

## LA SECURITE DES INFORMATIONS PERSONNELLES PRESENTES DANS LES DOCUMENTS PUBLICS DISPONIBLES EN LIGNE

par

**Pascal KISAKA KALENGA**

**MINTUSU MAMBU OTIS**

(Tous) Assistants, Faculté de Droit,  
Université de Kinshasa

### Résumé

*L'utilisation des moteurs de recherche soulève des défis importants en ce qui concerne la préservation de la vie privée. La diffusion des données publiques en format numérique provoque une évolution temporelle et spatiale, et elle bouleverse le concept traditionnel de publicité qui existait dans le monde papier. Nous examinerons comment garantir le respect du droit à la vie privée ainsi que les modalités d'accès et d'utilisation des informations personnelles, parfois sensibles, présentes dans les documents publics diffusés en ligne. Le cas spécifique des informations disponibles dans les banques de données.*

**Mots-clés** : sécurité, informations personnelles, documents publics, ligne

### Abstract

*Our understanding of time and space is altered by the digital distribution of public data, which also modifies the conventional understanding of public nature that was formerly connected to the "paper" cosmos. We'll look at ways to safeguard privacy as well as the requirements for getting access to and using personal data – sometimes even "sensitive" data – found in publicly available papers that are uploaded online. Due to the nature of the data accessible through judicial data banks, unique security measures are required, meaning that the required.*

**Keywords** : security, personal information, public documents, online

### INTRODUCTION

La République démocratique du Congo (RDC) vient d'alimenter son arsenal juridique en promulguant le 13 mars 2023 un code numérique<sup>20</sup> dans lequel la question relative aux données personnelles ou les données à caractère personnel ainsi que les données publiques ont été définies en son article 2.

Les droits et libertés de la personne sont certainement menacés par la multiplication des moyens de communication et de diffusion des données à caractère personnel, ainsi que par les immenses possibilités de la technologie informatique et du réseau Internet, notamment l'accumulation des données et la mémoire sans faille. Il est possible d'exposer une donnée ou de la rendre accessible à certaines personnes dans un but spécifique et pour une période déterminée, mais « sa mémoire et son stockage peuvent influencer sa signification ». Il est donc essentiel de prévoir des lois spécifiques afin de réguler l'accès à ces données publiques « stockées », et même de reconnaître de nouveaux droits de la personne en raison des possibilités de l'informatique.

Les informations publiques désignent les informations transmises par les documents publics et rendues accessibles à la collectivité afin de respecter le principe de transparence de l'État. Les questions de protection de la vie privée se posent lorsque ces documents renferment des informations personnelles et, surtout, lorsque certaines informations "sensibles" sont divulguées. Que l'information ait été diffusée de manière intentionnelle par les autorités publiques ou que certains citoyens se soient approprié leur droit d'accès, l'utilisation des nouvelles technologies a profondément modifié la manière dont ces données sont communiquées. La diffusion des informations publiques en ligne modifie la manière dont elles sont diffusées et introduit de nouveaux aspects qui ont un impact direct sur les dispositifs de protection des données personnelles.<sup>21</sup>

Avec la numérisation des données administratives et leur diffusion sur Internet, la distinction entre l'accès et la diffusion tend à disparaître progressivement. Le développement du marché de l'information depuis quelques années souligne l'importance économique des données publiques et renforce la diffusion des banques de données issues du secteur public. Nous étudierons tout d'abord les problèmes qui se posent concernant l'équilibre entre l'accès aux données publiques et la préservation de la vie privée des personnes

<sup>20</sup> ORDONNANCE-LOI N° 23/010 DU 13 MARS 2023 PORTANT CODE DU NUMERIQUE

<sup>21</sup> Marcel PINET, « Données publiques ou accessibles au public et données personnelles », communication présentée dans le cadre de la XXe Conférence internationale des commissaires à la protection des données personnelles tenue à Saint-Jacques-de-Compostelle les 16-18 septembre 1998, disponible à l'adresse suivante: <http://www.cnil.fr/thematic/docs/annexe4.pdf>(dernière consultation le 03/02/2022)

concernées, puis les évolutions engendrées par l'utilisation des nouvelles technologies lors de la publication et de la diffusion de ces données. Dans cette première section, nous examinerons également les solutions générales concernant la préservation des informations personnelles présentes dans les documents et registres publics disponibles en ligne.<sup>22</sup>

