Projet d'appui aux instances indépendantes en Tunisie

Financé par l'Union européenne et le Conseil de l'Europe

UNION EUROPÉENNE

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Mis en œuvre par le Conseil de l'Europe

ETUDE COMPARATIVE SUR L'ARTICULATION DES DROITS D'ACCÈS À L'INFORMATION ET DE PROTECTION DES DONNÉES

Bertil Cottier
Professeur honoraire
Faculté de droit de l'Université de Lausanne (Suisse)

Novembre 2021

Cette étude a été réalisée avec le support du programme co-financé par l'Union européenne et le Conseil de l'Europe sous le programme PAII-T. L'Union européenne et le Conseil de l'Europe ne sont pas responsables du contenu de cette étude ou de l'utilisation des données y figurant.

ETUDE COMPARATIVE SUR L'ARTICULATION
DES DROITS D'ACCÈS À L'INFORMATION ET DE PROTECTION DES DONNÉES

Table des matières

1. Introduction

1.1. Mandat

La présente étude a été commanditée par le Conseil de l'Europe dans le cadre du programme de coopération « Appui aux Instances indépendantes en Tunisie ».

Destinée principalement à l'Instance nationale d'accès à l'information (INAI) et à l'Instance nationale de protection des données (INPDP), elle présente, sous forme synthétique et comparative, différents mécanismes législatifs tendant à concilier les droits d'accès à l'information et de protection des données.

1.2. Champ de recherche

Il aurait été vain d'examiner les mécanismes de conciliation institués par les quelque trois cents législations sur la publicité des documents administratifs et sur la protection des données recensées de par le monde.[1] La présente étude se focalisera sur les solutions consacrées par législateurs étrangers qui disposent déjà d'une certaine pratique de la problématique ou qui ont mis en œuvre des mécanismes originaux. Le cas échéant, elle abordera aussi les deux conventions du Conseil de l'Europe portant sur la thématique de cette étude – à savoir la Convention 205 sur l'accès aux documents publics[2] et la Convention 108 sur la protection des données,[3] car elles font respectivement droit, de manière croisée, aux dispositions l'une de l'autre.

Quoi qu'il en soit, ces mécanismes n'instituent pas seulement des « règles de conflit » dont la vocation est de déterminer dans quelle mesure la protection des données restreint le droit d'accès, mais aussi des normes de droit procédural. En conséquence la présente étude ne se contentera pas de passer en revue divers modèles de telles règles (3), mais abordera aussi ces questions d'ordre pratique que sont l'existence d'un droit d'être entendu de la personne concernée (4) ou les interactions entre l'instance de protection des données et l'instance en charge de l'accès aux documents publics (5).

On notera que la problématique de l'articulation entre droit d'accès et protection des données concerne la possibilité ou non de prendre connaissance, au nom de la transparence des activités

[1] Le nombre peut paraître élevé, mais il tient compte du fait que dans les États fédéraux, il appartient aux entités fédérées (telles les provinces canadiennes et australiennes, les *Länder* allemands, ou encore les cantons suisses) de régler de manière autonome le sort des informations qu'elles détiennent ; partant chacune d'elles a adopté ses propres règles sur la protection des données et l'accès aux documents administratifs.

[2] Convention sur l'accès aux documents administratifs du 18 juin 2009 (STE 205 ; aussi appelée convention de Tromsø).

[3] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981 (STE 108) ; ce texte a fait l'objet d'une profonde modernisation par le biais du Protocole d'amendement du 10 octobre 2018 (STE 223).

des autorités publiques, de documents contenant des données personnelles. L'usage que le requérant fera par la suite des données personnelles obtenues est une question qui échappe à la législation sur le droit d'accès ; par contre elle ressortit pleinement à la législation sur la protection des données.[4]

1.3. Remarques formelles

Terminologie : pour des raisons de clarté, le terme *requête* désignera systématiquement et sans autre précision, une demande d'accès fondée sur la législation sur la publicité des documents administratifs, le terme *requérant* la personne qui fait une demande d'accès et le terme *autorité requise*, l'autorité publique appelée à se prononcer sur la requête. En outre, le terme *personne concernée* se rapporte à la personne dont les données tombent sous le coup de la législation sur la protection des données, c'est-à-dire une personne qu'il est possible d'identifier directement ou indirectement[5].

