à disposition et de diffusion des données.**

Les organismes publics ont la possibilité d'autoriser la réutilisation des documents sans conditions ou peuvent choisir d'imposer des conditions, le cas échéant par le biais d'une licence.

Par ailleurs, plusieurs dispositions de la directive 2013/37/UE imposent aux administrations, un **renforcement de l'obligation de transparence**.

Tel est notamment le cas de l'article 7 de la directive, imposant, en matière de réutilisation des documents détenus par des organismes du secteur public, la communication et la publication, dans la mesure du possible sous format électronique, de la méthodologie utilisée pour la détermination du montant des redevances.

La transposition de la directive 2013/37/UE par la loi VALTER

La loi VALTER du 28 décembre 2015 a consacré en droit français, le **principe de gratuité de l'utilisation et de la réutilisation des informations publiques**, tout en prévoyant deux dérogations.

L'affirmation du principe de gratuité

Depuis plusieurs années, les collectivités territoriales sont conscientes de l'enjeu important que représentent les données publiques et de la nécessité de les mettre gratuitement à disposition d'utilisateurs et de réutilisateurs pour **renforcer la démocratie, développer l'économie et moderniser leur action publique.**

Toutefois, de nombreuses administrations ont tout de même maintenu et/ou institué des redevances de réutilisation.

A titre d'exemple, le tableau ci-dessous synthétise, pour l'année 2012, les recettes tirées des redevances de réutilisation, par type d'administration :

RECETTES TIRÉES DES REDEVANCES DE RÉUTILISATION, PAR SERVICE BÉNÉFICIAIRE

Service bénéficiaire	2012
Institut national de la statistique et des études économiques	9 981 000 €
Institut national de l'information géographique et forestière	9 940 748 €
Ministère de l'Intérieur	3 865 282 €
Institut national de la propriété intellectuelle	2 744 054 €
Ministère économique et financier	1 955 234 €
Météo-France (hors recettes refacturées à sa branche commerciale)	1 585 000 €
Service hydrographique et océanographique de la marine	1 300 000 €
Direction de l'information légale et administrative	892 326 €
Service de l'observation et des statistiques	580 000 €
Agence technique de l'information sur l'hospitalisation	543 719 €
FranceAgriMer	300 000 €
Cour de cassation	264 120 €
Conseil d'État	231 508 €
Office national d'information sur les enseignements et les professions	155 143 €
Ministère de l'éducation nationale	131 091 €
Institut français du cheval et de l'équitation	81 671 €
Institut national de l'origine et de la qualité	79 265 €
Agence de services et de paiement	53 480 €
Ministère de l'agriculture	16 700 €
Commission d'accès aux documents administratifs	5 000 €
TOTAL	**34 705 341 €**

Source : M. Mohammed Adnène Trojette, rapport sur l'ouverture des données publiques, juillet 2013.

On constate néanmoins que depuis plusieurs années, la fixation des redevances a nettement tendance à diminuer.

De nombreuses études, en particulier, le rapport de M. Mohammed Adnène Trojette, « *Ouverture des données publiques, les exceptions au principe de gratuité sont-elles toutes légitimes ?* »[2] ont eu tendance à démontrer que les effets de la gratuité de l'utilisation et de la réutilisation des informations publiques sont, à terme, extrêmement bénéfiques pour la société dans son ensemble.

[2] M. Mohammed Adnène Trojette, rapport au Premier ministre, « Ouverture des données publiques, les exceptions au principe de gratuité sont-elles toutes légitimes ?», juillet 2013.

Dans le prolongement de ces réflexions, le législateur a donc saisi l'occasion de la transposition de la directive 2013/37/UE dans le corpus réglementaire national, en allant au-delà de la stricte transposition et en inscrivant dans la loi, le **principe de gratuité de la réutilisation.**

Les dérogations

Il existe néanmoins **deux dérogations au principe de gratuité** :

D'une part, l'Etat, les collectivités territoriales ainsi que les autres personnes de droit public ou les personnes de droit privé chargées d'une mission de service public peuvent établir une redevance de réutilisation « *lorsqu'elles sont tenues de couvrir par des recettes propres une part substantielle des coûts liés à l'accomplissement de leurs missions de service public.* ».