Souvent, la préservation de la vie privée des individus se heurte au droit à l'information des citoyens. Il est important de prendre des précautions spécifiques afin de préserver les droits de la personne que la diffusion de l'information pourrait compromettre, en prenant en considération le principe de la libre circulation de l'information à caractère public, tant qu'elle ne compromet pas un intérêt supérieur à protéger.

Les systèmes de protection des données personnelles reposent donc sur le critère de la finalité. L'objectif pour lequel les données publiques sont diffusées et publiées sur Internet est de déterminer les utilisations éventuelles de ces informations. Cependant, dans certains cas, la subjectivité et l'incertitude du principe de finalité rendent difficile la détermination de la portée de ce principe et rend difficile l'identification des actions qui ont conduit à un détournement de finalité. Nous examinerons également les différentes méthodes - juridiques et techniques - pour respecter le critère de finalité et réguler l'utilisation des données publiques ; nous examinerons également les conséquences potentielles de la détermination, à l'avance ou à la suite, de la finalité d'un traitement automatisé de données.<sup>23</sup>

Cependant, les conditions de protection des informations personnelles varient en fonction du modèle de réglementation adopté. De cette manière, en Europe, les dispositifs juridiques utilisés constituent un ensemble de normes qui établissent un troisième régime de protection des données personnelles. Il est nécessaire que l'État assure la protection des droits des individus en ce qui concerne la finalité, la durée de conservation et le traitement de ces données. En revanche, aux États-Unis, on substitue cette vision « politique » de la protection par une approche plus économique où le marché joue le rôle d'arbitre : l'autorégulation y définit les conditions de protection des données personnelles.

Une masse considérable de données personnelles - elles forment un ensemble très diversifié - est rendue publique. Le besoin de mesures de protection spécifiques découle de cette réalité, bien que certains soutiennent que ces données ne sont pas "confidentielles" et ne devraient pas bénéficier d'une telle protection. L'objectif est de déterminer si les règles de protection prévues lui sont applicables ou non pour chaque situation spécifique. Le cas des jugements diffusés en ligne et celui des comptes rendus judiciaires disponibles en ligne sont de bons exemples de ce qui est en jeu lorsqu'il s'agit de saisir le conflit entre vie privée et droit à l'information.<sup>24</sup>

Dans la deuxième partie de notre article, nous examinerons les spécificités des données juridiques une fois que le grand principe de la publicité de la justice a été mis en œuvre. Le droit à la vie privée peut être en conflit avec ce principe lorsque ces données sont numérisées et diffusées grâce aux nouvelles technologies. On examinera également les mesures spécifiques prises pour protéger les données à caractère personnel présentes dans les comptes rendus judiciaires et les décisions de justice disponibles en ligne. Les grandes banques de données juridiques sont commercialisées, numérisées et diffusées sur des sites Internet à accès libre ou à accès limité.

Depuis quelques années, certaines interrogations ont été soulevées quant aux répercussions de l'émergence de ce nouveau média sur l'équilibre traditionnel entre la vie privée du justiciable et le principe de transparence judiciaire. L'accumulation quasiment illimitée d'informations et l'utilisation de moteurs de recherche puissants ont engendré des risques qui se manifestent par la possibilité de dresser des profils de comportement et de « suivre » les individus.<sup>25</sup>

Dans toutes ces circonstances, le débat sur l'équilibre entre le principe de la publicité des décisions de justice et celui de la protection des données personnelles, tous deux reconnus par de nombreuses lois nationales ou internationales, a repris vie. Cependant, le premier de ces principes, établi dans le cadre de l'univers « papier », est actuellement bouleversé par l'utilisation des nouvelles technologies de diffusion et la diffusion des informations à travers le monde, pour une période indéterminée : l'émergence du phénomène Internet.

