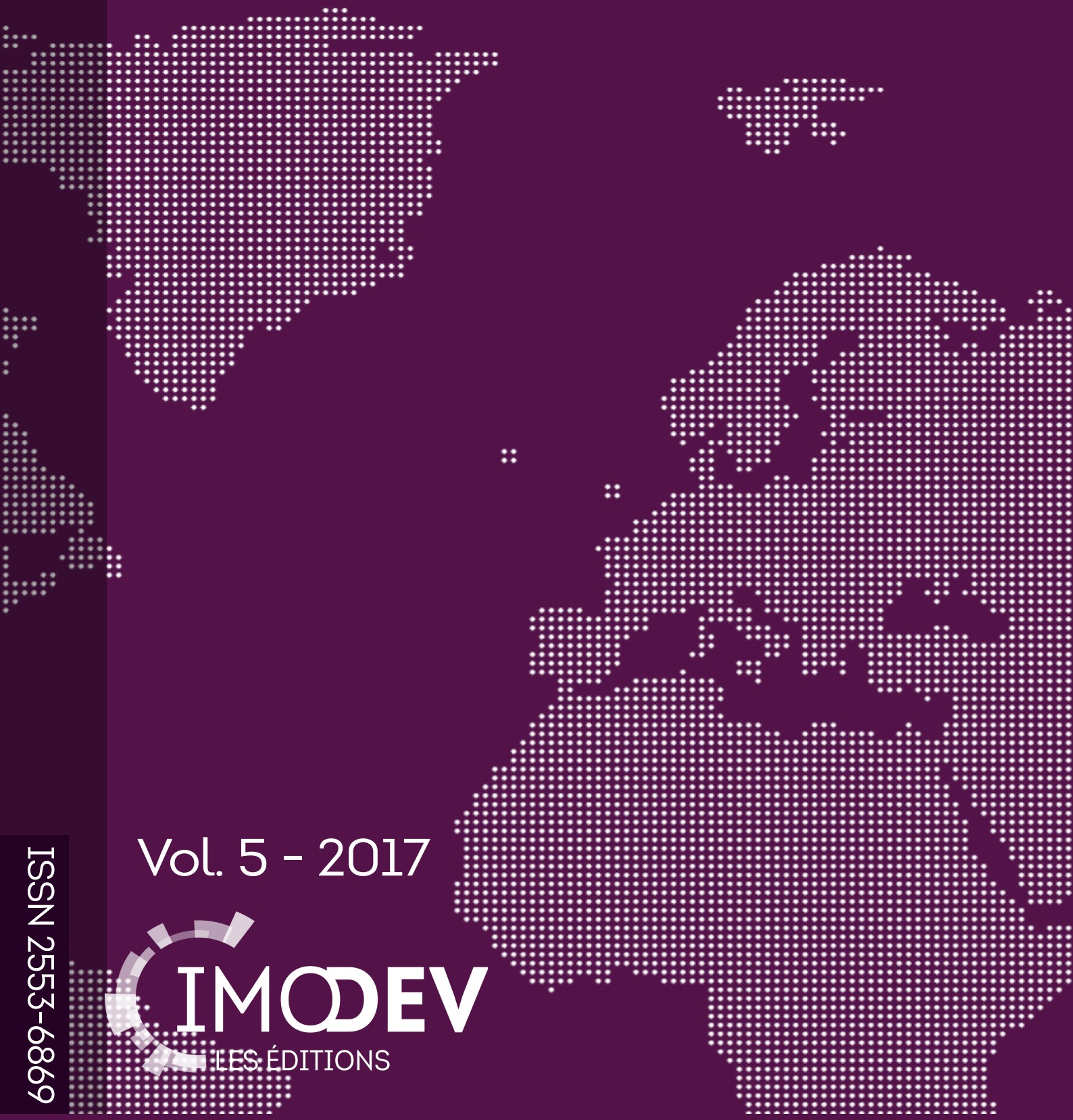
INTERNATIONAL JOURNAL OF **OPEN GOVERNMENTS**

REVUE INTERNATIONALE DES **GOUVERNEMENTS OUVERTS**



Vol. 5 - 2017

ISSN 2553-6869

IMODEV
LES ÉDITIONS

International Journal of Open Governments
Revue internationale des gouvernements ouverts

Direction :
Irène Bouhadana & William Gilles

ISSN : 2553-6869

IMODEV
49 rue Brancion 75015 Paris – France
www.imodev.org
ojs.imodev.org

Les propos publiés dans cet article n'engagent que leur auteur.

The statements published in this article are the sole responsibility of the author.

À PROPOS DE NOUS

La **Revue Internationale des Gouvernements ouverts (RIGO)/ the International Journal of Open Governments** est une revue universitaire créée et dirigée par Irène Bouhadana et William Gilles au sein de l'IMODEV, l'Institut du Monde et du Développement pour la Bonne Gouvernance publique.

Irène Bouhadana, docteur en droit, est maître de conférences en droit du numérique et droit des gouvernements ouverts à l'Université Paris 1 Panthéon-Sorbonne où elle dirige le master Droit des données, des administrations numériques et des gouvernements ouverts au sein de l'École de droit de la Sorbonne. Elle est membre de l'Institut de recherche juridique de la Sorbonne (IRJS). Elle est aussi fondatrice et Secrétaire générale de l'IMODEV.

William Gilles, docteur en droit, est maître de conférences (HDR) en droit du numérique et en droit des gouvernements ouverts, habilité à diriger les recherches, à l'Université Paris 1 Panthéon-Sorbonne où il dirige le master Droit des données, des administrations numériques et des gouvernements ouverts. Il est membre de l'Institut de recherche juridique de la Sorbonne (IRJS). Il est aussi fondateur et Président de l'IMODEV.

IMODEV est une organisation scientifique internationale, indépendante et à but non lucratif créée en 2009 qui agit pour la promotion de la bonne gouvernance publique dans le cadre de la société de l'information et du numérique. Ce réseau rassemble des experts et des chercheurs du monde entier qui par leurs travaux et leurs actions contribuent à une meilleure connaissance et appréhension de la société numérique au niveau local, national ou international en en analysant d'une part, les actions des pouvoirs publics dans le cadre de la régulation de la société des données et de l'économie numérique et d'autre part, les modalités de mise en œuvre des politiques publiques numériques au sein des administrations publiques et des gouvernements ouverts.

IMODEV organise régulièrement des colloques sur ces thématiques, et notamment chaque année en novembre les *Journées universitaires sur les enjeux des gouvernements ouverts et du numérique / Academic days on open government and digital issues*, dont les sessions sont publiées en ligne [ISSN : 2553-6931].

IMODEV publie deux revues disponibles en open source (ojs.imodev.org) afin de promouvoir une science ouverte sous licence Creative commons CC-**BY-NC-ND** :

1) la *Revue Internationale des Gouvernements ouverts (RIGO)/ International Journal of Open Governments* [ISSN 2553-6869] ;

2) la *Revue internationale de droit des données et du numérique (RIDDN)/International Journal of Digital and Data Law* [ISSN 2553-6893].

ABOUT US

The **International Journal of Open Governments / Revue Internationale des Gouvernements ouverts (RIGO)** is an academic journal created and edited by Irène Bouhadana and William Gilles at IMODEV, the Institut du monde et du développement pour la bonne gouvernance publique.

Irène Bouhadana, PhD in Law, is an Associate professor in digital law and open government law at the University of Paris 1 Panthéon-Sorbonne, where she is the director of the master's degree in data law, digital administrations, and open governments at the Sorbonne Law School. She is a member of the Institut de recherche juridique de la Sorbonne (IRJS). She is also the founder and Secretary General of IMODEV.

William Gilles, PhD in Law, is an Associate professor (HDR) in digital law and open government law at the University of Paris 1 Panthéon-Sorbonne, where he is the director of the master's degree in data law, digital administration and open government. He is a member of the Institut de recherche juridique de la Sorbonne (IRJS). He is also founder and President of IMODEV.

IMODEV is an international, independent, non-profit scientific organization created in 2009 that promotes good public governance in the context of the information and digital society. This network brings together experts and researchers from around the world who, through their work and actions, contribute to a better knowledge and understanding of the digital society at the local, national or international level by analyzing, on the one hand, the actions of public authorities in the context of the regulation of the data society and the digital economy and, on the other hand, the ways in which digital public policies are implemented within public administrations and open governments.

IMODEV regularly organizes conferences and symposiums on these topics, and in particular every year in November the Academic days on open government and digital issues, whose sessions are published online [ISSN: 2553-6931].

IMODEV publishes two academic journals available in open source at ojs.imodev.org to promote open science under the Creative commons license CC-**BY-NC-ND**:

1) the *International Journal of Open Governments*/ la *Revue Internationale des Gouvernements ouverts (RIGO)* [ISSN 2553-6869] ;

and 2) the *International Journal of Digital and Data Law* / la *Revue internationale de droit des données et du numérique* (RIDDN) [ISSN 2553-6893].

L'ENCADREMENT DU DROIT D'ACCÈS À L'INFORMATION EN COLOMBIE À L'ÈRE DU NUMÉRIQUE

Par **Angela CUBILLOS VELES,** Professeur-chercheur à l'Université Externado de Colombie, Membre fondatrice du Centre de Recherche de Droit Informatique CIDI, Colombie.