L'article 5 de la loi, désormais intégré dans l'article L. 324-1 précité du CRPA, prévoit que :

> « *Le produit total du montant de cette redevance, évalué sur une période comptable appropriée, ne dépasse pas le montant total des coûts liés à la collecte, à la production, à la mise à la disposition du public ou à la diffusion de leurs informations publiques.* »

Cette précision signifie que les redevances ne pourront donc plus prendre en compte, comme cela était le cas avant l'entrée en vigueur de la loi VALTER, la rémunération raisonnable des investissements, comprenant, le cas échéant, une part au titre des droits de propriété intellectuelle.

Au cours des débats parlementaires, ce choix a été justifié par le fait qu'une administration n'avait pas pour vocation de générer des bénéfices.

D'autre part, aux termes du nouvel article L. 324-2 du CRPA, la réutilisation peut également donner lieu au versement d'une redevance dans un cas plus spécifique, à savoir :

> « *Lorsqu'elle porte sur des informations issues des* ***opérations de numérisation des fonds et des collections des bibliothèques, y compris des bibliothèques universitaires, des musées et des archives****, et, le cas échéant, sur des informations qui y sont associées lorsque ces dernières sont commercialisées conjointement. Le produit total du montant de cette redevance, évalué sur une période comptable appropriée, ne dépasse pas le montant total des coûts de collecte, de production, de mise à disposition ou de diffusion, de conservation de leurs informations et d'acquisition des droits de propriété intellectuelle.* »

Là encore, il est précisé que les redevances ne pourront donc plus prendre en compte, comme cela était le cas avant l'entrée en vigueur de la loi VALTER, la rémunération

raisonnable des investissements, comprenant, le cas échéant, une part au titre des droits de propriété intellectuelle.

Dans les deux cas, le montant de la redevance doit être fixé selon des **critères objectifs, transparents, vérifiables et non discriminatoires.**

Il peut faire l'objet d'une révision de ces montants au moins tous les cinq ans.

Les interrogations suscitées par la loi VALTER

Il est regrettable que le sujet des conditions financières de réutilisation des informations publiques n'ait pas été traité dans le cadre de la loi pour une République numérique.

Le manque de précisions, tant dans la loi que dans les travaux parlementaires, sur les modalités de mise en œuvre des redevances traduit la rapidité avec laquelle le Parlement a dû traiter un sujet aussi majeur.

En effet, comment interpréter la notion ***« part substantielle des coûts liés à l'accomplissement de leurs missions de service public » ?***

Comment calculer le montant total des coûts ***« liés à la collecte, à la production, à la mise à la disposition du public ou à la diffusion de leurs informations publiques » ?***

Alors que le rapport Trojette précité incitait l'Etat à engager une réflexion sur les ***« modèles économiques »*** qui pourraient être envisagés pour les administrations, ni la loi VALTER, ni la loi pour une République numérique n'en font mention.

Pourtant, et comme le relevait Monsieur Trojette dans son rapport, « *les opérateurs dont la mission même est de produire des données doivent rechercher des modèles économiques leur permettant de faire face à un paysage économique en profonde reconstitution* ».

Ainsi, en l'absence de précisions du législateur, il appartiendra donc aux collectivités territoriales de rechercher des modèles stimulant l'innovation autour de leurs données, à la fois pour les entrepreneurs innovants, mais également pour les citoyens eux-mêmes.

La cyberdéfense : nouvel enjeu de sécurité nationale

Afin de profiter des progrès des technologies de l'information et de la communication, les **infrastructures critiques** reposent de plus en plus sur des systèmes d'informations complexes et se sont largement connectés à des réseaux publics.

Ces interconnexions rendent les infrastructures interdépendantes et les exposent à l'ensemble des vulnérabilités des systèmes informatiques.