---

<sup>22</sup> Marcel PINET, *op.cit*

<sup>23</sup> Joel R. REIDENBERG, « Protection de la vie privée et l'interdépendance du droit, de la technologie et de l'autorégulation », communication présentée dans le cadre de la XXIII<sup>e</sup> Conférence internationale des commissaires à la protection des données personnelles tenue à Paris les 24-26 septembre 2001, disponible à l'adresse suivante : [http://www.cnil.fr/conference\\_2001/fr/Contribution/reidenberg\\_contrib.pdf](http://www.cnil.fr/conference_2001/fr/Contribution/reidenberg_contrib.pdf) (dernière consultation le 12 février 2021)

<sup>24</sup> Bernard BEIGNIER, « La protection de la vie privée », dans Rémy CABRILLAC, Marie-Anne FRISON-ROCHE et Thierry REVET (dir.), *Libertés et droits fondamentaux*, 6<sup>e</sup> éd., Paris, Dalloz, 2000, p. 160 (nous avons souligné)

<sup>25</sup> Marcel PINET, *op.cit*

## I. DES MESURES GÉNÉRALES POUR PROTÉGER LES INFORMATIONS PERSONNELLES PRÉSENTES DANS LES DOCUMENTS ET REGISTRES PUBLICS DISPONIBLES EN LIGNE.

### 1.1. Les informations de confidentialité et les informations personnelles présentes dans les documents publics

Les informations publiques sont des informations qui peuvent être transmises par des documents publics, comme les registres. La protection de la vie privée des citoyens se pose lorsque ces documents renferment des informations personnelles, en particulier lorsque ces informations sont considérées comme "sensibles".

#### 1.1.1 Concepts et catégories de données ouvertes

La grande quantité de données rendues publiques nous contraint à les définir et à les classer pour en saisir les spécificités et en distinguer les différents types. Ce travail de recensement préliminaire devrait nous donner l'opportunité de mener une étude méthodique des mesures de sécurité concernant les informations personnelles accessibles au public via Internet. Il s'agit de « données publiques » qui englobent toutes les informations que les administrations, sous diverses formes, vont recueillir, générer, traiter, utiliser, préserver, protéger, communiquer et diffuser. Effectivement, les données personnelles accessibles au public comprennent tous les renseignements personnels qui font partie du domaine public et qui peuvent être consultés par n'importe quel moyen.<sup>26</sup>

H. Maisl signale que le mot « donnée » est préféré au mot « information » car le premier de ces mots traduit le fait que « dans les administrations comme dans tous les secteurs de la société, la part du "papier" va en déclinant au profit des traitements informatiques »<sup>27</sup>.

La donnée représente de l'information, un produit préparé pour être traité par un système informatique, et c'est sur cet objet spécifique que se posent les problèmes juridiques. Au lieu d'être un document administratif, la donnée, en général, est "recueillie et conservée par un service public, peu importe sa forme juridique".

Le rapport Diffusion des données publiques et révolution numérique utilise le terme « donnée » pour désigner la « collecte dans le cadre de l'exécution d'une mission de service public ». En particulier, pour différencier les données publiques des documents ou des correspondances, ce rapport examine les données publiques comme des outils de collecte relativement permanents qui structurent systématiquement l'information concernant une variété de personnes physiques ou morales sur un territoire spécifique.

La doctrine a examiné plusieurs définitions possibles des mots « données publiques ». Certains auteurs les ont définies comme l'ensemble des données produites dans le cadre de l'activité d'un service public, en se basant sur un critère « d'origine publique » de manière matérielle<sup>21</sup>, ce qui signifie que ces données « sont produites dans le cadre de [...] et non détenues par une quelconque personne publique ». M. Bruguière distingue deux définitions possibles de l'adjectif « publiques » associé au mot données : elles peuvent être publiques par leur origine ou par leur destination.<sup>28</sup>