Citations : à chaque fois, les dispositions pertinentes seront citées en langue originale, pour autant que celle-ci soit le français ou l'anglais. Si tel n'est pas le cas, la présente étude se fondera sur une traduction dans l'une ou l'autre de ces deux langues officielles du Conseil de l'Europe.

Liens hypertextes : pour ne pas alourdir la présente étude par des annexes reproduisant les divers textes législatifs et rapports officiels auxquels l'étude fait référence, des liens hypertextes permettent au lecteur de les consulter directement à l'écran.

2. Exposé du problème

2.1. Deux institutions en opposition

Les relations entre droit d'accès à l'information détenues par les autorités publiques et protection des données personnelles ont de tout temps été conflictuelles.

D'un côté, il en va de la libre circulation de l'information et du débat d'idées ainsi que du contrôle citoyen sur l'État et ses organes ; inutile de préciser qu'en ces temps de désinformation et de manipulation de l'opinion, il est plus que jamais d'importance que la population puisse bénéficier de connaissances exactes et complètes sur les activités des autorités.[6]

---

[4] Le cas échéant aux réglementations qui régissent la communication proactive de l'État (notamment *l'open data*) ; ces réglementations contiennent entre autres des normes sur la réutilisation des données publiques.

[5] Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel (Convention 108+), Rapport explicatif, paragraphe 17

[6] La liberté de médias, la confiance du public et le droit de savoir des citoyens, Rapport de la Commission de la culture, de la science, de l'éducation et des médias de l'Assemblée parlementaire du Conseil de l'Europe, Doc. 15308, 7 juin 2021, chiffre 3.

De l'autre côté, c'est le droit à l'autodétermination informationnelle qui est en jeu, par quoi il faut entendre le droit pour la personne concernée de pouvoir déterminer elle-même si et dans quels buts des informations à son sujet peuvent être traitées. Au-delà de cette valeur de consécration récente[7], c'est plus généralement la protection de la sphère privée des individus qui est sur la sellette. Cela dit, on ne saurait oublier que la protection de la vie privée ne doit pas servir de paravent à l'administration pour occulter « des informations compromettantes, des conflits d'intérêts potentiels, d'éventuels arrangements entre camarades, des vérités dérangeantes, voire de véritables affaires de corruption ».[8]

2.2 Une opposition relative

Reste que l'antagonisme entre droit d'accès et protection des données ne doit pas occulter une finalité commune : l'un et l'autre tendent à rendre l'État redevable (au sens de l'anglais *accountable*) des informations qu'il détient ; ne pouvant plus en disposer selon son bon vouloir, il est soumis à des obligations quant à leur collecte, leur conservation, leur exploitation et leur communication. Partant, les règles sur l'accès à l'information et celles sur la protection des données concourent, ensemble mais chacune à sa manière, à définir un statut de l'information publique.

Soucieux de donner corps à ce statut de l'information publique, plusieurs juridictions ont réuni les règles sur le droit d'accès à l'information et celles sur la protection des données au sein d'un seul et même texte législatif, à l'image de la province canadienne du Québec dont la loi de 1982 sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels fit œuvre de pionnier. Parachevant cette logique unitaire, le canton suisse du Valais a inséré dans sa loi topique les règles sur l'archivage des documents officiels (cf. la loi sur l'information du public, la protection des données et l'archivage de 2008).

Reste que réunion au sein d'un texte commun ne rime pas avec fusion : à chaque fois, la protection de données et la transparence font l'objet de corpus législatifs propres au sein de

[7] Consacré pour la première fois par la Cour constitutionnelle allemande sous le nom de *Recht auf informationelle Selbstbestimmung* (« Volkszählungsurteil », BVerfGE, vol. 65 [1983], p. 1 ss), ce principe est désormais reconnu par la Cour européenne des droits de l'Homme (*Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande* [GC], n° 931/13, 27 juin 2017, ad 137), par la jurisprudence de nombreux pays européens ainsi que par la Convention modernisée du Conseil de l'Europe sur la protection des personnes à l'égard du traitement des données à caractère personnel (Convention 108+) dans son préambule.