Présentation du programme PEPIC

Le Programme européen pour la protection des infrastructures critiques (**programme PEPIC**), lancé en 2004 par le Conseil européen, vise à identifier et à protéger les infrastructures critiques, entendues comme **toute sorte d'infrastructure (y compris les services), considérée comme essentielle au fonctionnement de l'économie et de la société.**

Plus précisément, il s'agit des **installations physiques, technologies de l'information, réseaux, services et actifs qui, en cas d'arrêt ou de destruction, peuvent avoir de graves incidences sur la santé, la sécurité ou le bien-être économique des citoyens ou encore le travail des gouvernements des Etats membres.**

Indispensables au bon fonctionnement de l'Etat dans son ensemble, elles constituent des cibles privilégiées.

Il s'agit notamment des infrastructures relatives à :

- La distribution d'énergie électrique (auprès d'autres infrastructures : hôpitaux, etc.) ;
- La production d'énergie électrique en particulier nucléaire ;
- Des réseaux d'alimentation et de production des raffineries ;
- La distribution et production d'eau douce ;
- Les réseaux de transport (réservations billets d'avions, contrôle aérien, réseaux de signalisation des voies ferrées, etc.) ;
- Les réseaux de communication (téléphone filaire, cellulaires, réseau Internet, etc.), y compris ceux des forces de police et de la défense.

L'objectif du programme PEPIC était alors de fixer un cadre commun, au niveau de l'Union européenne, pour la **protection des infrastructures critiques** en Europe afin de s'assurer que tous les États membres offrent des niveaux de protection suffisants de ces infrastructures.

Dans ce cadre, la Commission s'est ainsi vue confier la tâche de :

- Recenser et diffuser les informations relatives aux meilleures pratiques en matière de protection de ces infrastructures,
- Adopter des normes communes au niveau de chaque secteur,
- Evaluer les menaces et les risques.

Il en résulte un cadre réglementaire composé des éléments suivants :

- Une procédure pour l'identification et la désignation des infrastructures critiques européennes et une approche commune pour évaluer le besoin d'amélioration de leur sécurité ;
- Des mesures destinées à faciliter l'amélioration du programme incluant un **plan d'action, un réseau d'alerte concernant les infrastructures critiques (CIWIN),** l'établissement de groupes d'experts de la **protection des infrastructures critiques (PIC)** au niveau de l'UE, des procédures de partage d'informations concernant la PIC et l'identification et l'analyse des liens de dépendance ;
- Un soutien aux États membres en ce qui concerne la sécurité des infrastructures critiques nationales, sur leur demande et des plans d'intervention ;
- Une dimension extérieure ;
- Des mesures financières d'accompagnement, et en particulier le programme spécifique « *Prévention, préparation et gestion des conséquences en matière de terrorisme et autres risques liés à la sécurité* » de l'UE, qui fournira des opportunités de financement pour les mesures liées à la protection des infrastructures critiques.

Tout en gardant à l'esprit que la protection des infrastructures critiques nationales incombe aux acteurs nationaux (propriétaires, exploitants, États membres eux-mêmes), la Commission prévoit néanmoins un soutien en la matière, à la demande des États.

Chaque État membre est, par ailleurs, encouragé à établir son **programme national de protection** incluant les éléments suivants :

- Le classement des infrastructures, tenant compte des effets suivant l'arrêt ou la destruction de chaque infrastructure (ampleur de la zone géographique touchée et gravité des conséquences) ;
- Le recensement des liens de dépendance géographique et sectorielle ;
- L'établissement de plans d'intervention.

Le cadre juridique national

Si l'Etat français a atteint un haut degré dans la diffusion et l'usage des **systèmes d'informations**, il n'a sans doute pas accordé suffisamment d'importance à la sécurité de ces systèmes.

Les entreprises et les grands opérateurs nationaux demeurent encore insuffisamment sensibilisés à la menace liée aux attaques contre les systèmes d'information.

Ce constat, dressé par le rapport Lasbordes en 2006[3], reste encore largement d'actualité.

Or, **face à l'espionnage informatique, la problématique de la sécurité des systèmes d'information des entreprises - et notamment de celles des secteurs jugés stratégiques - représente un enjeu majeur.**

Seuls douze secteurs d'importance vitale ont été identifiés, regroupant environ deux cents trente opérateurs ou entreprises, issus du secteur public ou du secteur privé.