La donnée publique peut être celle qui témoigne de l'intervention de l'État, qu'elle soit organique (l'information provient d'un organe spécifique) ou matérielle (l'information provient d'une activité de service public, de police administrative). La donnée peut également être considérée comme publique en raison de sa finalité intellectuelle et économique. La destination intellectuelle de la donnée publique est celle qui peut ou doit être connue du public, c'est-à-dire une chose publiée, accessible, communiquée.<sup>29</sup>

Dans notre cas, l'information est administrative lorsqu'elle concerne la fonction même du gouvernement, cette information administrative peut être « information fondamentale à la démocratie » - lois et jugements des tribunaux - ou ne pas être administrative, l'information non administrative est l'information sur le monde extérieur qui est collectée au moment de l'exécution des obligations publiques : l'information géographique et l'information sur la fonction recherche-développement en sont des exemples.

On peut également classer l'information en fonction de sa valeur économique, comme nous le mettons en évidence dans les pages qui suivent. Selon certaines personnes, une information est considérée comme publique si elle répond à trois critères : le critère organique, qui implique que la donnée soit générée par une personne publique ou une entité dépendante de celle-ci ; le critère matériel, qui implique que la donnée est générée par l'administration dans le cadre de sa mission de service public, dans tous les cas dans le but de répondre à un intérêt public. Le dernier critère se réfère à son objectif car, par définition, une donnée publique doit être accessible à tous. H. Maisl propose quant à lui trois critères pour établir une classification juridique

<sup>26</sup> Roseline LETTERÛN, « Le droit à l'oubli », Revue de Droit Public et de la Science Politique. 1996. vol. 112, nOs 1-3. 393.

<sup>27</sup> Herbert MAISL, Le droit des données publiques, Paris, L.D.G.J., 1996, p. 14

<sup>28</sup> Jean-Michel BRUGUIÈRE, Les données publiques et le droit, Paris, Litec, 2002, p. 3.

<sup>29</sup> Idem, p. 4

des données publiques : la détention (par l'ensemble des personnes publiques), la forme (fichiers, dossiers, répertoires, mais aussi données publiques qui sont stockées sur des supports liés aux nouvelles technologies) et l'objets. Mais! distingue entre :

- les normes et les décisions, comme les lois, les règlements, les arrêtés et les décisions de jurisprudence;
- toutes les données sur les particuliers et sur les entreprises qui sont détenues par les collectivités publiques à des fins de gestion;
- les données conservées à des fins d'information ou d'étude, dans des domaines variés, en vue de rendre ces données disponibles pour le grand public : données socio-économiques, juridiques, scientifiques, médicales, etc. La doctrine américaine dit « public records » en parlant de ce type de documents accessibles au public, mais le sens de cette expression change en ce moment à cause du format électronique qui fait de plus en plus concurrence aux documents « papier».<sup>30</sup>

#### 1.1.2 Définition et origines des informations personnelles présentes dans les documents officiels

En explorant le domaine du droit international, La Directive 95/46/CE utilise le terme « données à caractère personnel » pour reprendre les termes de la Convention pour la protection des personnes contre le traitement des données à caractère personnel du 28 janvier 1981 du Conseil de l'Europe<sup>30</sup> • Bien que certains des termes employés puissent différer d'un texte à l'autre, ce concept est toujours défini de manière très similaire dans les lois nationales de divers pays.

En droit interne congolais, le code numérique définit les données personnelles comme suit : toute information se rapportant à une personne physique identifiée ou identifiable directement ou indirectement.

L'article 54 de la Loi québécoise sur l'accès aux documents publics et sur la protection des renseignements personnels établit la notion de « renseignements nominatifs ». Cet article est libellé dans ces termes : « Dans un document, sont nominatifs les renseignements qui concernent une personne physique et pénètrent de l'identifier. »

La Commission d'accès à l'information du Québec a analysé cette définition et affirme « qu'un renseignement nominatif dans le contexte de l'article 54, doit non seulement faire connaître quelque chose à quelqu'un (renseignement), mais avoir un rapport avec une personne physique (concernée) et il doit aussi être susceptible (permettre) de distinguer cette personne par rapport à quelqu'un d'autre ou de reconnaître sa nature (identifier) ».