[8] FLÜCKIGER ALEXANDRE, La transparence des données personnelles au service de l'intégrité de l'administration, in : Annuaire de l'Association suisse du droit public de l'organisation 2019-2020, Berne 2020, p. 79. Dans le même sens, les Lignes directrices sur la protection de la vie privée dans les médias, Conseil de l'Europe, Strasbourg 2018, p. 11 : « la liberté d'expression recevrait un coup fatal si des personnalités publiques pouvaient censurer la presse et le débat public au nom des droits de la personnalité ».

subdivisions distinctes de la loi unitaire.[9] Distinctes, car, hormis des champs d'application ou des concepts communs (tel celui de donnée personnelle), les deux domaines ne se recoupent qu'en partie : « Le droit d'accès et l'information du public ne concernent pas en priorité des données personnelles, mais des documents dont le contenu informationnel essentiel est souvent indifférent sous l'angle de la protection des données. A l'inverse, la protection des données ne consiste pas uniquement à poser des limites à la diffusion au public de ces données ; elle s'étend à différentes questions telles que leur collecte, leur usage interne, leur communication à des personnes privées ou à d'autres administrations, leur destruction ou la possibilité pour les personnes concernées de pouvoir les vérifier et rectifier au besoin. »[10]

Dès lors, il importe finalement peu que la protection des données et la transparence soient régies par des lois séparées ou par des chapitres séparés au sein d'une loi unitaire : dans les deux cas le législateur ne peut pas faire l'impasse sur des règles de coordination.

2.3. Résoudre le problème

Si la réunion des règles sur l'accès aux documents administratifs et des règles sur la protection des données au sein d'une loi unitaire ne permet pas, à elle seule, d'éviter le conflit, il en va autrement de deux autres « remèdes » : le consentement de la personne concernée d'une part, ou l'anonymisation du document requis d'autres part.

2.3.1. Le consentement

Toutes les législations examinées font du consentement un sésame qui habilite l'autorité requise à donner une suite favorable à la requête d'accès (à condition bien entendu qu'il n'y ait pas d'autres motifs de secret, telle la sécurité intérieure ou la protection des secrets d'affaires). D'ordinaire, la validité du consentement est déterminée par les règles générales en la matière posées par la législation sur la protection des données. Certains États ont toutefois posé des règles particulières en matière d'accès aux documents administratifs admettant un consentement tacite lorsque celui-ci peut être déduit des circonstances, notamment lorsque la personne concernée a fait circuler des informations personnelles sur les réseaux sociaux.

---

[9] Notable exception, le canton suisse de Zurich. Sa loi sur l'information et la protection des données de 2007 fusionne au sein d'un seul et même chapitre les règles sur le droit général d'accès basé sur la transparence et le droit spécial d'accès de la personne concernée à ses propres données (cf. art. 20ss).

[10] VOLLERY LUC, La loi fribourgeoise sur l'information et l'accès aux documents, Revue Fribourgeoise de Jurisprudence 2009, 370, note 68. Voir aussi : *Human Dynamics Consulting, Legal balance of interests between transparency of public life and data protection* (project supported by the EU), « *An act that covers both areas comprehensively will need to be almost as detailed as two single acts because there is little overlap (except for the definitions and the oversight body*) (traduction non officielle : Une loi qui porte extensivement sur les deux domaines devra être presque aussi détaillée que deux lois distinctes car les chevauchements sont peu nombreux (sauf pour les définitions et l'organe de contrôle)", p. 6.

- Exemple : l'art. 19 al. 1 litt. b et c de la loi fédérale suisse sur la protection des données dispose que : « Les organes fédéraux ne sont en droit de communiquer des données personnelles qu'à l'une des conditions suivantes. (…) b. la personne concernée y a, en l'espèce, consenti ; c. la personne concernée a rendu ses données accessibles à tout un chacun et ne s'est pas formellement opposée à la communication.

2.3.2. L'anonymisation

Cette opération consiste à éliminer les données permettant d'identifier la personne concernée, soit directement (nom, numéro de contribuable ou d'assuré, etc.), soit indirectement (caractéristiques physiques ou corrélation d'informations contextuelles). Généralement, pareille élimination des identifiants s'effectue par caviardage ou par suppression pure et simple. Vide de données personnelles, le document ne tombe plus sous le coup de la loi sur la protection des données, partant aucun obstacle de cet ordre ne s'oppose à sa remise au requérant.

L'anonymisation soulève cependant deux problèmes. D'abord il importe que cette intervention soit reconnaissable. En effet, le requérant doit être en mesure de se rendre compte qu'il n'a pas en mains l'intégralité du document requis ; le cas échéant, il pourra recourir contre ce qui doit être considéré comme un accès partiellement refusé.