« *Je crois d'ailleurs, Monsieur, que vous rendez un vrai service à la nation, en vous élevant contre le secret des procédures* »
Voltaire[1]

La question concernant le droit d'accès à l'information n'est pas nouvelle. Dans le *Traité de l'administration des finances de la France,* publié en 1784, Necker, contrôleur général des finances de Louis XVI se demandait si ce n'est pas *exhausser « pour ainsi dire, la majesté du prince, que de révéler un peu la nation qu'il gouverne, en lui faisant connaître le motif des lois qu'on lui donne ? ».* Sous le Premier Empire, au contraire, le devoir de réserve devient la règle. Champagny, ministre de l'Intérieur, le rappelait en 1804 dans une circulaire adressée aux préfets :

> « Il ne doit être envoyé des bureaux aucune notice aux journaux sur les affaires qui s'y traitent, sans une autorisation spéciale et, de toute façon, on ne doit jamais parler aux journalistes »[2].

Cette dichotomie entre devoir de réserve et publicité persiste encore de nos jours. En Colombie, comme partout dans le monde, il existe aujourd'hui des règles strictes protégeant les secrets administratifs, militaires et diplomatiques, qui se justifient au nom de l'intérêt général : ainsi l'exemple des négociations de paix récentes entre la Colombie et les FARC, dont l'information a été réservée à une sphère restreinte au sein du gouvernement. À l'inverse, d'autres exemples apparaissent plus contestables, comme le programme de surveillance PRISM mis en place par les États-Unis.

La recherche d'une plus grande transparence est devenue essentielle aujourd'hui. Avec le développement des nouvelles technologies de l'information, les rapports entre l'administration et les citoyens se sont améliorés, car les services publics disposent de plus d'outils pour mettre en place l'ouverture des données.

En outre, le droit d'accès à l'information est encadré et limité par la protection des données à caractère personnel, afin d'empêcher leur utilisation intempestive et d'éviter la surveillance injustifiée

[1] Voltaire, *Correspondance,* A M. Dodin, avocat à Paris, 12 juillet 1775.
[2] B. LASSERRE, N. LENOIR, B. STIRN, *La transparence administrative. Politique d'aujourd'hui*, Presses Universitaires de France PUF, Paris 1987.

des individus. Tout au long de cette démarche, le modèle européen a exercé une grande influence en Amérique latine et plus précisément en Colombie.
Il convient donc d'étudier en premier lieu la matérialisation du droit d'accès à l'information (§1), puis d'examiner les défis constitués par la mise en œuvre du droit d'accès à l'information (§2).

§ 1 – LA MATERIALISATION DU DROIT D'ACCES A L'INFORMATION

Le droit d'accès à l'information a été encadré par l'obligation de transparence (A) et limité par l'obligation de réserve et de confidentialité contenant entre autres la protection des données à caractère personnel (B).

A) Le droit d'accès à l'information : une obligation de transparence pour l'administration publique

Le droit d'accès à l'information est la prérogative donnée à une personne de chercher, de recevoir et de diffuser l'information détenue par le gouvernement et, d'une manière générale, par toute l'administration publique.
En Colombie, ce droit a été consacré par la Constitution, car il constitue une des valeurs fondamentales garantissant un régime démocratique ; d'autre part, la diminution de la culture du secret par la publication des décisions administratives prévient de manière efficace la corruption et le clientélisme.
La Constitution reconnaît aux citoyens le droit de recevoir une information fiable et impartiale[3] ; elle autorise une action de pétition[4] ayant pour but de promouvoir la transparence et la publicité de l'information ; enfin, elle prévoit expressément le droit d'accès aux documents publics[5], sauf dans les cas prévus par la loi, comme par exemple celui du secret professionnel. La Constitution reconnaît également l'importance du caractère public de la fonction administrative.
La reconnaissance du droit d'accès à l'information n'est pas nouvelle, puisqu'elle apparaît déjà dans la loi 57 de 1985[6], en vertu de laquelle la publication des actes et des documents officiels est la condition *sine qua non* de leur entrée en vigueur. Dans le même

[3] Artículo 20 Constitución de Colombia. "Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación. Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura".
[4] Artículo 23 Constitución de Colombia. "Toda persona tiene derecho a presentar peticiones respetuosas a las autoridades por motivos de interés general o particular y a obtener pronta resolución. El legislador podrá reglamentar su ejercicio ante organizaciones privadas para garantizar los derechos fundamentales".
[5] Artículo 74 Constitución de Colombia.
[6] Ley 57 de 5 de junio 1985. Por la cual se ordena la publicidad de los actos y documentos oficiales.

sens, la loi 190 de 1995[7] édicte des normes destinées à préserver la moralité au sein de l'administration publique en éradiquant la corruption administrative ; elle consacre également le caractère obligatoire de l'information et de la publication des décisions.

Plus récemment et d'une manière plus détaillée, la loi 1755 de 2014 a réglementé l'obligation de transparence et le droit d'accès à l'information publique. Cette loi résulte d'une initiative des ambassades de Grande-Bretagne et des Pays-Bas, désireuses de voir s'améliorer à tous les niveaux la transparence dans l'État colombien.

Elle donne une définition précise du droit d'accès à l'information : elle prévoit ainsi dans son article 4 que toute personne peut avoir accès à l'information publique détenue par une personne morale ou physique, publique ou privée, exerçant une fonction publique[8]. Nul n'est exclu du champ d'application subjectif de la loi, comme le montre l'emploi de l'expression « *toute personne* »[9].

Concernant le champ d'application subjectif de la loi. L'administration publique ne pourra exiger aucune demande de qualification du titulaire ou de justification d'intérêt particulier pour rendre effectif ce droit. Autre précision supplémentaire, le droit à la communication des documents détenus par l'administration publique est un droit de portée générale, dont peut jouir toute personne dans son intérêt, quels que soient sa nationalité ou son lieu de résidence. Ce droit de recevoir une information fiable[10] constitue une rupture à la tradition du secret administratif[11]. Enfin, lorsqu'une personne considère que son droit à l'information comporte un risque pour son intégrité ou pour celle de sa famille, elle peut effectuer sa démarche auprès du Ministère public, qui est l'autorité chargée du contrôle et de la mise en œuvre de la loi sur la transparence.

On constate également un accroissement du nombre des personnes tenues au respect de la loi, qui donne une liste exhaustive où figurent toutes les personnes, physiques ou morales, indépendantes ou autonomes, qui exercent une fonction publique ou administrent des fonds d'origine publique[12]. En vertu

---

[7] Ley 190 de 6 de junio de 1995. Por la cual se dictan normas tendientes a preservar la moralidad en la Administración Pública y se fijan disposiciones con el fin de erradicar la corrupción administrativa.

[8] Artículo 4. Ley 1712 6 de marzo 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. [En ligne]
http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882 Site consulté le 11 janvier 2016.

[9] Article 4. Ley 1712 6 de marzo 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. [En ligne]
http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882 Site consulté le 11 janvier 2016.

[10] Corte Constitucional de Colombia sentencia C-274/13.

[11] *Refonder le droit à l'information publique à l'heure du numérique : un enjeu citoyen, une opportunité stratégique* (Rapport) http://www.senat.fr/rap/r13-589-1/r13-589-13.html

[12] Artículo 5. Ley 1712 6 de marzo 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan

de ce principe de transparence, toute l'information que détiennent ces personnes est considérée comme publique et sa diffusion ne peut être limitée que par la loi ou par la Constitution[13]. Cette information est définie comme l'ensemble des données organisées et contenues dans un document produit, obtenu, acquis, transformé ou contrôlé, ayant rapport avec l'activité des personnes concernées par cette loi. Ainsi, les collectivités territoriales, même les plus petites, sont tenues au respect de la loi et à la publication en ligne des documents administratifs.

Le droit d'accès aux documents publics garantit trois fonctions essentielles : premièrement, ce droit assure la participation démocratique et l'exercice des droits politiques, deuxièmement, le droit d'accès permet la matérialisation d'autres droits constitutionnels, par exemple : l'accès à l'information est un outil essentiel pour concrétiser le droit de connaître la vérité des faits concernant les victimes du conflit armé et pour préserver le droit à la mémoire historique de la société. En fin, le droit à savoir garantit la transparence de la gestion publique, permettant le contrôle des activités de l'État[14].

La loi comporte également les principes directeurs concrétisant le droit d'accès à l'information, en particulier le principe de transparence disposant que toute l'information en pouvoir de l'administration est présumée publique[15], cette obligation pèse sur les sujets obligés antérieurement définis. On constate ainsi, la présence d'un principe général de publicité, dans lequel l'obligation de réserve constitue l'exception.