La doctrine a repéré les risques liés à la préservation de la vie privée lorsque les informations publiques sont à la fois accessibles en ligne et disponibles en format numérique. Effectivement, il est essentiel de garantir la protection de ces données personnelles devenues publiques, mais il est nécessaire de mettre en place des règles de protection spécifiques car il s'agit de données de natures très variées.

Nombreuses sont les sources des renseignements personnels accessibles au public. Mentionnons à titre d'illustrations les inscriptions aux annuaires téléphoniques, les registres d'immatriculation des automobiles, les dossiers de naissance, de mariage, de divorce, de décès, certains dossiers médicaux, le registre des biens mobiliers, les bases de données sur les décisions judiciaires, les comptes rendus judiciaires et d'autres dossiers judiciaires, etc.

En se basant sur la nature de chaque document provenant du secteur public et l'objectif pour lequel il a été élaboré, certains auteurs ont décrit trois types de sources qui renferment des informations personnelles. Ils évoquent d'abord les registres publics sociaux, tels que les registres de naissance, d'adoption, de mariages et de décès, ainsi que les registres judiciaires. Il est possible que d'autres registres publics soient politiques, comme les listes électorales, par exemple.

Il existe de nombreuses sources de ces données à caractère public, ce qui légitime l'analyse de leurs spécificités ainsi que des mesures de protection nécessaires pour préserver la vie privée des individus, si nécessaire.

#### 1.1.3 Données « confidentielles » divulguées

Il est également possible de trier ces données en fonction de leur "niveau de sensibilité" et de confidentialité. Les catégories suivantes ont été définies par la doctrine :

- les informations considérées comme "très sensibles" sont celles qui présentent des risques d'atteinte à l'intimité ou de discrimination. Les données détournées peuvent causer de graves dommages aux personnes concernées. • Données « sensibles » : ce sont des données qui sont des appréciations ou qui deviennent sensibles lorsqu'elles sont rapprochées d'autres données déjà connues ou susceptibles de

<sup>30</sup> Herbert MAISL, op.cit, p.8

l'être facilement et qui sont liées à une personne. Le détournement de ces informations peut entraîner de graves conséquences sur la sérénité et la réputation des individus ;

- données « neutres » : ces informations mettent en lumière la dimension la plus sociale de la personne.

Selon la doctrine, leur propagation ne cause que des dommages très minimes aux personnes concernées.

Toutefois, selon certains écrivains, presque toutes les informations peuvent devenir sensibles : « En fonction de la nature de l'information, le risque découle du propriétaire, de la proximité et de la finalité de l'utilisation des données personnelles, même celles qui semblent insignifiantes. »<sup>31</sup>

Quant à nous, nous pensons qu'il est envisageable que certains documents publics diffusés sur Internet renferment des informations confidentielles qui ont pu sembler insignifiantes à première vue. Toutefois, personne ne peut assurer que leur acquisition et leur utilisation seront effectuées dans des conditions suffisantes pour éviter leur détournement. Il existe toujours un risque d'atteinte aux droits et libertés fondamentaux de la personne, car il est envisageable de rapprocher et de combiner les différentes informations fournies par les nouvelles technologies. De cette manière, certaines informations publiques qui ne sont pas considérées comme "sensibles" à première vue peuvent enfreindre le droit au respect de la vie privée des individus en raison du traitement informatisé auquel ils sont soumis.

Comme nous pouvons le constater, certaines données qui n'étaient pas initialement considérées comme « sensibles » peuvent le devenir en raison de leur accessibilité élevée sur Internet, à tout moment et depuis n'importe quel endroit. Dans certains documents publics « imprimés », les informations étaient indéfiniment anodines ; le support numérique utilisé de plus en plus souvent pour traiter ces informations et leur diffusion en ligne peuvent les rendre « sensibles ». Nous aborderons ce sujet dans les prochaines pages. Cependant, il est nécessaire d'examiner en détail les défis que pose la diffusion des données personnelles.