Enfin, reste la question centrale des **opérateurs d'importance vitale.**

Indispensables au bon fonctionnement du pays, les opérateurs d'importance vitale représentent aujourd'hui des cibles particulièrement vulnérables aux attaques informatiques. La principale difficulté tient cependant à leur très grande diversité.

On constate, en effet, de fortes différences entre les secteurs concernés, qu'il s'agisse de l'existence ou non d'une autorité de régulation, de la réglementation applicable ou encore des relations entretenues avec la puissance publique.

Ainsi, dans certains secteurs, à l'image du secteur bancaire, de l'aviation civile ou encore de l'énergie nucléaire, les préoccupations de sécurité sont majeures et l'autorité de régulation joue un rôle important.

Mais il n'en va pas de même dans tous les secteurs.

L'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI), autorité nationale compétente en matière de sécurité et de défense des systèmes d'information, assiste les administrations et les opérateurs d'importance vitale. Elle est chargée de la promotion des technologies, des systèmes et des savoir-faire nationaux. Elle contribue au développement de la confiance dans le numérique.

Or, l'ANSSI n'a pas les moyens d'assurer la protection de tous les opérateurs d'importance vitale et il est donc indispensable d'encourager les opérateurs, sur une base sectorielle, à renforcer les mesures de protection de leurs systèmes d'information.

De nombreux pays, à l'image des Etats-Unis ou de l'Allemagne, ont fait de la protection des infrastructures d'importance vitale une priorité nationale. Or, dans ce domaine, la France accuse encore un réel retard par rapport à nos principaux alliés et partenaires.

De l'aveu même de l'Agence, les échanges avec les opérateurs d'importance vitale demeurent très limités.

Par ailleurs, en raison de leur diversité, la protection des systèmes d'information n'est clairement pas une priorité pour la plupart de ces opérateurs.

---

[3] Rapport intitulé « *La sécurité des systèmes d'information - Un enjeu majeur pour la France* », Pierre Lasbordes, remis au Premier ministre Dominique de Villepin le 13 janvier 2006.

Surtout, la plupart des opérateurs d'importance vitale ne sont pas organisés pour répondre efficacement à un grave incident informatique et l'ANSSI n'a pas les moyens de faire face à une crise générale paralysant un secteur entier du pays.

Enfin, la France ne dispose pas de capacités de protection et de systèmes permanents de détection des attaques informatiques à l'entrée des réseaux des opérateurs d'importance vitale.

A ce jour, il apparaît donc indispensable de faire de cette question une priorité nationale.

L'État a la responsabilité, en relation avec les représentants des secteurs stratégiques économiques, de la protection de ces infrastructures vitales.

Le pilotage général de la protection des infrastructures vitales est aujourd'hui confié au **Secrétariat général de la défense et de la sécurité nationale**, avec un rôle particulier pour le **Centre Opérationnel de la Sécurité des Systèmes d'Information (COSSI).**

Le COSSI assure la mise en œuvre de la fonction d'autorité de défense des systèmes d'information dévolue à l'ANSSI. Son action s'exerce en priorité au profit des administrations de l'État et des opérateurs d'importance vitale.

Un des objectifs de ce nouveau dispositif consiste à parvenir à un nombre de points d'importance vitale sensiblement inférieur à celui des actuelles installations et points sensibles, afin de mieux les protéger.

L'insuffisante sensibilisation des collectivités territoriales en matière de sécurité informatique

Les collectivités territoriales n'ont pas encore suffisamment pris conscience de la nécessité de sécuriser leurs systèmes d'informations, alors même qu'elles sont bien évidemment des cibles potentielles.

A ce jour, un faible nombre de collectivités a organisé des formations pour sensibiliser les agents et moins de 15% d'entre-elles ont admis ne pas avoir pris connaissance du **Référentiel Général de Sécurité (RGS) de l'ANSSI,** cadre réglementaire permettant d'instaurer la confiance dans les échanges au sein de l'administration avec les citoyens, auquel les collectivités territoriales doivent pourtant se conformer, depuis mai 2013, en ce qui concerne les certificats électroniques.