Ensuite, il peut arriver que l'anonymisation s'avère déraisonnable ou disproportionnée. Il en est ainsi lorsque les éliminations sont si nombreuses que le document requis en devient incompréhensible ou lorsque le travail nécessaire à l'élimination de tous les identifiants (notamment indirects) est considérable. De plus, comme le souligne le rapport explicatif de la Convention 108+, la combinaison de différents types de données peut permettre la réidentification d'une personne, déqualifiant ainsi l'anonymisation.[11] Il en est aussi ainsi dans le cas, de loin le plus fréquent, où le requérant souhaite expressément consulter des documents afférents à une ou des personnes nommément désignées. Dans ces trois hypothèses, l'anonymisation n'entre plus en considération ; l'autorité requise n'a alors d'autre choix que d'examiner la requête à la lumière des règles destinées à concilier droit d'accès et protection des données.

3. Les règles de conflits destinées à concilier droit d'accès et protection des données

3.1. Le paradigme : le compromis

Les premiers pays à être confrontés à l'antagonisme entre accès aux documents administratifs et protection des données ont résolu le conflit sans nuance, en donnant la primauté à l'une des

[11] Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel (Convention 108+), Rapport explicatif, paragraphe 19

deux institutions sur l'autre. Pays pionnier en matière de transparence, la Suède a d'emblée accordé la priorité à la transparence, au motif qu'il ne saurait être dérogé à une institution qui, en deux siècles, s'était imposée comme un pilier de la démocratie nationale.[12] A l'inverse la France, qui a toujours été soucieuse de protéger la personnalité de ses citoyens[13], a consacré la primauté de la protection des données : l'article premier de la loi sur l'accès aux documents administratifs de 1978 excluait du champ d'application de la publicité les données nominatives.

Des solutions aussi absolues ne sont aujourd'hui plus de mise. Partout, des compromis, plus ou moins heureux, ont été trouvés afin d'accorder transparence et protection des données.[14] Une approche conciliatrice est expressément préconisée par le Règlement européen de protection des données de 2016[15] ; son article 86 souligne effet que « Les données à caractère personnel figurant dans des documents officiels détenus par une autorité publique ou par un organisme public ou un organisme privé pour l'exécution d'une mission d'intérêt public peuvent être communiquées (…) afin de concilier le droit d'accès du public aux documents officiels et le droit à la protection des données à caractère personnel au titre du présent règlement». Cela dit, si le droit communautaire enjoint les États membres à adopter des règles de conflit, il leur laisse en revanche pleine latitude quant à déterminer la mesure et la forme du compromis préconisé.

Il en va de même s'agissant du Conseil de l'Europe ; la Convention 205 sur l'accès aux documents administratifs enjoint, par la voie de son rapport explicatif, les États membres à consacrer un compromis, tout en demeurant muette sur sa teneur : « Les documents contenant des données personnelles entrent dans le champ d'application de cette Convention. La Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981 (STE 108) n'interdit pas, en principe, l'accès de tiers à des documents contenant des données personnelles ».[16] Quant à Convention sur la protection des données, modernisée en 2018, elle « permet de prendre en compte, dans la mise en œuvre des règles qu'elle fixe, le principe du droit d'accès aux documents officiels ».[17]

---

[12] On sait que la Suède fut le premier pays au monde, en 1766, à avoir consacré la transparence des autorités publiques (voir le chapitre II de la loi organique sur la liberté de la presse) ; on sait moins que c'est aussi le premier pays à avoir adopté, en 1973, une loi sur la protection des données.

[13] On rappellera que la France fut le premier pays à incriminer la publication d'informations attentatoires à la vie privée (art. 11 de la loi sur la liberté de la presse de 1868).

[14] Sauf en Suède où le législateur, contre l'avis de l'instance nationale de protection des données, persiste à donner la priorité à la transparence : l'art. 7 chapitre 1 de la loi 2018 :218 de mise en œuvre du RGPD dispose que : « Le règlement européen sur la protection des données et la présente loi ne s'appliquent pas dans la mesure où ils entreraient en conflit avec la loi sur la liberté de la presse ou la loi fondamentale sur la liberté d'expression ».

[15] Règlement 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après RGPD).

[16] La Convention du Conseil de l'Europe sur l'accès aux documents publics et son rapport explicatif, Strasbourg 2019, p. 25.

[17] La Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel (Convention 108+), préambule.

Quant seul texte de droit international global qui traite du droit d'accès aux documents officiels, la Convention des Nations Unies de 1998 sur l'accès à l'information en matière d'environnement (aussi appelée Convention d'Aarhus), il envisage le conflit, mais renvoie expressément au droit interne des États membres pour déterminer dans quelle mesure les données personnelles requises doivent rester confidentielles (art. 4 al. 4 litt. f).