## 1.2 La diffusion des informations publiques

### 1.2.1 Développements technologiques et partage des informations publiques

Il est possible que la communication des données publiques soit effectuée à l'initiative de l'administration ou autrement résulte de l'exercice de son droit d'accès à l'information par l'administrateur. Différentes méthodes conduisent à ces deux voies de communication des données publiques et de nombreuses interrogations sont posées concernant l'importance des nouvelles technologies.

#### 1.2.1.1. La propagation des renseignements

Actuellement, le nombre d'informations diffusées au public est considérable. De nombreux domaines sont concernés par cette information, et la population qui la reçoit est extrêmement variée. Elle est diffusée à travers des supports très variés et les méthodes utilisées évoluent rapidement.

La diffusion désigne la transmission des informations publiques effectuée à l'initiative de l'administration. L'information diffusée comme celle qui devient publique par suite de la volonté de la personne qui est chargée de produire cette information et de la faire parvenir au plus grand nombre.

La diffusion par Internet permet aux citoyens et aux entreprises de trouver sans difficulté l'information émanant du secteur public. Certains parlent de « la révolution électronique » et de l'impact majeur qu'elle a eu sur la façon d'accéder à l'information et de la diffuser.

Selon plusieurs auteurs, la numérisation massive des documents administratifs rend obsolète la distinction qui existait auparavant entre la diffusion et l'accès. Cependant, ces écrivains nous rappellent que les deux concepts ne peuvent pas être complètement confondus.

L'accès est plus vaste car il est possible d'accéder à certains documents administratifs qui ne sont pas destinés à être diffusés. En revanche, le domaine des données publiques peut sembler plus large que celui des documents administratifs, ce qui limite le concept d'accès à une diffusion plus restreinte.

#### 1.2.1.2 La liberté d'accéder aux informations

La garantie du droit d'accès implique que les citoyens puissent accéder aux documents non publiés ou non diffusés – donc à l'ensemble des données publiques –, à moins que les lois ne prévoient une exception à l'exercice de ce droit. Dans les sociétés démocratiques, la majorité des lois affirment le droit d'accès.

Il incombe à l'administration d'informer les administrés de l'existence des données publiques, par des moyens adéquats. Comme nous en avons touché un mot précédemment, l'exercice de ce droit par les administrés suppose un processus bilatéral puisque, pour sa part, l'administration a l'obligation de communiquer les données en question.

Tout d'abord, nous étudierons les situations où le droit à l'accès contraint l'administration à transmettre les documents administratifs non publiés à tout citoyen qui en est demandeur. Dans la deuxième partie de

<sup>31</sup> Catherine COSTAZ, « Le droit à l'oubli », Gaz. Pal. 1995.doctr.961.

notre article, nous examinerons le droit de chaque individu à accéder aux informations non publiées qui lui sont personnelles. Ce droit est accompagné du droit de communiquer de telles informations.

Ainsi, le droit d'accès est en constante évolution en raison d'une part de l'utilisation des nouvelles technologies pour la communication des documents publics, et d'autre part de la variété des supports utilisés pour garantir leur disponibilité. À l'avenir, il est essentiel que le droit d'accès soit élaboré de manière à ce que tout le monde puisse bénéficier pleinement des opportunités offertes par les sites Internet ouverts aux citoyens. Ces plateformes rendent les documents publics plus accessibles : les utilisateurs n'ont plus besoin de se déplacer ou de faire une demande d'accès formelle pour les obtenir. Il est nécessaire d'adapter les lois sur l'accès à ce nouveau média et de prévoir des mesures qui prennent en considération les spécificités des nouveaux supports de documents.<sup>32</sup>

Les bases de données du secteur public sont très riches et variées : textes de lois, jurisprudence, données météorologiques et géographiques, données statistiques et économiques, etc. À cette liste partielle s'ajoute l'immense quantité d'informations contenues dans les bases de données nominatives créées par l'administration en raison du monopole qu'elle possède sur la collecte de ces données.<sup>33</sup>

Les défenseurs de la vente des données publiques se demandent si le secteur public devrait ajouter à son monopole sur la collecte des données celui de leur diffusion. Selon leurs homologues aux États-Unis, il est essentiel que le droit à la libre concurrence et la liberté d'accès aux données publiques soient nécessaires pour légitimer l'utilisation commerciale de ces données. Les promoteurs de la commercialisation des données publiques qui invoquent le droit à la libre concurrence dénoncent également les abus imputables au secteur public : il a tendance à tirer parti de sa position dominante pour imposer des tarifs excessifs.