---

otras disposiciones. [En ligne]
http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882 Site consulté le 11 janvier 2016. Champ d'application. "Las disposiciones de esta ley serán aplicables a las siguientes personas en calidad de sujetos obligados:
a) Toda entidad pública, incluyendo las pertenecientes a todas las Ramas del Poder Público, en todos los niveles de la estructura estatal, central o descentralizada por servicios o territorialmente, en los órdenes nacional, departamental, municipal y distrital;
b) Los órganos, organismos y entidades estatales independientes o autónomos y de control;
c) Las personas naturales y jurídicas, públicas o privadas, que presten función pública, que presten servicios públicos respecto de la información directamente relacionada con la prestación del servicio público;
d) Cualquier persona natural, jurídica o dependencia de persona jurídica que desempeñe función pública o de autoridad pública, respecto de la información directamente relacionada con el desempeño de su función;
e) Los partidos o movimientos políticos y los grupos significativos de ciudadanos;
f) Las entidades que administren instituciones parafiscales, fondos o recursos de naturaleza u origen público".

[13] Artículo 2. Ley 1712 6 de marzo 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. [En ligne]
http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882 Site consulté le 11 janvier 2016.

[14] Corte Constitucional de Colombia. Sentencia C-274/13. Magistrada ponente: María Victoria Calle Correa. http://www.corteconstitucional.gov.co/relatoria/2013/c-274-13.htm

[15] Artículo 2. Ley 1712 6 de marzo 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. [En ligne]
http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882 Site consulté le 11 janvier 2016.

La pratique de la transparence doit encore se développer ; cependant, même avant l'adoption de cette réglementation on a observé la création de plusieurs sites sur Internet contenant des documents publics, tels que le portail unique des contrats de l'État colombien[16], le site des acquisitions de l'État[17], le site du gouvernement en ligne[18] contenant des données publiques ouvertes. Chaque entité publique possède également son site internet ; enfin, le projet d'un gouvernement ouvert a été mis en place. Un portail des données ouvertes réunit de manière centralisée les données publiques des entités[19]. Ainsi, la transparence au sein de l'administration publique permet-elle aux citoyens d'exercer un contrôle direct sur les pouvoirs publics et de lutter également contre la corruption et le clientélisme.

La création des données dites ouvertes est l'expression maximale du principe de transparence. Ces données ont été cataloguées comme étant de libre accès sur Internet[20] sans qu'aucune demande ne soit requise au préalable. La réutilisation des données ouvertes est admise en Colombie ; par ailleurs, la loi autorise sans aucune restriction la création de services à partir de la réutilisation des données[21].

Le principe de bonne foi comprend également le droit d'accès à l'information, ainsi que l'obligation d'agir de manière loyale envers tous ceux qui en jouissent[22]. L'exercice du droit d'accès à l'information publique doit être facilité, en évitant toute discrimination et en garantissant le même accès pour tous, sans qu'aucune justification préalable ne soit requise. Par ailleurs, le droit colombien a consacré les garanties aux différents groupes ethniques et culturels existants dans le pays, afin d'assurer l'accès à l'information dans sa langue d'origine.

En outre, en vertu du principe de gratuité, le seul prix à payer est celui de la reproduction de l'information. La diligence et l'efficacité font également partie des principes du droit d'accès à une information qui doit être opportune, objective, fiable, complète, réutilisable et disponible sous des formats différents.

---

16 https://www.contratos.gov.co/consultas/inicioConsulta.do

17 http://www.colombiacompra.gov.co/

18 http://estrategia.gobiernoenlinea.gov.co/623/w3-channel.html

19 www.datos.gov.co

20 Artículo 7. Ley 1712 6 de marzo 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. [En ligne]
http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882 Site consulté le 11 janvier 2016.

21 Artículo 6. J. Ley 1712 6 de marzo 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. [En ligne]
http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882 Site consulté le 11 janvier 2016.

22 Artículo 3. Ley 1712 6 de marzo 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. [En ligne]
http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882 Site consulté le 11 janvier 2016.

La portée du droit d'accès à l'information en Colombie est double. En effet, il est obligatoire de donner une réponse à ceux jouissant de ce droit ; d'autre part, tous les fonctionnaires de l'État sont tenus de promouvoir la publication des documents et des dossiers reflétant l'activité de l'État en accord avec l'intérêt public, sans qu'aucune demande préalable ne soit requise. Lorsque la promotion et la publication des données ouvertes ne sont pas effectuées de manière active, on peut considérer alors qu'il existe un manquement de la part des fonctionnaires soumis à l'obligation de transparence. Enfin, la mise à jour de l'information doit être effectuée régulièrement et son contenu doit demeurer accessible et compréhensible.

Par ailleurs, la loi institue un principe de responsabilité dans l'utilisation de l'information[23]. En vertu de ce principe, tous ceux qui jouissent du droit d'accès, c'est-à-dire les titulaires, sont obligés d'utiliser l'information donnée par l'État d'une manière responsable, ce principe est d'ailleurs important pour empêcher la déformation du droit d'accès comme on l'examinera par la suite.

En outre, afin d'éviter toute dérive. En effet, si l'importance du droit à l'information est primordiale pour l'exercice de la démocratie, ce droit d'accès doit être cependant encadré afin de respecter la vie privée des individus et de faire des données un usage légitime, car ce droit ne doit pas être en contradiction avec les autres droits fondamentaux des individus.

B) Les limites au droit d'accès à l'information publique

Si le droit d'accès à l'information est un principe général, la loi et la Constitution prévoient expressément des exceptions et une limitation de ce droit, dans le respect des principes démocratiques.

Il existe trois types des données publiques : *les données ouvertes ou de libre accès*, dont il a été parlé précédemment, *l'information publique classifiée* et *l'information publique réservée*. La loi permet ainsi de limiter l'accès à l'information publique afin de préserver le droit à la vie privée. Cette *information publique classifiée*[24] se définit comme l'ensemble des données appartenant à la sphère privée d'une personne morale ou physique : l'accès à ces données demeure limité et peut être refusé par l'administration publique afin de préserver les droits des particuliers.

---

[23] Artículo 3. Ley 1712 6 de marzo 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. [En ligne]
http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882 Site consulté le 11 janvier 2016.

[24] Artículo 6. Ley 1712 6 de marzo 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. [En ligne]
http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882 Site consulté le 11 janvier 2016.

Un autre type d'information publique demeure exclu du champ d'application de la loi : *l'information publique réservée*[25], cette information détenue par l'administration publique ne pourra dans aucun cas être mise à disposition des citoyens, car l'accès peut nuire à l'intérêt public.

Afin de prévenir les dommages contre les personnes morales ou physiques et contre l'intérêt public, la loi donne une liste exhaustive des exceptions au droit d'accès à l'information. L'accès à ces données peut être refusé lorsqu'il est susceptible de constituer un dommage au droit à la vie, à la santé, à la vie privée ou à la sécurité de personnes morales et physiques[26]. Pour le cas des personnes morales, il existe également une exception, dans le cas des secrets commerciaux, industriels et professionnels ; néanmoins, une réponse motivée par écrit demeure exigée[27]. Il convient de préciser que ces exceptions ont une durée limitée et ne s'appliquent pas lorsque la personne morale ou physique a donné son consentement pour la publication des données personnelles. La loi autorise la publication quand l'information a été donnée dans le cadre du régime de publicité des données publiques.

S'agissant de l'information publique réservée[28], son accès peut être refusé lorsque la publication de ces données pourrait nuire à l'intérêt général, par exemple dans le cas de la défense ou de la sécurité nationale, de la sécurité publique, des relations internationales, de la prévention, de l'investigation ou de la poursuite de délits, des droits de l'enfance et de l'adolescence, de l'égalité entre les parties lors d'un procès judiciaire, du fonctionnement de la justice, de la stabilité économique et financière du pays et de la santé publique. Sont également exceptés du champ d'application de la loi, les procès-verbaux des délibérations des fonctionnaires de l'État. Le refus de l'accès à ces données doit être signifié par un écrit motivé.

La Cour constitutionnelle colombienne considère que la réserve doit « *porter sur le contenu d'un document public, mais non sur l'existence*

---

[25] Artículo 6. Ley 1712 6 de marzo 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. [En ligne]
http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882 Site consulté le 11 janvier 2016.

[26] Artículo 18. Ley 1712 6 de marzo 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. [En ligne]
http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882 Site consulté le 11 janvier 2016.

[27] Artículo 18. Ley 1712 6 de marzo 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. [En ligne]
http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882 Site consulté le 11 janvier 2016.

[28] Artículo 19. Ley 1712 6 de marzo 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. [En ligne]
http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882 Site consulté le 11 janvier 2016.

du document en lui-même»[29], car il ne faut pas succomber dans l'extrémisme, la publication de l'existence du document permet aux citoyens d'exercer leur droit fondamental de contrôle des pouvoirs publics[30]. En outre, la réserve ne doit pas constituer un obstacle au contrôle juridique et politique interne au sein de l'administration.

En Colombie, la loi sur la transparence et le droit d'accès à l'information doit être examinée à la lumière de la réglementation sur la protection des données à caractère personnel. Ces données peuvent être considérées de deux manières : soit l'on considère, en suivant le modèle américain, qu'il s'agit de biens pouvant être vendus, ce qui favorise la croissance économique ; soit l'on considère, en suivant le modèle européen, qu'elles constituent un attribut de la personnalité. La Colombie suit pour sa part le modèle européen.