Par ailleurs, aucune d'entre elles n'a encore eu recours au chiffrement des données.

Lors d'un colloque organisé le 16 mars 2016 par la **Mission Ecoter**, association ayant en charge le développement des systèmes de communication et d'information dans les collectivités territoriales, les intervenants ont pris le temps d'expliquer que les collectivités territoriales étaient bien des cibles potentielles d'attaques, contrairement à ce que beaucoup d'entre elles tendent à penser.

Ces offensives pourraient pourtant déboucher sur la perte de données sensibles.

Primo France, association dédiée à la gouvernance et à la gestion du risque public, a conduit une enquête portant sur l'exposition des collectivités publiques locales au **cyber risque**, laquelle a conclu aux enseignements suivants :

- Les directeurs généraux des services, par leur vision transversale, restent les acteurs les plus impliqués en matière de gestion des risques ;
- Malgré une sensibilité aux risques qui ne cesse de croître, les mécanismes mis en place pour la gestion des cyber risques demeurent insuffisants ;
- L'exposition croissante des collectivités aux cyber risques est due, d'une part, à l'augmentation des accès connectés en interne et en externe (guichet unique, sites des collectivités, données sensibles, etc.) et, d'autre part, à la montée d'un **cyber terrorisme**, idéologique ou purement mercenaire ;
- L'achat d'assurances reste encore un outil de protection peu utilisé par les collectivités qui appréhendent surtout des freins politiques, techniques et réglementaires liés à sa mise en œuvre.

Pour anticiper les problèmes, l'ANSSI a mis en place une démarche d'homologation en neuf étapes permettant aux collectivités territoriales de sécuriser leurs systèmes d'information.

Ce processus assez lourd doit impérativement être adapté aux enjeux, au contexte d'emploi, à la nature des données et aux utilisateurs.

Le constat est néanmoins bien présent : **les collectivités peinent à atteindre un niveau minimal de protection de leurs données, et sont, de fait, mal préparées aux futures révolutions apportées par le guichet unique et la ville connectée.**

Les acteurs privés du secteur informatique poussent à centraliser les données, tout en les délocalisant (Cloud, gestion électronique à distance, etc.), envoyant ainsi des signaux contradictoires et exposant les collectivités locales à un risque accru, nécessitant la **mise en place d'une couverture efficace afin de réduire les conséquences néfastes d'une cyber-attaque.**

Proposition de clausier type : éléments susceptibles d'être intégrés au sein des contrats de la commande publique

Il appartient aujourd'hui aux collectivités territoriales de décider du degré de contrôle qu'elles souhaitent exercer sur la **gestion des données des services publics délégués**, en particulier.

Eléments de contexte

Ces dernières années, les collectivités locales ont rencontré des difficultés pour récupérer les données de leurs services publics.

En effet, il n'est pas toujours aisé pour les collectivités territoriales d'obtenir de la part de leurs partenaires privés, l'ensemble des informations relatives aux services qu'elles délèguent, lesquelles ne sont en général pas accessibles « en ligne ».

Or, l'exploitation d'une concession donne aujourd'hui lieu à la production d'un volume croissant de données, en particulier dans des domaines tels que celui de l'eau ou des transports.

Au vu de ce constat, il est plus qu'indispensable, pour chaque collectivité, de pouvoir disposer de ces données, afin d'en assurer la mise à disposition d'une part, et afin de pouvoir assurer efficacement le suivi, l'évolution mais surtout le renouvellement des contrats en cause d'autre part.

Articulation du dispositif de protection des données personnelles avec celui institué dans le cadre des contrats de concession

La notion de données à caractère personnel telle que réglementée par les dispositions de la loi CNIL semble constituer une limite juridique qui interdit, sauf consentement de l'intéressé, fondement légal ou anonymisation, la communication ou la réutilisation des données.

En effet, le **dispositif de protection des données personnelles** se préoccupe peu des relations susceptibles d'exister entre la personne publique et le concessionnaire.