Il y a encore aux États-Unis un cadre juridique spécialement établi pour permettre au secteur public de réutiliser toutes les bases de données détenues par l'administration fédérale. Selon plusieurs études, le secteur américain de l'édition est actuellement cinq fois plus important que le secteur européen correspondant et le marché de la commercialisation de l'information en Europe est à 90 % contrôlé par les États-Unis.

Le secteur public comme le secteur privé devront se conformer à l'objectif pour lequel certaines données personnelles ont été collectées et restreindre les utilisations qui en seront faites. Les banques de données issues du secteur public peuvent renfermer des données qui nécessiteront une protection pour préserver la vie privée des individus concernés.

#### 1.2.2.2 Les entreprises publiques et les entreprises privées

Nous ne nous intéressons pas aux problèmes liés aux droits d'auteur des personnes qui créent les banques de données publiques, mais plutôt à l'étude des enjeux liés au respect de la vie privée que peut engendrer la commercialisation des banques de données privées. Toutefois, nous allons consacrer quelques lignes de notre texte à identifier certaines des banques de données que le secteur public ou privé pourrait être autorisé à diffuser en raison de leur nature.

Au sein du rapport « Données publiques et révolution numérique » déjà évoqué, l'objectif principal était de voir comment le secteur public pourrait être tenu d'une obligation légale de fournir en format numérique les données publiques « de base », numérisées, moyennant rémunération le cas échéant, à l'exception des données « essentielles », qui devraient être diffusées gratuitement.

Cependant, ce rapport suggère que cette exigence ne remplace pas les droits d'accès aux documents administratifs régis par la législation française en vigueur ; en revanche, elle serait en quelque sorte le "complément" qui aurait été inspiré par le même souci de transparence<sup>88</sup>. Cette obligation serait restreinte, elle ne serait exercée que « sous réserve des secrets protégés par des textes spécifiques, ainsi que de la protection de la vie privée ».

Il est crucial de définir et de préciser les responsabilités du secteur public dans sa mission de service public, ainsi que de vérifier si les frais liés à la mise à disposition des données publiques sont inclus dans cette mission. En ce qui concerne l'utilisation des "données essentielles", il est nécessaire de les accompagner de logiciels de présentation, de recherche, et bien d'autres encore, ce qui entraîne des frais pour les organismes qui devront fournir ces outils gratuitement.

La valeur économique des données publiques, comme nous venons de le constater, soulève certaines questions complexes, surtout en ce qui concerne les rôles que le secteur public et le secteur privé devront jouer

<sup>32</sup> Pierre TRUDEL, « L'accès aux documents publics: des ajustements pour assurer la transparence de l'État en réseau », dans Service de la formation permanente, Barreau du Québec, Développements récents en droit de l'accès à l'information (2002), Cowansville, Éditions Yvon Blais, 2002, p. 46.

<sup>33</sup> Pierre TRUDEL, *op.cit.*, p. 47

à l'avenir. La mission de « service public » confiée aux organismes du secteur public et le devoir de transparence administrative sont des notions qui méritent analyse : nous y venons dans les pages qui suivent.

### 1.2.3 Les données publiques ont une valeur sociale

La diffusion des données publiques est intimement liée à la notion d'intérêt général, qui ne peut pas être mise à l'écart en l'occurrence. La mission de « service public » qui a été confiée à l'administration nous rappelle la valeur sociale des données publiques.

## CONCLUSION

La protection des données découle du droit à la vie privée, qui est reconnu dans le monde entier comme un droit de l'homme fondamental inscrit dans les conventions internationales, notamment à l'article 12 de la Déclaration universelle des droits de l'homme et à l'article 17 du Pacte international relatif aux droits civils et politiques.

