

Charte métropolitaine de la donnée

Un cadre éthique pour protéger les citoyens
et réguler l'utilisation des données sur le territoire

Protection

Confiance

Sobriété



Johanna ROLLAND
Maire de Nantes
Présidente de Nantes Métropole



PRÉAMBULE

Les données sont de plus en plus présentes dans nos vies quotidiennes. Elles sont produites et collectées en masse dans toutes nos activités. Chacun est concerné comme **citoyen, salarié, usager de services publics ou privés. La gestion des villes n'échappe pas à cette évolution.**

Des données sont aujourd'hui produites en grand volume par la gestion des services publics, par des opérateurs de mobilité, des distributeurs d'énergie, des gestionnaires de déchets et bien d'autres. En 2020, le volume des données produites en une seule journée pour la gestion des villes européennes, sera 4 fois supérieur à celui des données produites pour toute l'année 2015.

Maîtriser et contrôler la gestion qui est faite de ces données est indispensable car cette nouvelle étape de la transition numérique des territoires pose des enjeux juridiques, économiques et éthiques.

Plusieurs grandes collectivités dans le monde comme Boston, Montréal, Amsterdam, Barcelone s'en sont saisies. Chacune imagine **des dispositifs pour que la puissance publique encadre la façon dont les données de leurs habitants sont utilisées.**

Nantes Métropole a fait le choix d'élaborer une charte métropolitaine de la donnée qui pose des principes rigoureux et éthiques pour **protéger les citoyens et encadrer les usages de la donnée sur le territoire.**

Ce choix est le **fruit d'une histoire et d'une méthode.** Le dialogue entre la société civile et la collectivité s'est développé depuis plusieurs années autour du numérique et des enjeux relatifs à la donnée. Il s'est notamment traduit par une participation active d'habitants, de collectifs, de partenaires à des démarches de dialogue citoyen comme par exemple « *WiFi public : quel internet pour tous sur l'espace public ?* », « *Construisons ensemble les règles du jeu des rues connectées de l'île de Nantes* ».

Lors de ces démarches, une diversité de points de vue a été exprimée sur les usages de la donnée comme levier de la participation, l'accès à une information claire et instantanée, un besoin de pédagogie et de transparence concernant la sécurité et la protection des données personnelles.

Ces engagements, la collectivité les prend d'abord pour elle-même. Ils s'appliquent aussi aux acteurs publics et privés qui œuvrent dans le cadre de ses activités de service public.

La collectivité s'engage également à **mettre en place un cadre de dialogue avec les acteurs qui interviennent sur l'espace public afin de créer les conditions d'un accès à ces données au service de l'intérêt général.**

Protection Confiance **Sobriété**

Les valeurs de la charte métropolitaine de la donnée

- > **CONFIANCE et ÉTHIQUE** pour la protection des données des citoyens et les usages de la donnée au service de l'intérêt général ;
- > **TRANSPARENCE** des politiques publiques, pour rendre compte, au service de la vie démocratique ;
- > **SOBRIÉTÉ et TRANSITION ENERGETIQUE** dans la collecte et la conservation des données pour contrôler et limiter les effets liés à la consommation énergétique des données massives ;
- > **INNOVATION** pour susciter et animer l'expérimentation de nouveaux usages au service des citoyens ;
- > **COLLABORATION** pour créer des espaces de dialogue sur le territoire et avancer collectivement sur ces enjeux complexes.

Les 4 engagements de la collectivité

- > Engagement 1 : **Garantir la souveraineté de la collectivité sur ses données**
- > Engagement 2 : **Protéger les données**
- > Engagement 3 : **Garantir la transparence**
- > Engagement 4 : **Favoriser de nouveaux usages**



© Philippe Delarue / La Ville de Nantes

ENGAGEMENT 1

Garantir la souveraineté sur les données du service public

Principe 1 | Données publiques

La mise en œuvre des missions de service public nécessite l'utilisation de données nombreuses. Les données produites, collectées, traitées ou gérées par la collectivité ou par un tiers intervenant pour son compte dans le cadre de ses activités de service public et en lien avec ses compétences, ont le statut de « données publiques ». **Elles constituent un patrimoine qui est un bien public.**

Principe 2 | Propriété des données publiques



Les données publiques sont propriété de la collectivité. **La collectivité est garante de leur utilisation et à ce titre elle se doit de définir les droits d'usage qui peuvent être accordés à des tiers.**

Ce principe ne s'applique pas aux **données personnelles dont la propriété est inaliénable** et reste celle des citoyens.

Principe 3 | L'hébergement des données publiques



Face aux enjeux de sécurité et de souveraineté des données liées à la gestion des services publics, la collectivité fixe les règles d'hébergement de ses données.

Afin de garantir la sécurité de ses données les plus sensibles, la collectivité impose leur hébergement en France. Les autres données publiques sont hébergées en France ou dans l'Union Européenne.

La collectivité s'inscrit dans la démarche engagée par l'État pour définir une doctrine pour un hébergement souverain.