En outre, le droit pénal constitue un obstacle supplémentaire en ce que la **responsabilité pénale** ne saurait se transférer ou se déléguer.

Il convient donc de s'interroger sur le lien contractuel qui pourrait être institué, avant la conclusion du contrat entre le concessionnaire et le concédant, et sur le niveau de responsabilité qui pourrait être mis à la charge de l'administration en sa qualité de **responsable de traitement.**

En réalité, il conviendrait d'établir un lien entre le fait que la collectivité reste toujours responsable de l'organisation de son service public et qu'elle ne se contente que d'en déléguer la gestion, conformément à l'esprit même d'une convention de concession.

En tout état de cause, ces difficultés pourraient être réduites si l'administration acceptait de prendre l'engagement de s'assurer du respect des dispositions de la loi CNIL, au risque de se voir suspendre son droit de réutilisation, et acceptait de supprimer ou de demander le rapatriement du jeu de données au profit du concessionnaire, s'il s'avérait qu'il présente un risque pour le respect de la vie privée.

Types de clauses susceptibles d'être insérées dans les contrats publics

La nécessité pour les collectivités territoriales d'insérer, dans leurs contrats, des **clauses relatives à la gestion des données et bases de données collectées ou produites à l'occasion de l'exécution du contrat** s'avère aujourd'hui nécessaire.

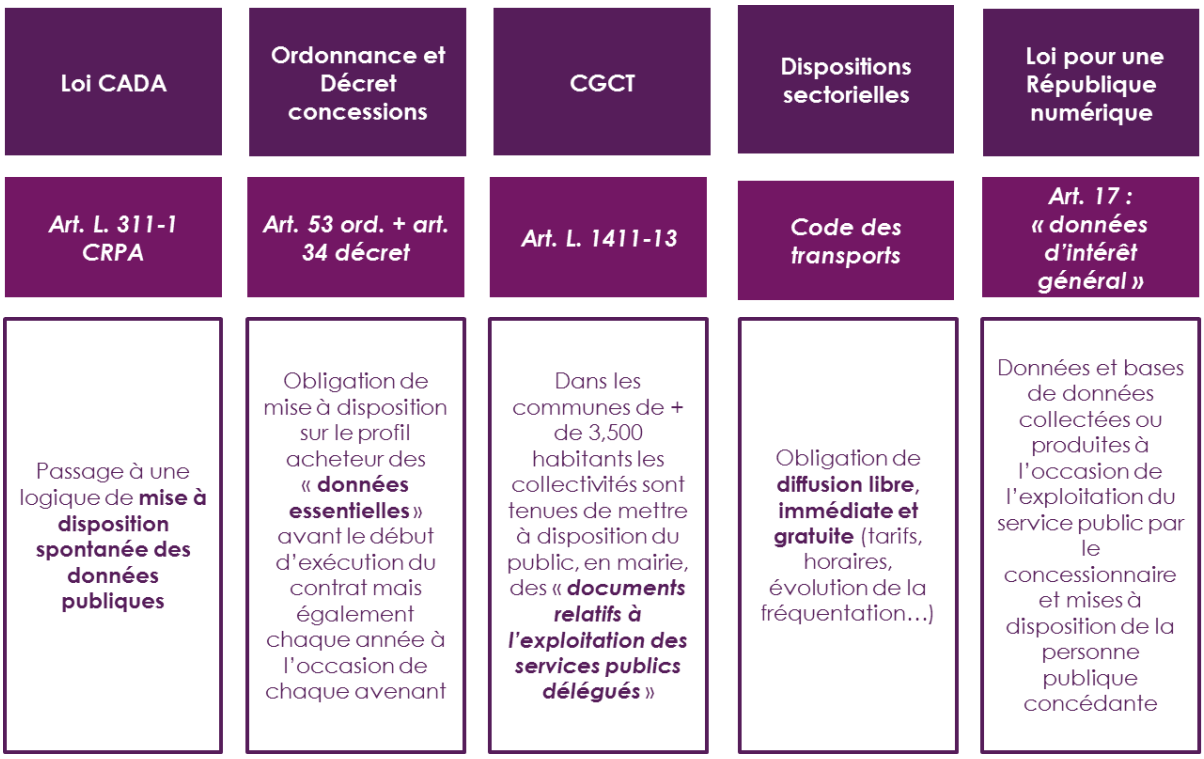
Il convient à cet égard de distinguer, les types de clauses qui pourraient être introduites selon qu'elles ont vocation à régir :