La majorité des lois concernant la protection des informations personnelles sont structurées autour de principes essentiels tels que la finalité, la proportionnalité, la loyauté, le droit d'accès et le droit de correction. Il ne faut pas oublier que c'est le principe de finalité qui est le fondement des systèmes de protection, car il est la fondation de tous les autres. Selon certaines personnes, le principe de finalité est considéré comme la "pierre angulaire" de la Loi Informatique et Libertés, car toutes les dispositions essentielles de celle-ci en découlent. C'est également en ce sens que la CNIL examine l'application des dispositions de cette même Loi.

Ce principe se manifeste de manière plus explicite dans les lois qui protègent les données personnelles. Ces dernières font parfois référence directe à ce principe, mais sans qu'il soit défini, ce qui rend la tâche plus difficile. Toutefois, de manière générale, la nécessité de se conformer à ce principe de finalité est stipulée dans les lois.

Dans le contexte actuel où l'information circule dans les réseaux, il existe toujours un risque que soit détournée la finalité particulière - par exemple le droit des citoyens à l'information - pour laquelle les documents sont devenus accessibles au public. C'est uniquement à condition que la raison qui a motivé la publication ou la diffusion d'une donnée publique soit explicitement élucidée qu'il devient possible de prendre des mesures en vue d'éviter son détournement. Toutefois, le concept de « détournement » de finalité garde un rapport très étroit avec l'origine même du critère de finalité. Pour arriver à parler de détournement, il faut d'abord bien cerner le critère de finalité, ce qui n'est pas chose facile. La difficulté réside dans la nature subjective et indéterminée du concept de « finalité ».

## BIBLIOGRAPHIE

### 1. Instruments internationaux

- Déclaration universelle des Droits de l'Homme du 10 décembre 1948.
- Pacte international relatif aux droits civils et politique du 16 décembre 1966.

### 2. Texte national

- Ordonnance-loi N° 23/010 DU 13 MARS 2023 PORTANT CODE DU NUMERIQUE

### 3. Ouvrages

- BEIGNIER, B., « La protection de la vie privée », dans CABRILLAC, R., FRISON-ROCHE, A-M., et REVET, T. (dir.), *Libertés et droits fondamentaux*, 6° éd., Paris, Dalloz, 2000
- BRUGUIÈRE, J.-M., *Les données publiques et le droit*, Paris, Litec, 2002
- COSTAZ, C., *Le droit à l'oubli*, Paris, ed. Gaz. Pal. 1995.
- MAISL, H., *Le droit des données publiques*, Paris, L.D.G.J., 1996
- TRUDEL, P., « L'accès aux documents publics: des ajustements pour assurer la transparence de l'État en réseau », dans Service de la formation permanente, Barreau du Québec, *Développements récents en droit de l'accès à l'information (2002)*, Cowansville, Éditions Yvon Blais, 2002

### 4. Revue

- LETTERUN, R., « Le droit à l'oubli », in *Revue de Droit Public et de la Science Politique*. 1996. vol. 112, n° 1-3. 393.

## 5. Webographie

- PINET, M., « Données publiques ou accessibles au public et données personnelles », communication présentée dans le cadre de la XXe Conférence internationale des commissaires à la protection des données personnelles tenue à Saint-Jacques-de-Compostelle les 16-18 septembre 1998, disponible à l'adresse suivante: <http://www.cnil.fr/thematic/docs/annexe4.pdf>(dernière consultation le 03/02/2022)
- REIDENBERG, J., « Protection de la vie privée et l'interdépendance du droit, de la technologie et de l'autorégulation », communication présentée dans le cadre de la XXIIIe Conférence internationale des commissaires à la protection des données personnelles tenue à Paris les 24-26 septembre 2001, disponible à l'adresse suivante : [http://www.cnil.fr/conference/2001/fr/Contribution/reidenberg\\_contrib.pdf](http://www.cnil.fr/conference/2001/fr/Contribution/reidenberg_contrib.pdf)(dernière consultation le 12 février 2021)