En outre, un modèle hybride de réglementation sur la protection des données a été implanté en Colombie[31]. En effet, la loi 1581 du 17 octobre 2012[32] est une réglementation centrale contenant des dispositions générales destinées à assurer la protection minimale de toutes les données à caractère personnel ; d'autre part, la loi de protection des données commerciales et financières de 2008[33] est une réglementation sectorielle qui soumet certaines données à une réglementation spéciale.

La Colombie est l'un des douze pays d'Amérique latine ayant conféré une valeur constitutionnelle à la protection des données à caractère personnel ainsi qu'au droit de l'*habeas data* dans l'article 15 de sa Constitution[34]. L'État doit donc lui-même

---

[29] Corte Constitucional de Colombia. Sentencia C-274/13. Magistrada ponente: María Victoria Calle Correa. http://www.corteconstitucional.gov.co/relatoria/2013/c-274-13.htm

[30] Artículo 40 de la Constitución Política de Colombia.

[31] Corte Constitucional de Colombia. Sentencia C-748/11. Magistrado Ponente: Jorge Ignacio Pretelt Chaljub. Bogotá D.C., 6 octobre 2011. « En droit comparé, il existe deux modèles largement reconnus de protection des données : un modèle centralisé et un modèle de secteur. Le modèle centralisé (mis en œuvre dans les pays européens) […]. Et le modèle du secteur, qui ne fait pas partie d'une catégorie commune des données personnelles et ne considère donc pas que ces données devraient être soumises à la même réglementation minimale, et donc, en vertu de ce modèle règlements spéciaux sont adoptés […] pour chaque type de données à caractère personnel, en fonction de leur relation avec l'intimité ou la vie privée comme est appelé dans le système anglo-saxon et avec la protection d'intérêts supérieurs - comme la sécurité et de la défense nationale, à savoir, que la réglementation sectorielle est fondée sur une sorte d'équilibre des intérêts menant à des règles différentes selon le type de données et (…) les pouvoirs d'intervention donnés aux autorités.

En Colombie il s'agit d'un modèle hybride de protection des données ».

[32] Ley estatutaria 1581 de 17 octobre 2012. Reglamentada parcialmente por el Decreto Nacional 1377 de 2013. Por el cual se dictan disposiciones generales para la protección de datos personales".

[33] Ley estatutaria No. 1266 de 31 décembre 2008. Diario Oficial No. 47.219 de 31 de diciembre de 2008. Revisión Previa de Constitucionalidad. Declarado Exequible mediante Sentencia C-1011 del 16 de octubre de 2008.

[34] Constitution politique de Colombie. Article 15 « Toutes les personnes ont le droit à leur vie privée et familiale et à leur réputation, et l'État doit le respecter et le faire respecter. De même, ils ont le droit de connaître, de mettre à jour et rectifier les informations qui se sont recueillies à leur sujet dans les bases de données et dans les archives des entités publiques et privées.

respecter ces principes et les faire respecter. De même, la Constitution prévoit dans l'article 15 que les individus ont le droit de connaître, de mettre à jour et de rectifier les informations recueillies à leur sujet dans les bases de données et dans les archives des entités publiques et privées. Il est possible d'en déduire que la Constitution consacre explicitement la protection des données à caractère personnel, de sorte que le niveau de protection est celui d'un droit fondamental bénéficiant d'une protection juridique spéciale.

Cette consécration est essentielle afin de garantir la vie privée de l'individu et plus particulièrement afin d'assurer le droit à la dignité humaine. Les dispositions constitutionnelles sur la protection des données ont pour objectif de protéger l'individu dans tous ses domaines d'activité, et d'assurer un traitement légitime des données à caractère personnel par des organismes publics ou des entreprises privées.

Le droit d'*habeas data* est défini par la Cour constitutionnelle colombienne comme la faculté qu'a la personne concernée par les données *« d'exiger des administrateurs l'accès, l'inclusion, l'exclusion, la correction, l'ajout, la mise à jour et la certification des données. De plus, le titulaire a la faculté de limiter les possibilités de diffusion, publication ou cession des données. Cet ensemble doit être conforme aux principes qui régissent le processus de gestion ou d'administration des données personnelles. Ce droit est autonome et possède des caractéristiques qui le différencient des autres droits avec lesquels le droit d'*habeas data *est en relation permanente, comme les droits à la vie privée et à l'information »*[35]. Ainsi, l'on peut considérer que le droit fondamental d'*habeas data* réside dans l'exercice effectif et actif de la personne concernée.

En ce qui concerne le champ d'application matériel de la loi de 2012, ses principes et ses dispositions sont applicables aux données personnelles enregistrées dans une base de données susceptible d'être traitée par des entités publiques ou des entités à caractère privé[36]. Ainsi, il est clair que le traitement des données à caractère personnel effectué par les entités publiques est soumis au respect de la protection consacrée par la loi. Cette loi de portée générale définit la *donnée personnelle* comme toute information pouvant être associée ou liée à une ou plusieurs personnes physiques déterminées ou déterminables[37]. Il s'agit là d'une définition large, car il est possible de protéger une plus grande

Dans la collecte, le traitement et la diffusion de données, la liberté et d'autres garanties prévues par la Constitution seront respectées.
La correspondance et autres formes de communication privée sont inviolables. Elles ne peuvent être interceptées ou enregistrées par injonction, dans les cas et avec les formalités prescrites par la loi ».

[35] Corte Constitucional de Colombia. Sentencia T-058/13. Magistrado Ponente: Alexei Julio Estrada. Bogotá D.C. 7 février 2013 :
http://www.corteconstitucional.gov.co/ relatoria/2013/T-058-13.htm

[36] Artículo 2. Ley estatutaria 1581 de 17 octobre 2012. Reglamentada parcialmente por el Decreto Nacional 1377 de 2013. Por el cual se dictan disposiciones generales para la protección de datos personales".

[37] Artículo 3.C. Ley estatutaria 1581 DE 17 octubre 2012. Reglamentada parcialmente por el Decreto Nacional 1377 de 2013. Por el cual se dictan disposiciones generales para la protección de datos personales.

quantité de données personnelles en créant des liens, même indirects, entre la donnée et la personne. Tel est le cas par exemple d'une adresse IP ou d'un cookie qui s'installe sur un ordinateur, permettant d'identifier la personne concernée.

En revanche, la loi limite la définition de donnée personnelle en exigeant que l'information soit associée à une personne. Par exemple, si à des fins statistiques ou de sondage, une entité publique responsable du traitement des données des citoyens effectue un transfert de données à un sous-traitant sans fournir l'identification des personnes concernées (noms, prénoms, adresses, etc.), on considère que le sous-traitant n'a pas d'accès aux données à caractère personnel, car il ne possède pas les moyens pour associer l'information à une personne ni pour l'identifier.

De plus, la loi définit une *base de données* comme un ensemble organisé de données à caractère personnel faisant l'objet d'un traitement[38]. Le *traitement* est défini comme toute opération ou ensemble d'opérations sur les données personnelles, comme la collecte, le stockage, l'utilisation, la circulation ou la suppression[39]. En l'état actuel des choses, on peut constater que la définition n'exclut pas les traitements non automatisés du champ d'application de la loi.

Par ailleurs, on remarque que les responsables du traitement ayant besoin de mettre en place un traitement de données se considèrent constamment de manière illégitime en dehors du champ d'application de la loi lorsque la collecte des données est nécessaire pour exercer leur activité. Ainsi, une liste de noms publiée en ligne est un traitement des données, même si elle est nécessaire à l'activité du responsable du traitement. En ce sens, la finalité du traitement des données personnelles devient une question fondamentale, notamment en ce qui concerne les formalités : la question principale consiste en effet à savoir ce que l'on fait des données et non pas quel est l'objectif du traitement. Par exemple, la collecte des données sur la couleur de peau des citoyens, qui vise à assurer la sécurité de l'État, peut être considérée comme sensible, si elle est utilisée à des fins discriminatoires.

Concernant le traitement, le droit colombien exclut du champ d'application de la loi[40] les traitements de bases de données et de fichiers dont le but est la sécurité, la défense, le contrôle national du blanchiment d'argent et du financement du terrorisme, les traitements qui ont pour objet ou qui contiennent des renseignements sur l'espionnage et le contre-espionnage et les

[38] Artículo 3.B. Ley estatutaria 1581 de 17 octubre 2012. Reglamentada parcialmente por el Decreto Nacional 1377 de 2013. Por el cual se dictan disposiciones generales para la protección de datos personales.

[39] Artículo 3.G. Ley estatutaria 1581 de 17 octubre 2012. Reglamentada parcialmente por el Decreto Nacional 1377 de 2013. Por el cual se dictan disposiciones generales para la protección de datos personales.

[40] Artículo 2. Ley estatutaria 1581 de 17 octubre 2012. Reglamentada parcialmente por el Decreto Nacional 1377 de 2013. Por el cual se dictan disposiciones generales para la protección de datos personales.

traitements de bases de données sur l'information journalistique, qui font partie de l'information publique réservée. Le contrôle de la finalité du traitement occupe une place importante, malgré l'existence d'une liste d'exclusion du champ d'application. Ainsi, dans le cas d'activités de surveillance et de contre-espionnage, il est indispensable que la finalité du traitement d'information soit légitime et ne dépasse pas les limites de l'exclusion.