- Les modalités d'ouverture et de mise à disposition des données à destination des administrés ;
- Le régime de propriété des données ;
- La responsabilité liée au traitement desdites données.

Modalités d'ouverture et de mise à disposition des données à destination des administrés

Si le législateur s'est engagé dans une politique volontariste d'ouverture des données publiques allant même, dans le cadre de la loi pour une République numérique, à instituer une **obligation pour les administrations de mettre à disposition les données qu'elles détiennent,** ces obligations se trouvent plus particulièrement renforcées dans le cadre des contrats publics et, en particulier, des concessions.

Or, il a déjà été rappelé ci-avant que l'étude approfondie des différents textes, fait ressortir un **empilement des différentes obligations dans des textes divers**, rendant ainsi la réglementation quelque peu illisible, du moins difficile à mettre en œuvre :



Dans ce contexte, il appartiendra aux collectivités territoriales de s'interroger sur les **modalités de mise en œuvre des nouvelles obligations d'open data** qui ont été mises à sa charge, d'autant plus que souvent, les différents échelons de collectivités territoriales n'ont pas tous appréhendé, dans la même mesure, ces nouvelles obligations.

Une fois que les collectivités territoriales auront en quelque sorte défini leur « **politique en matière d'open data** », et dès lors que les dispositions de la loi CNIL seront respectées, il pourra être inscrit dans les contrats que **toutes données, produites ou reçues dans le cadre de son exécution, pourront être mises à la disposition du public dans les conditions définies par la personne publique et après avoir recueilli son accord préalable.**

Le régime de propriété des données

Il nous semble important qu'il soit désormais prévu, dès le lancement d'une procédure de passation d'un contrat public, que **la collectivité souhaite être propriétaire de toutes les données et bases de données nécessaires à l'exploitation du service public.**

Pour ce faire, il appartient aux collectivités d'inscrire au sein de leurs contrats que lesdites données relèvent de la catégorie juridique des **« biens de retour ».**

Pour rappel, les biens de retour correspondent aux biens affectés au service public et nécessaires à son exploitation et qui sont considérés comme étant, dès leur acquisition ou

leur réalisation, propriété de la personne publique, et ce, même dans les cas où ils ont été financés par le concessionnaire.

Aussi, il conviendrait d'indiquer expressément dans les futurs contrats que l'ensemble des données et bases de données produites ou reçues par le concessionnaire dans le cadre des missions qui lui ont été confiées, constituent des **biens de retour dès lors qu'ils sont par ailleurs nécessaires à la continuité du service public.**

Il pourrait être par ailleurs envisagé que soient consenties au concessionnaire des **licences non exclusives d'exploitation de ces bases de données** pour toute la durée du contrat.

La responsabilité liée au traitement des données

Afin que les collectivités locales disposent d'un pouvoir de contrôle plus étendu sur la gestion de l'ensemble des données du service public, elles ont la possibilité de revêtir la qualité de **« responsable de traitement »** au sens des dispositions de l'article 3 de la loi CNIL, lequel définit le responsable de traitement comme étant ***« sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens ».***

En l'occurrence, dès lors que la collectivité concédante détermine les finalités et les moyens de mise en œuvre du traitement des données du service, elle nous semble pouvoir être considérée comme le responsable du traitement correspondant et assumer à ce titre, l'ensemble des obligations prescrites par la loi CNIL, mais également les responsabilités civiles et pénales qui en découlent.