Principe 4 | Données d'intérêt métropolitain



Des acteurs divers interviennent dans la vie du territoire métropolitain et sont susceptibles de produire **des données qui revêtent un caractère d'intérêt général.**

Certaines sont produites par des acteurs publics (services de l'Etat, collectivités territoriales, entreprises publiques ou délégataires de l'Etat...), d'autres sont produites par des acteurs privés.

Lorsqu'il est de l'intérêt de tous qu'elles soient partagées avec la puissance publique parce qu'elles peuvent contribuer utilement à la connaissance des dynamiques du territoire et à la mise en œuvre des politiques publiques, **la collectivité propose un cadre de dialogue avec les acteurs concernés pour créer les conditions d'un accès à ces données respectueux des droits de tous. Ces données sont dites d'intérêt métropolitain.**



© Valéry Jorret



ENGAGEMENT 2

Protéger les données

Principe 5 | La protection des données personnelles

La législation européenne (Règlement Général de Protection des Données Personnelles - RGPD) et la loi française (loi Informatique et Libertés de 1978 modifiée par le RGPD) **imposent aux entreprises comme aux acteurs publics un cadre qui protège de manière renforcée les données personnelles des Européens**. Ce cadre est entré en application le 25 mai 2018.

La collectivité applique ces règles pour ses propres services et veille également à leur respect par les entreprises qui travaillent pour son compte. Afin de garantir le niveau le plus élevé de protection des données des citoyens, la collectivité intègre des **clauses de protection des données personnelles dans ses marchés publics comme dans ses contrats** dès lors que les projets soutenus impliquent la collecte et le traitement de données personnelles.

La collectivité s'engage à **favoriser les initiatives visant à renforcer la compréhension et la connaissance par les citoyens de leurs nouveaux droits créés par la législation sur la protection des données** (modalités de recueil du consentement, droit à l'oubli et effacement des données, portabilité des données...).

Principe 6 | La sécurité des systèmes d'information

La protection des systèmes d'information de la collectivité permet de **garantir la sécurité des données des citoyens, de se prémunir des attaques extérieures, d'éviter les risques de perte ou de divulgation des données et de garantir la continuité du service public**.

La collectivité met en place des mesures certifiées pour assurer la résistance de ses systèmes d'information et maintenir la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées et collectées par elle.

Principe 7 | La sobriété dans la collecte et la conservation des données

Les nouveaux outils de collecte et de traitement multiplient les possibilités d'exploiter des données de plus en plus massives. La collectivité adopte un principe de sobriété. **Elle collecte les données uniquement nécessaires à l'accomplissement de ses missions de service public et en limite le stockage.**

La durée de conservation de toutes les données, personnelles ou non, est déterminée en fonction de leur nature et de l'objectif poursuivi (à l'exception des données conservées et archivées à des fins de recherche scientifique ou historique).



ENGAGEMENT 3

Garantir la transparence

Principe 8 | Ouverture des données publiques

L'ouverture des données publiques par la collectivité répond à trois objectifs prioritaires : **contribuer à la transparence de la vie publique, alimenter le dialogue citoyen et créer les conditions du développement de nouveaux services.**

La collectivité s'engage à ce que les **données publiques de la collectivité soient accessibles gratuitement sur le portail <https://data.nantesmetropole.fr>** en consultation et en téléchargement.

Les données mises à la disposition du public excluent les données protégées par la loi (données personnelles, données d'entreprises relevant du secret industriel ou commercial, données couvertes par des droits d'auteur).

La collectivité privilégie l'utilisation d'une licence d'utilisation des données qui permet l'usage le plus large des données ouvertes. Elle se réserve le droit d'appliquer des restrictions pour protéger l'intérêt général et limiter des utilisations de données qui iraient à l'encontre des politiques publiques du territoire.

Principe 9 | Publication et transparence des algorithmes

Pour mettre en œuvre ses missions de service public, **la collectivité utilise des outils de calculs automatisés, par exemple pour définir des droits, calculer une aide ou établir une facture.**

La collectivité garantit la protection des droits des citoyens et s'engage pour une **transparence de l'utilisation des algorithmes**. Dans le respect des droits des éditeurs, elle publie le code informatique des algorithmes entraînant une prise de décision individuelle automatisée.

ENGAGEMENT 4

Favoriser de nouveaux usages

Principe 10 | Expérimentations

La collectivité soutient et favorise les innovations et les expérimentations dans différents domaines (transports, énergie, éclairage public, habitat...).

La collectivité et les acteurs du projet s'engagent par un protocole à définir ensemble les conditions de la mise en œuvre des expérimentations, de leur évaluation et de leur déploiement. Ce protocole s'inscrit dans les principes de la charte.

Dans l'hypothèse où une expérimentation nécessiterait de déroger à l'un ou l'autre de ces principes, le protocole encadrera la dérogation. Il limitera notamment la durée de conservation des données.

Ces principes sont applicables à toute expérimentation conduite par des acteurs, publics ou privés, intervenant sur l'espace public métropolitain.