En outre, la loi définit les personnes faisant l'objet de la protection. Ainsi la personne protégée est appelée *titulaire* : il s'agit donc d'une personne physique dont les données font l'objet d'un traitement[41]. En droit français, le titulaire est la personne concernée[42]. La loi ne prévoit pas de protection pour les personnes morales, cependant, il est important de noter que les personnes morales peuvent également engager une procédure pour protéger leur droit d'*habeas data* grâce à une décision jurisprudentielle[43]. Sur ce point, il est contestable que la loi n'ait pas assuré une protection aux personnes morales, étant donné que les données acquises dans le cours normal des affaires doivent bénéficier d'une protection spéciale pour empêcher la concurrence déloyale et l'abus de position dominante, lorsque d'autres entreprises utilisent les données de la personne morale. Malgré le silence de la loi de protection des données, la loi d'accès à l'information publique protège de manière expresse les secrets commerciaux, industriels et professionnels, en considérant qu'il s'agit d'une information publique classifiée.

En ce qui concerne le *responsable du traitement*, il peut s'agir d'une personne physique ou morale, publique ou privée, qui de lui-même ou bien en association avec d'autres personnes, prend des décisions sur la base de données ou sur le traitement des données[44]. Il a l'obligation d'accomplir toutes les formalités, ainsi que de respecter l'obligation d'information et les conditions de licéité du traitement prévues dans la loi. Le responsable du traitement peut être sanctionné, car c'est lui qui, seul ou conjointement avec d'autres responsables, détermine les finalités et les moyens du traitement des données personnelles. Le cas échéant, si le contrôleur donne un mandat à un sous-traitant, il a l'obligation de surveiller la façon dont les données personnelles sont traitées, afin de ne pas engager sa responsabilité.

---

41 Artículo 3. F. Ley estatutaria 1581 de 17 octubre 2012. Reglamentada parcialmente por el Decreto Nacional 1377 de 2013. Por el cual se dictan disposiciones generales para la protección de datos personales.

42 Article 2 alinéa 5 de la Loi informatique et libertés n° 78-17 du 6 janvier 1978.

43 Corte Constitucional. Sentencia T-462/97. Magistrado Ponente : Vladimiro Naranjo Mesa. Santafé de Bogotá, D.C. 24 septembre 1997. Droit d'habeas data de la personne morale. « Si les personnes morales ont le droit fondamental à une bonne réputation, ils ont donc également le droit à l'habeas data ». Voir aussi Corte Constitucional de Colombia. Sentencia C-748/11. Magistrado Ponente: Jorge Ignacio Pretelt Chaljub. Bogotá D.C., 6 octobre 2011. « … la référence est légitime pour les personnes physiques, ce qui ne veut pas dire qu'éventuellement, la protection s'étend pour les personnes morales lorsque leurs droits sont affectés ».

44 Artículo 3. E. Ley estatutaria 1581 DE 17 octubre 2012. Reglamentada parcialmente por el Decreto Nacional 1377 de 2013. Por el cual se dictan disposiciones generales para la protección de datos personales.

Concernant le *gestionnaire du traitement des données*, cela peut être également toute personne physique ou morale, publique ou privée, qui effectue le traitement des données à caractère personnel par lui-même ou en association avec d'autres en agissant pour le compte du *responsable du traitement*. Le gestionnaire du traitement est le sous-traitant pour le droit français[45]. En termes de responsabilité, malgré l'absence de régulation dans la loi colombienne, le contrat conclu par le sous-traitant ou par le gestionnaire du traitement avec le responsable du traitement doit stipuler la répartition des obligations en matière de sécurité et de confidentialité, car le sous-traitant ne peut pas agir que sur instruction du responsable de l'information. Ainsi, plus les instructions vont être larges, plus le risque d'engager la responsabilité du sous-traitant est important.

Concernant l'application territoriale de la loi, cette loi s'applique au traitement des données à caractère personnel effectué en Colombie ou lorsque le responsable du traitement ou le gestionnaire du traitement (sous-traitant) bien qu'il ne soit pas établi en Colombie, est soumis à la loi colombienne, en vertu des normes ou des traités internationaux[46]. Ainsi, pour l'application de la loi, il y a traitement de données personnelles en Colombie quand il y a utilisation des moyens de traitement sur le territoire afin d'éviter la délocalisation des données. L'utilisation d'ordinateurs, d'hébergeurs et de serveurs sur le territoire colombien ou la simple installation d'un cookie dans un serveur est considérée comme un traitement de données personnelles.

Après avoir examiné le champ d'application matériel et territorial de la loi, il convient d'analyser *les conditions de licéité des traitements de données à caractère personnel* en étudiant ce qui est au cœur de la protection des données personnelles : *le consentement préalable de la personne concernée*, qui constitue la condition de licéité la plus importante, quelle que soit la législation sur la protection des données.

Dans le cadre du traitement de données personnelles, pour respecter les conditions de licéité du traitement, il est indispensable de demander au titulaire de l'information son consentement *préalable, exprès et informé* conformément à l'article 9 de la loi 1581 de 2012 qui prévoit que l'autorisation du titulaire doit être préalable, informée, et obtenue sur un support durable. Dans ce cas, la charge de la preuve incombe au responsable du traitement. La loi colombienne interdit tout consentement tacite ; ce dernier doit être donné expressément et de façon indiscutable. La Cour constitutionnelle a clairement précisé la nécessité du consentement libre, préalable, exprès et informé du titulaire[47].

---

[45] Article 35 de la Loi informatique et libertés n° 78-17 du 6 janvier 1978. La loi française a prévu un autre mécanisme qui n'est pas une disposition expresse prévue dans les autres États membres de l'Union européenne.

[46] Artículo 2. Ley estatutaria 1581 de 17 octubre 2012. Reglamentada parcialmente por el Decreto Nacional 1377 de 2013. Por el cual se dictan disposiciones generales para la protección de datos personales.

[47] Corte Constitucional de Colombia. Sentencia C-748/11. Magistrado Ponente: Jorge Ignacio Pretelt Chaljub. Bogotá D.C., 6 octobre 2011.

Le consentement doit être également informé, c'est-à-dire que la collecte de données doit être faite de façon claire et loyale. Pour que le consentement soit valable, il est nécessaire que l'information sur la nature du traitement soit complète et de qualité et qu'elle soit présentée à la personne concernée de façon claire, expresse, compréhensible et visible. Par exemple, si la case à cocher demandant l'autorisation pour l'utilisation des données personnelles à la personne concernée se trouve précochée, cela peut être considéré comme une collecte déloyale et illicite. Aussi, dans le cas d'un transfert de données, le responsable du traitement ou le sous-traitant devra informer la personne concernée si les données recueillies seront transmises à des tiers et, il devra, de ce fait, demander une autorisation préalable. La Cour Constitutionnelle a fixé la limite à partir de laquelle on considère qu'il y a eu violation de la protection des données personnelles. Elle affirme en effet que *le consentement* est le critère qui permettra de déterminer s'il y a eu ou non violation du droit fondamental au regard de l'*habeas data*. En effet, le consentement donné au gestionnaire du traitement (sous-traitant) ou au responsable du traitement doit être préalable, exprès et éclairé.

Par ailleurs, la publication démesurée de l'information sur les données personnelles sera considérée comme illégale et contraire à la Constitution, lorsque cette information publiée ne respecte pas les exigences du consentement préalable. Le consentement du titulaire de l'information concernant l'enregistrement de ses données, est lié à la nécessité d'avoir la possibilité réelle d'exercer son pouvoir d'opposition, de suppression, de correction et de mise à jour de ces données pendant les différentes étapes du traitement. Le consentement permet également à la personne concernée de pouvoir protéger sa vie privée et sa réputation.

Il existe néanmoins un régime de dérogation en ce qui concerne l'autorisation. L'article 10 de la loi[48] prévoit en effet qu'elle n'est pas requise lorsque l'information est demandée par un organisme public ou administratif dans l'exercice de ses fonctions statutaires ou par décision du juge, lorsque l'information est de nature publique ; de même en présence de cas d'urgence médicale ou de santé ; enfin lorsque le traitement porte sur des informations autorisées par la loi à des fins historiques, statistiques, scientifiques ou relatives à l'enregistrement civil des personnes.

Une autre question essentielle que la loi a incluse est la création de conditions spécifiques de licéité pour une catégorie particulière de données devant bénéficier d'une protection spéciale. Comme l'affirme Benjamin Constant, il y a « *une partie de l'existence humaine qui, de nécessité, reste individuelle et indépendante, et qui est de droit hors de toute compétence sociale* »[49]. Toute la difficulté consiste alors à

[48] Article 10. Ley estatutaria 1581 DE 17 octobre 2012. Reglamentada parcialmente por el Decreto Nacional 1377 de 2013. Por el cual se dictan disposiciones generales para la protección de datos personales.

[49] B. CONSTANT, *Commentaire sur l'ouvrage de Filangieri*, Paris, Les Belles Lettres, 2004, p. 59.

déterminer cette partie, qui concerne des données sensibles et la protection spéciale des mineurs.