Dans l'hypothèse où la collectivité serait considérée comme responsable du traitement, il reviendrait alors au concessionnaire, en qualité de **« sous-traitant »** au sens des dispositions de la loi CNIL, d'assurer la confidentialité et la sécurité des données du service, conformément aux engagements qui seront inscrits dans le contrat pour la couverture des risques résiduels. En sa qualité de sous-traitant, le concessionnaire ne pourrait alors agir que sur instruction de la personne publique.

En effet, il sera rappelé qu'aux termes de l'article 35 de la loi CNIL, un sous-traitant est défini comme ***« toute personne traitant des données à caractère personnel pour le compte du responsable des traitements ».***

Dès lors, lorsqu'un traitement est sous-traité à un prestataire externe, ledit prestataire ne devient pas le responsable du traitement pour autant, étant donné que seul ledit responsable de traitement conserve toute la responsabilité du traitement aux yeux de la loi.

Ainsi, au regard de ces différents éléments, il appartiendra aux collectivités territoriales, compte tenu des conséquences attachées en termes de responsabilité à la qualité de responsable de traitement, de décider d'inscrire ou non un tel principe dans le projet de convention de concession, en cours de négociation.

Synthèse : schéma récapitulatif des différents types de clauses susceptibles d'être introduites au sein des contrats de concession

Liste des principaux textes examinés dans le cadre du présent document

Textes communautaires :

- Directive 2013/37/UE modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public ;
- 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 et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

Textes nationaux :

- Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite « loi CNIL » ;
- Loi n°78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal dite « loi CADA » ;
- Loi n°79-18 du 3 janvier 1979 sur les archives ;
- Décret n°2005-1755 du 30 décembre 2005 relatif à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques, pris pour l'application de la loi n° 78-753 du 17 juillet 1978 ;
- Ordonnance n° 2015-899 du 23 juillet 2015 relative aux marchés publics ;
- Loi n° 2015-912 du 24 juillet 2015 relative au renseignement ;
- Loi n° 2015-990 du 6 août 2015 pour la croissance, l'activité et l'égalité des chances économiques, dite « loi MACRON » ;
- Loi n° 2015-991 du 7 août 2015 portant nouvelle organisation territoriale de la République, dite « loi NOTRe » ;
- Loi n° 2015-992 du 17 août 2015 relative à la transition énergétique pour la croissance verte, dite « loi TECV » ;
- Loi n° 2015-1779 du 28 décembre 2015 relative à la gratuité et aux modalités de la réutilisation des informations du secteur public, dite « loi VALTER » ;
- Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé ;
- Ordonnance n° 2016-65 du 29 janvier 2016 relative aux contrats de concession ;
- Décret n° 2016-86 du 1er février 2016 relatif aux contrats de concession ;
- Décret n° 2016-360 du 25 mars 2016 relatif aux marchés publics ;
- Loi n°2016-1321 du 7 octobre 2016 pour une République numérique.

Glossaire

ANSSI : Agence Nationale de Sécurité des Systèmes d'Information

CADA : Commission d'Accès aux Documents Administratifs

CGCT : Code général des collectivités territoriales

CIWIN : Réseau d'alerte concernant les infrastructures critiques (en anglais *Critical Infrastructure Warning Information Network)*

CNIL : Commission Nationale de l'Informatique et des Libertés

COSSI : Centre Opérationnel de la Sécurité des Systèmes d'Information

CRPA : Code des relations entre le public et l'administration

Directive PSI : Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 sur la réutilisation des informations du secteur public (en anglais, *Public Sector Information directive*)

Loi CADA : Loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal

Loi CNIL : Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Loi NOTRe : Loi n° 2015-991 du 7 août 2015 portant nouvelle organisation territoriale de la République

Loi VALTER : Loi n° 2015-1779 du 28 décembre 2015 relative à la gratuité et aux modalités de la réutilisation des informations du secteur public

Mission ECOTER : Association ayant en charge le développement des systèmes de communication et d'information dans les collectivités territoriales

PIC : Protection des infrastructures critiques

Primo France : Association dédiée à la gouvernance et à la gestion du risque public

Programme PEPIC : Programme européen pour la protection des infrastructures critiques

RGS : Référentiel Général de Sécurité de l'ANSSI