Principe 11 | Intelligence artificielle



Dans l'avenir, il est possible que des outils d'intelligence artificielle accompagnent les acteurs publics dans leurs missions. Dans ce cadre, **la collectivité anticipe et fixe des principes éthiques et protecteurs.** Elle régule les expérimentations en imposant le respect de règles rigoureuses et responsables partagées avec les acteurs nantais du collectif NaonedIA en faveur d'une intelligence artificielle responsable.

La collectivité s'interdit et interdit aux acteurs publics et privés agissant pour son compte, toute utilisation de l'intelligence artificielle pour des décisions individuelles concernant les usagers des services publics.

MODALITÉS DE MISE EN ŒUVRE

Principes d'action

Principe 12 | Mise en œuvre et évaluation de la charte

Il appartiendra aux parties prenantes (la collectivité, les acteurs publics et privés engagés dans la mise en œuvre des politiques publiques et les autres partenaires qui souhaitent s'engager) d'organiser les conditions d'application des principes et d'en garantir un suivi transparent et public.

Principe 13 | Présentation d'un rapport annuel

Un rapport public est présenté chaque année pour dresser un état des lieux et assurer le suivi de la mise en œuvre de la charte.

Ce rapport détaille les modalités d'application des obligations légales ayant trait à la protection des données personnelles des citoyens.

GLOSSAIRE

ALGORITHME

Désigne une suite de calculs nécessaires pour effectuer une opération complexe.

Un algorithme informatique est la description dans un langage formel (un langage de programmation) d'une suite finie et ordonnée de processus qui, à partir de données en entrée, livre des données en sortie en un temps fini, en vue d'un objectif prédéterminé.

CITOYEN

Désigne chaque personne concernée par la gestion de ses données personnelles par la collectivité ou ses opérateurs sur le territoire métropolitain. Le terme citoyen rassemble les multiples dimensions que peut revêtir la relation personnelle de chacune et chacun au territoire et à l'action publique : habitant, usager, bénéficiaire, client, électeur...

CYBERSÉCURITÉ

Désigne l'état recherché pour un système d'information lui permettant de résister à des événements issus du cyberspace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.

DONNÉE

Une donnée est une information stockée dans un format qui permet son utilisation par un programme. Par exemple, si l'on souhaite des informations sur l'âge des habitants d'un quartier, les données seront les âges disponibles (ou les dates de naissance) des habitants du quartier. Les données peuvent prendre de nombreuses formes : des chiffres, du texte (par exemple des couleurs), des coordonnées géographiques...

DONNÉES À CARACTÈRE PERSONNEL

Désigne aux termes de l'article 2 de la Loi Informatique et Libertés : *« 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. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne ».*

DONNÉES D'INTÉRÊT MÉTROPOLITAIN

Désigne toutes les données publiques ou privées dont l'intérêt général sur le territoire de la métropole justifie que la collectivité puisse y avoir accès.

DONNÉES PUBLIQUES

Désigne l'ensemble des données produites ou collectées par la collectivité ou les opérateurs intervenant pour son compte, dans le cadre de ses activités de service public.

DONNÉES OUVERTES (OU OPEN DATA)

Désigne les données qu'un organisme met à la disposition de tous sous forme de fichiers numériques afin de permettre leur réutilisation. La loi pour une République Numérique votée en 2016 a notamment pour objectif de favoriser une politique d'ouverture des données et des connaissances, dans un objectif de transparence ou afin de permettre leur réutilisation, notamment à des fins économiques.

EXPÉRIMENTATION

Désigne tout dispositif ayant pour objet de tester des produits, des usages ou des services innovants qui pourraient correspondre aux besoins du territoire métropolitain ou des Nantais.

INTELLIGENCE ARTIFICIELLE

Désigne l'ensemble des théories et des techniques développant des programmes informatiques complexes capables de simuler certains traits de l'intelligence humaine (raisonnement, apprentissage...) et notamment des algorithmes susceptibles de réviser eux-mêmes les règles qu'ils appliquent pour améliorer leur performance.

LOI INFORMATIQUE ET LIBERTÉS

Désigne la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, aujourd'hui complétée par le Règlement Général sur la Protection des Données Personnelles.

LOI POUR UNE RÉPUBLIQUE NUMÉRIQUE

Désigne la loi n°2016-1321 du 7 octobre 2016 pour une République numérique également appelée « Loi Lemaire ».

PARTENAIRES

La présente charte entend comme partenaires de la collectivité les différents acteurs qui agissent sur le territoire quel que soit leur statut. Certains partenaires ont un statut public, d'autres un statut privé. Certains agissent dans le cadre d'une délégation de service public ou d'une concession, d'autres interviennent au titre d'un partenariat privé.

RESPONSABLE DE TRAITEMENT

Désigne aux termes de l'article 3 de la Loi Informatique et Libertés : *« 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 ».*

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES PERSONNELLES (RGPD)

Désigne le règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, abrogeant la directive 95/46/CE. Il est entré en vigueur le 25 mai 2018.

SERVICES PUBLICS

Désigne les activités exercées directement par la collectivité ou sous son contrôle, dans le but de satisfaire un besoin d'intérêt général.



En savoir plus sur la Charte métropolitaine de la donnée :
metropole.nantes.fr/charte-donnee