En ce qui concerne les données sensibles, la loi de 2012[50] a considéré comme données sensibles celles qui affectent la vie privée du titulaire, et dont l'usage indu peut être à l'origine d'une discrimination, comme celles révélant l'origine raciale ou ethnique, l'orientation politique, les convictions religieuses ou philosophiques, l'adhésion à des syndicats ou à des organisations sociales, les droits de l'homme, les droits et garanties des partis politiques d'opposition, ainsi que les données concernant la santé, la vie sexuelle et les données biométriques[51].

Pour assurer une protection renforcée, le traitement des données sensibles est interdit, même si le responsable du traitement est une entité publique. Ainsi, l'administration publique ne doit communiquer cette information qu'à la personne concernée.

Cependant, malgré ce principe d'interdiction générale, la loi prévoit des exceptions au traitement des données sensibles dans les cas suivants :

a – lorsque le titulaire a donné son consentement explicite à un tel traitement, sauf dans les cas visés par la loi de ne pas accorder une telle autorisation ;

b – lorsque le traitement est nécessaire pour protéger les intérêts vitaux d'un titulaire physiquement ou juridiquement incapable : dans ces cas précis, les représentants devront donner leur consentement ;

c – lorsque le traitement est effectué dans le cadre d'activités légitimes et avec des garanties appropriées par une fondation, ONG, association ou tout autre organisme à but non lucratif dont l'objectif est politique, philosophique, religieux ou syndical, mais les données ne peuvent être fournies à des tiers sans l'accord du titulaire ;

d - lorsque le traitement se réfère aux données nécessaires à la reconnaissance, à l'exercice ou à la défense d'un droit en justice ;

e – lorsque le traitement est réalisé à des fins historiques, statistiques ou scientifiques : dans ce cas, les mesures conduisant à la suppression de l'identité des titulaires doivent être prises[52].

Dans les cas autorisés par la loi, il faut informer le titulaire du caractère de donnée sensible des informations et de la possibilité qui lui est donnée de ne pas en autoriser le traitement, et lui préciser, dans le cas où il serait d'accord, que son consentement doit être expressément signifié.

---

[50] Article 5 et ss. Ley estatutaria 1581 DE 17 octobre 2012. Reglamentada parcialmente por el Decreto Nacional 1377 de 2013. Por el cual se dictan disposiciones generales para la protección de datos personales.

[51] La biometría es una palabra que proviene del griego *bio* (vida) y *metron* (medida), a través de esta disciplina es posible medir, analizar y posteriormente identificar cada individuo con el fin de conocer su identidad, gracias al uso de diferentes técnicas. Dentro de los parámetros biométricos se encuentran entre otros la huella digital, el iris del ojo, la identificación por voz, la identificación por los rasgos del rostro.

[52] Article 6. Ley estatutaria 1581 de 17 octobre 2012. Reglamentada parcialmente por el Decreto Nacional 1377 de 2013. Por el cual se dictan disposiciones generales para la protección de datos personales.

La protection des données sensibles est par ailleurs assurée, parce qu'aucune activité ne peut être subordonnée à l'autorisation du titulaire de fournir des données personnelles sensibles[53]. En d'autres termes, par exemple, sur Internet, aucun site ne peut refuser son entrée ou limiter son utilisation à un titulaire qui n'aurait pas fourni l'autorisation d'utiliser des données personnelles sensibles.

Lors de l'examen de constitutionnalité de la loi, la Cour constitutionnelle a considéré que les personnes qui effectuent des traitements dans ces cas particuliers ont une responsabilité renforcée qui se traduit par une augmentation des exigences, et qui devrait également se traduire par une sanction administrative et pénale en cas de manquement aux obligations[54].

D'autre part, la loi dispose que le traitement des données personnelles des enfants et des adolescents est interdit, à l'exception des données qui sont de nature publique[55]. Ainsi, les institutions de l'État et de l'éducation sont toutes liées à l'obligation d'information des représentants légaux et des tuteurs sur les risques potentiels pour les enfants et les adolescents concernant un éventuel traitement inapproprié de leurs données personnelles. Cette protection inclut des exceptions[56], dans le cas d'informations de nature publique, ou lorsque le traitement respecte les intérêts des enfants et des adolescents et que le respect des droits fondamentaux est assuré.

L'analyse de la protection des données à caractère personnel repose sur un examen des exigences suivantes :

1. Déterminer s'il s'agit d'une donnée personnelle. À titre d'exemple, une donnée utilisée avec à des fins statistiques n'est pas considérée comme une donnée personnelle s'il n'y a pas de liens entre l'information et la personne concernée, car l'identification du titulaire devient impossible.
2. Établir s'il existe un traitement de données personnelles, qu'il soit automatisé ou non.
3. Identifier qui est le responsable du traitement et, le cas échéant, qui est le sous-traitant.
4. Analyser si le champ d'application territorial est applicable.
5. Examiner si toutes les conditions de licéité du traitement des données à caractère personnel sont respectées, c'est-à-dire s'il existe une collecte de données loyale, licite, transparente, qui détermine de manière explicite les finalités du traitement. Il faut également examiner si le traitement de données personnelles est proportionnel, adéquat, pertinent et non excessif et si les données stockées qui font l'objet d'un traitement sont exactes, complètes

[53] Article 6. Decreto 1377 de 27 juin 2013, par lequel la loi de 20 121 581 est partiellement réglementée.

[54] Corte Constitucional de Colombia. Sentencia C-748/11. Magistrado Ponente: Jorge Ignacio Pretelt Chaljub. Bogotá D. C., 6 octobre 2011.

[55] Article 7. Ley estatutaria 1581 DE 17 octobre 2012. Reglamentada parcialmente por el Decreto Nacional 1377 de 2013. Por el cual se dictan disposiciones generales para la protección de datos personales.

[56] Article 12. Decreto 1377 de 27 juin 2013, par lequel la Loi de 20 121 581 est partiellement réglementée.

et à jour. Il faut observer encore si la durée de conservation des données ne dépasse pas le temps fixé pour la finalité du traitement. Il faut étudier enfin si la personne concernée a signifié son consentement expressément, de façon indiscutable, libre, spécifique et informée. Les conditions de licéité du traitement sont des exigences nécessaires et préalables qu'il faut considérer avant de regarder les formalités.

6. Après avoir examiné les critères ci-dessus, il est nécessaire de vérifier si les formalités requises par la loi ont été respectées, notamment si les droits des personnes concernées et les obligations du responsable de traitement ont été respectés. Enfin, il faudra examiner s'il y a lieu d'appliquer des sanctions ou d'effectuer des contrôles à la charge de l'autorité colombienne de contrôle homologue de la CNIL.

Les différents types d'information et ses modalités d'accès sont récapitulés dans le tableau suivant :

INFORMATION.	MODALITÉ D'ACCÈS.
INFORMATION PUBLIQUE LIBRE. DONNÉES OUVERTES	Information en libre accès sur Internet sans demande préalable nécessaire. La réutilisation de l'information est permise.
INFORMATION PUBLIQUE RÉSERVÉE. Données concernant la défense ou la sécurité nationale, la sécurité publique, les relations internationales, ou relatives à un délit commis, etc.	Information ne pouvant en aucun cas être mise en accès libre dans la mesure où cela peut nuire à l'intérêt public. Le refus doit être motivé et signifié par écrit.
INFORMATION PUBLIQUE CLASSIFIÉE. Données appartenant à la sphère privée d'une personne.	Information susceptible d'être restreinte sauf si la personne morale ou physique en a autorisé la publication. Une demande préalable est requise. La réponse, favorable ou défavorable, doit être motivée et signifiée par écrit. La demande d'information peut être refusée lorsqu'il y a risque portant sur la vie, la santé, la vie privée, ou la sécurité d'une personne physique. Elle peut être également refusée lorsque sont mis en jeu des secrets commerciaux, industriels et professionnels de personnes morales. Un recours est possible en cas de refus.

Comme l'on constate, les contours du secret administratif ne sont pas fixés par un texte de portée générale en Colombie. Ce qui reste clair c'est que la loi colombienne a encadré l'accès à l'information personnelle des individus, et qu'une analyse sur la qualification des données s'avère nécessaire, notamment aujourd'hui, quand on constate que les grandes entreprises du numérique bénéficient économiquement de l'information publique et privée.

§ 2 – LES DÉFIS DE LA MISE EN ŒUVRE DU DROIT D'ACCÈS À L'INFORMATION

En Colombie, l'encadrement du droit d'accès à l'information présente deux grands défis : la faculté d'accéder à l'information (A) et le risque de dénaturation du droit à savoir (B)

A) Les problématiques de l'accès à l'information

Parmi les problématiques qui se posent concernant le droit d'accès à l'information figurent la limitation injustifiée de l'accès à l'information et l'accès démesuré aux données à caractère personnel.

Concernant **la limitation injustifiée du droit d'accès,** on constate que la décision sur l'accès à l'information publique est un pouvoir de l'État : ainsi, le caractère discrétionnaire dans la prise de décisions sur l'accès est-il incontestable. Les sujets obligés ont la faculté de refuser l'accès.

Parmi les particularités de l'exercice du droit d'accès, on observe que le refus d'une demande d'information doit être soigneusement argumenté[57] ; que la charge d'apporter la preuve que l'information est soumise à réserve appartient à l'administration publique[58] ; qu'il est possible enfin de présenter un recours contre cette décision[59].

Comme il s'agit d'un droit fondamental, l'action de tutelle[60] prévue par le droit constitutionnel colombien est également valable pour demander la protection. Dans le même sens, la durée du maintien de l'information considéré comme réservée est de quinze ans[61]. Une sanction pénale[62] est également prévue dans les

---

57 Artículo 26. Ley 1712 6 de marzo 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. [En ligne]
http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882 Site consulté le 11 janvier 2016.

58 Artículo 28. Ley 1712 6 de marzo 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. [En ligne]
http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882 Site consulté le 11 janvier 2016.

59 Artículo 27. Ley 1712 6 de marzo 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. [En ligne]
http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882 Site consulté le 11 janvier 2016.

60 C'est une action propre du droit colombien qui a été créé pour protéger les droits fondamentaux.

61 Artículo 22. Ley 1712 6 de marzo 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. [En ligne]
http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882 Site consulté le 11 janvier 2016.

62 Artículo 29. Ley 1712 6 de marzo 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. [En ligne]
http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882 Site consulté le 11 janvier 2016.

cas de dissimulation, destruction ou altération totale ou partielle de l'information publique. Le défi sera alors d'effectuer un contrôle permanent sur les réponses données par l'administration publique aux titulaires du droit.

En outre, en ce qui concerne les limites au droit d'accès, la loi dispose que, pour l'exercice du droit, il faudra prendre en considération les limites raisonnables des ressources humaines, matérielles et financières. Cette restriction reste contestable, car la loi ne précise pas ce qu'il faut entendre par raisonnable, et cela peut servir d'excuse pour empêcher l'accès à certaines informations de l'État. Car la corruption se sert du secret : en Colombie, les données officielles sur la richesse n'étant pas accessibles, le contrôle des capitaux reste faible.

Concernant **l'accès démesuré aux données à caractère personnel,** l'administration publique et plus généralement les sujets obligés au respect de la loi sur la transparence et le droit d'accès à l'information stockent les données en dehors du territoire colombien. Dans le même sens, les grandes entreprises du numérique fournissent les services de traitement des données personnelles à l'État colombien. Dans ce sens, l'un des défis de la protection des données à caractère personnel concerne également l'internationalisation, car, dans la plupart des cas, le traitement des données détenues par l'administration publique ainsi que le stockage s'effectuent sur un autre territoire. De plus, grâce à la dématérialisation, l'utilisation des données est plus variée. Par exemple, l'utilisation du Cloud Computing rend difficile la protection des données, en raison du phénomène de la mondialisation et du système d'interconnexion.

L'utilisation des données à caractère personnel par les grandes entreprises d'Internet est également très variée et difficile à contrôler aujourd'hui. Ce qui reste clair, c'est qu'il y a une monétisation de l'audience grâce au modèle de gratuité. Ainsi, l'on constate la création de publicité ciblée, l'installation de cookies, la surveillance, la localisation et l'identification d'une personne concernée grâce à l'application du Big Data. Il est donc permis de se demander si les politiques de traitement et de stockage de données mis en place en Colombie par les sujets obligés protègent suffisamment les données personnelles. Les grandes entreprises prestataires de services d'Internet utilisent les données personnelles, afin d'identifier les personnes ou de connaître leur identité à partir de données biométriques qui analysent les caractéristiques biologiques (par exemple à travers la reconnaissance vocale) ou l'identification des caractéristiques faciales (par exemple à travers les photos). Ainsi, à partir de ces données, il est même possible de réaliser des prédictions par exemple sur les épidémies, s'agissant d'une vente massive de données personnelles aux assurances, pharmacies, etc. Ces données sont utilisées dans certains cas sans le consentement préalable de la personne concernée.

La loi ouvre la porte à un régime dérogatoire à l'interdiction du transfert international des données. Ainsi, dans le cas des

transferts requis par la loi pour protéger l'intérêt public ou pour la constatation, l'exercice ou la défense d'un droit dans une procédure judiciaire[63]. Cette exception ne précise pas ce que l'on doit entendre par protection de l'intérêt public. La jurisprudence constitutionnelle a analysé cette exception en considérant que

> « l'exception emploie des termes assujettis à des incertitudes et qui, compte tenu de son caractère large et ambigu, peuvent créer des problèmes au moment de son application. De plus, la Cour soutient que ce qui est en jeu c'est la régulation du droit fondamental à l'habeas data, donc, que les limites à son exercice par la consécration d'exceptions doivent être précises, sans utiliser des concepts qui ont un certain degré d'incertitude, ce qui peut compromettre l'exercice ou la jouissance d'autres droits constitutionnels »[64].

En outre, un aspect qui révèle l'inefficacité des politiques de stockage de données de la part de l'administration publique concerne l'existence de grandes quantités d'informations : cela rend difficile le contrôle efficace qui doit être effectué par l'autorité chargée de la protection des données.

En raison du volume important des données stockées aujourd'hui, qui ne cesse de s'accroître, on assiste à une difficulté majeure de contrôle efficace sur l'utilisation de ces données. Selon une étude financée par EMC (entreprise prestataire des services de cloud computing et Big Data) et Gartner Inc. (société de conseil dans le domaine des technologies de l'information), les données numériques ont dépassé 2,7 zettaoctets en 2012[65]. Pour mesurer la quantité de données uniquement sur Facebook, 10 téraoctets sont créés chaque jour, et 7 téraoctets en ce qui concerne Twitter[66], l'administration publique est également face à la même problématique.

L'usage du Big Data[67] est très varié. Dans le secteur public, les États-Unis investissent dans des projets relatifs au Big Data afin de contrôler les utilisateurs d'Internet. À l'heure actuelle, l'Agence de sécurité nationale (NSA) est en train de construire un centre de données capable de stocker yottaoctets d'informations collectées sur Internet[68]. L'utilisation des données personnelles par l'autorité

---

63 Article 26. Ley estatutaria 1581 DE 17 octobre 2012. Reglamentada parcialmente por el Decreto Nacional 1377 de 2013. Por el cual se dictan disposiciones generales para la protección de datos personales.

64 Corte Constitucional de Colombia. Sentencia C-748/11. Magistrado Ponente : Jorge Ignacio Pretelt Chaljub. Bogotá D. C., 6 octobre 2011.

65 C. Rogawski,"The GovLab Index: The Data Universe", 22 de agosto de 2013: http://thegovlab.org/govlab-index-the-digital-universe/ (consulté en ligne le 28 août 2014).

66 CNRS Centre National de Recherche Scientifique, *International magazine « The Big Data revolution »,* n° 28, January 2013.
http://www.cnrs.fr/fr/pdf/cim/28/#/1/(consulté en ligne le 28 septembre 2014).

67 Le phénomène du Big Data désigne la croissance exponentielle des données qui dépasse la capacité de stockage d'un logiciel classique.

68 J. BAMFORD, "The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)", 15 de marzo de 2012: http://www.wired.com/2012/03/ff_nsadatacenter/all/ (consulté en ligne le 26 septembre 2014.

publique doit également respecter la réglementation, car, bien qu'elle puisse effectuer un traitement de données, il est indispensable qu'elle recueille le consentement éclairé de la personne concernée. De plus, l'autorité publique ne doit pas outrepasser les finalités légitimes pour lesquelles le titulaire a donné l'autorisation.

Toutes ces multiples utilisations des données personnelles traduisent un manque de protection de l'information publique classifiée, les cas cités n'étant que des exemples de l'usage actuel de nos données. En effet, les différentes modalités d'utilisation des données restent encore méconnues des usagers et des experts informaticiens.

La protection des données à caractère personnel, comme tous les autres droits, n'a pas un caractère absolu et on trouve des limites tout particulièrement dans d'autres droits comme la liberté d'expression et le droit à l'information[69]. Il est donc possible de se trouver dans certaines situations, face à une certaine limitation de l'exercice du droit à la protection des données personnelles. Comme il a été dit précédemment, en Colombie, le droit à l'information est garanti par la Constitution[70].

Le conflit entre le droit à la vie privée et le droit à l'information n'est pas seulement un conflit entre une donnée privée ou publique ; c'est aussi une question de compréhension entre les différentes traditions et cultures. En effet, ce débat dépend aussi de l'importance que chaque société donne aux divers principes mis en cause. Par exemple, le critère pour résoudre le conflit entre ces deux droits en Colombie serait celui de l'intérêt général, dans le cas où l'information que l'on prétend publier apparaît réellement importante pour l'opinion publique où le droit de l'information s'imposerait alors[71].

À titre d'exemple jurisprudentiel, la Cour constitutionnelle de Colombie s'est prononcée à propos de l'accès indiscriminé aux données négatives, concrètement sur les sanctions effectuées à la personne concernée, en considérant que la publication indiscriminée des antécédents pénaux n'a pas une finalité légale ou constitutionnelle. Dans ce cas, elle a déterminé que cette information facilite l'usage incontrôlé du pouvoir informatique, ce qui constitue une barrière pour l'accès et la conservation du travail pour les personnes concernées et qui facilite les pratiques d'exclusion sociale et la discrimination interdites par la

---

[69] Constitution politique de Colombie. Article 20 « toute personne à la liberté d'exprimer et de diffuser ses idées et ses opinions, d'informer et de recevoir des informations véridiques et impartiales… ».

[70] Corte Constitucional de Colombia. Sentencia C-592/12 Magistrado Ponente: Jorge Iván PALACIO PALACIO. Bogotá D.C., 25 juillet 2012. « Par conséquent, la Cour a souligné l'importance et la signification de cette liberté, qui protège non seulement le droit de diffuser et d'exprimer des opinions et des idées, ou la liberté d'expression au sens strict, mais aussi la possibilité de rechercher, de recevoir et de répandre des informations de toute nature, ou le droit et la liberté d'informer et d'être informé ».

[71] M. A. ITURRALDE, *La libertad de información frente al derecho a la intimidad: el dilema entre una sociedad informada y el derecho a la soledad,* Revista Tutela, Acciones Populares y de Cumplimiento #7. Julio de 2000. Pág. 1525 y ss.

Constitution. Par contre, le cas de la circulation de l'information sur les antécédents pénaux en cas de protection des enfants peut être considéré comme une exception possible, par exemple en cas de délits sur la liberté sexuelle[72].

Si l'on choisit de faire prévaloir l'intérêt général, il est indispensable d'identifier ce qui est au cœur du droit[73], c'est-à-dire cette partie du contenu qui est absolument nécessaire pour que les intérêts juridiquement protégés soient réels, concrets et efficacement protégés. De même, en ce qui concerne le contenu de l'information, la Cour a expliqué « qu'il est également impératif que le contenu de l'information obéisse à un intérêt public véritable et légitime conformément à la signification et à l'impact social »[74].

Il faut continuer à défendre l'idée que les données personnelles sont un attribut de la personnalité. Il est également essentiel d'assurer la liberté d'utilisation des outils technologiques tout en garantissant la vie privée des personnes et de lutter contre les « paradis » de données personnelles situés dans plusieurs pays du monde. Ces questions devraient faire partie de l'objectif principal de la législation en Colombie et à l'étranger.

Dans le même sens, la réutilisation des données à caractère personnel à des fins illégitimes doit être contrôlée et interdite, même si c'est l'État qui utilise l'information. Car l'administration publique est en mesure de contrôler les données des citoyens et de garder les secrets sur l'information dont ils disposent. Ainsi, il est indispensable de trouver les moyens de protéger les informations à caractère personnel des citoyens, par exemple en employant des moyens cryptographiques[75].

B) Le risque de dénaturation du droit d'accès à l'information publique

Comme on l'avait évoqué, contrairement à l'information publique classifiée et l'information publique réservée, l'on trouve les données dites ouvertes. Ces données ont été cataloguées comme étant de libre accès sans qu'aucune demande préalable ne soit

[72] Corte Constitucional de Colombia. Sentencia SU458/12. Magistrado ponente: Adriana Maria Guillén Arango. Bogotá D.C. 21 juin 2012.

[73] En espagnol: *el núcleo esencial del derecho.* Corte Constitucional de Colombia. Sentencia C-756/08. Magistrado Ponente: Marco Gerardo Monroy Cabra. Bogotá D.C., 30 juillet 2008. « Il existe principalement deux critères utilisés pour déterminer l'essence d'un droit fondamental : i) font partie du noyau essentiel du droit, les caractéristiques et les facultés qui identifient le droit, sans lesquelles le droit aurait une dénaturation, ii) font partie cette partie essentielle du droit également, les compétences qui donnent la possibilité d'exercer le droit, de manière à ce que, s'il y a limitation, le droit fondamental devienne impraticable. Cela explique pourquoi le législateur constitutionnel exigeait que l'âme essentielle des droits fondamentaux soit soumise à la réserve de la loi statutaire. Il est clair que, l'écart entre la limitation légitime du noyau et son annulation (qui pour ce fait serait contraire à la Constitution) n'est pas seulement sensible, mais il est indispensable d'avoir un débat législatif responsable, conscient et fondé qui soutient la décision ».

[74] Corte Constitucional de Colombia. Sentencia SU-1723. Magistrado ponente: Alejandro Martínez Caballero. Bogotá D.C., 12 décembre 2000.

[75] Idée proposée par Julien Assange.

requise. La réutilisation des données ouvertes est admise, et il est possible de créer un service dérivé de la réutilisation des données[76].

Bien que cette liberté existe, les titulaires du droit d'accès sont obligés d'effectuer un emploi responsable et légitime de ces données, notamment quand il s'agit d'information publique classifiée et publique réservée. Ce principe a été consacré par la loi et il constitue la base fondamentale pour empêcher la dénaturation du droit à savoir.

Le droit d'accès aux documents publics doit garantir l'une de ces trois fonctions essentielles : assurer la participation démocratique et l'exercice des droits politiques ; permettre la matérialisation d'autres droits constitutionnellement reconnus ; garantir la transparence de la gestion publique et le contrôle de l'activité de l'État effectué par les citoyens.

En dehors de ses finalités, une utilisation des données à des fins différentes risque de dénaturer l'exercice du droit : par exemple, la monétisation de l'information ne constitue pas une finalité légitime à l'origine du droit à savoir. La réutilisation des données effectuée à des fins de surveillance et de monétisation des données personnelles est contraire aux finalités légitimes, même si elle est effectuée par l'État.

L'accès à l'information publique a pour objectif de garantir un droit fondamental des citoyens de connaître les différentes actions de l'administration publique ; cependant, cet objectif de transparence a été déformé par la réutilisation des données publiques à des fins purement économiques. Cette problématique se développe encore plus aujourd'hui, par exemple avec l'émergence du Big data et des techniques de reconnaissance biométrique. On le constate dans le domaine des données à caractère personnel et dans le domaine des données publiques, avec la réutilisation des données, où il est possible de rajouter une valeur aux données. Ce sujet est encore discuté, car, par exemple, grâce à l'utilisation du Big data, il est possible d'avoir accès à d'autres informations à partir des données publiques et de créer de nouvelles données.

En outre, le droit d'accès comprend également le droit de diffuser l'information de manière responsable, ce qui implique que la diffusion de l'information soit effectuée en respectant fidèlement le contenu et le contexte d'origine, afin d'empêcher la confusion et la désorientation. Ainsi, le contrôle sur l'utilisation ultérieure des données s'avère indispensable. La réutilisation des données « *implique aussi que leur qualité et leur intégralité soient garanties et que les jeux de données réutilisables comportent des éléments de contextualisation et*

[76] Artículo 6. J. Ley 1712 6 de marzo 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. [En ligne] http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882 Site consulté le 11 janvier 2016.

de description (métadonnées) permettant leur intelligibilité»[77]. La dénaturation des informations publiques devrait faire l'objet de sanction, sauf si elle est autorisée par l'administration dans le respect de la réglementation en vigueur.

Il est important de préciser que la réutilisation des données ne constitue pas une problématique en soi : la difficulté se trouve dans la finalité pour laquelle on réutilise les données. Si l'objectif poursuivi est, par exemple, de surveiller illégalement, on pourrait considérer qu'il existe une dénaturation du droit d'accès à l'information publique. En revanche, si la réutilisation des données publiques englobe une finalité universitaire ou scientifique, telle que la recherche publique ou l'élaboration de statistiques, dans ce cas il serait possible de considérer que cette finalité est légitime.

La réutilisation de l'information publique comportant des données personnelles doit respecter la réglementation en vigueur. Ainsi, l'on ne peut pas se prévaloir du droit d'accès à l'information publique pour réutiliser l'information à des finalités contraires aux principes directeurs de la loi de protection des données à caractère personnel. Il est important de promouvoir un droit de savoir libre, mais responsable, en protégeant la vie privée des individus. L'intérêt doit être concentré non seulement sur la finalité de la réutilisation, mais sur le type d'information réutilisé.

La personne concernée doit donner son accord si la finalité du traitement ultérieur est différente[78]. Par exemple, concernant la réutilisation des données personnelles détenues par l'administration publique, un site privé a publié sur internet toutes les données des avocats colombiens avec leur numéro d'identité professionnelle et leur numéro de carte d'identité, sans leur consentement. Cette information a été finalement effacée pour violation de la protection des données à caractère personnel.

Deux remarques peuvent être apportées pour conclure. Il subsiste encore aujourd'hui des zones grises dans la loi sur la transparence ainsi que des pratiques de restriction d'information. D'autre part, il est permis de se demander si la protection de la vie privée des individus demeure efficace devant le progrès des technologies de l'information, le respect et la transparence dans les pays tiers, l'utilisation des données par les géants d'Internet qui détiennent le monopole, la capacité des autorités publiques d'identifier et de sanctionner les manquements à la loi et la possibilité qu'ont les personnes concernées de faire valoir leurs droits.

[77] P. CANACAGGIO, *Vers un droit d'accès à l'information publique. Les avances récentes des normes et des pratiques*. UNESCO. 2014.

[78] http://www.gfii.fr/uploads/docs/la-reutilisation-des-donnees-publiques-un-enjeu-majeur-pour-la-societe-europeenne-de-l-information.pdf