Au vu de l'incertitude que le droit international, global ou régional, laisse planer sur la manière de résoudre le conflit entre droit d'accès et protection des données, on comprendra aisément que le paradigme du compromis se décline différemment d'un État à l'autre.

3.2. Les mécanismes de compromis

3.2.1. L'approche concrète et l'approche abstraite

Si les différences sont nombreuses, elles tiennent toutefois souvent à des questions de détails. De fait, il n'y a pas autant de mécanismes de compromis que d'États concernés par le conflit entre le droit d'accès et protection des données. Tous les mécanismes mis en œuvre se rattachent, peu ou prou, à l'une ou l'autre des deux approches fondamentales suivantes :

- *L'approche abstraite* (aussi appelée méthode des normes fixes) : le législateur énumère les types de données personnelles et/ou les types de documents renfermant des données personnelles qui d'entrée de cause sont inaccessibles (liste positive) ou, inversement, publics (liste négative) ; on notera qu'une liste combinant énumération positive et énumération négative est parfaitement possible.

    - Exemple de liste négative : L'art. 6 de la loi norvégienne sur l'accès à l'information interdit, entre autres, l'accès aux dossiers de candidature à des concours officiels ainsi qu'aux photographies d'individus contenues dans des registres officiels.

    - Exemple de liste positive : L'art. 57 de la loi québécoise sur l'information dispose que : « Les renseignements personnels suivants ont un caractère public :

      1° le nom, le titre, la fonction, la classification, le traitement, l'adresse et le numéro de téléphone du lieu de travail d'un membre d'un organisme public, de son conseil d'administration ou de son personnel de direction et, dans le cas d'un ministère, d'un sous-ministre, de ses adjoints et de son personnel d'encadrement ;

      2° le nom, le titre, la fonction, l'adresse et le numéro de téléphone du lieu de travail et la classification, y compris l'échelle de traitement rattachée à cette classification, d'un membre du personnel d'un organisme public ;

      3° un renseignement concernant une personne en sa qualité de partie à un contrat de services conclu avec un organisme public, ainsi que les conditions de ce contrat ;

4° le nom et l'adresse d'une personne qui bénéficie d'un avantage économique conféré par un organisme public en vertu d'un pouvoir discrétionnaire et tout renseignement sur la nature de cet avantage ;

5° le nom et l'adresse de l'établissement du titulaire d'un permis délivré par un organisme public et dont la détention est requise en vertu de la loi pour exercer une activité ou une profession ou pour exploiter un commerce. »

- *L'approche concrète* : le législateur s'abstient de trancher lui-même le conflit, mais prescrit à l'autorité requise de se prononcer sur l'accessibilité ou non d'une donnée personnelle sur la base d'une pondération de l'intérêt à la transparence et de l'intérêt à la protection des données personnelles[18] en fonction des circonstances du cas d'espèce.

  - Exemple : L'art. 5 (*Protection of personal data*) de la loi allemande de 2005 sur l'accès à l'information détenue par les autorités fédérales dispose que : « *Access to personal data may only be granted where the applicant's interest in obtaining the information outweighs the third party's interests warranting exclusion of access to the information* (…) ». [19]

Très souvent la jurisprudence a apporté des précisions sur la manière de procéder à la balance des intérêts en accordant à certaines circonstances personnelles un poids plus grand dans la balance des intérêts.

- Ainsi les tribunaux suisses attachent une grande importance au rôle joué par la personne concernée dans la société : plus ses fonctions ou sa position hiérarchique sont élevées, plus elle devra tolérer que ses données personnelles soient révélées. Il en va de même de celui qui bénéficie de subventions publiques (ou d'autres avantages tel qu'un contrat de mandat). En revanche, la vulnérabilité de la personne concernée, l'intensité de l'atteinte à la personnalité ou encore la sensibilité de l'information requise feront pencher la balance vers l'occultation.[20]

- Le commissaire à l'information de la Slovénie, pour sa part, juge l'intérêt public très élevé lorsque l'information requise relève d'une question qui suscite un large

[18] On relèvera que souvent la norme de conflit ne fait pas expressément référence à la protection des données mais mentionne, plus généralement, la protection de la vie privée ; dans ce cas, la doctrine et/ou la jurisprudence ont intégré la protection des données personnelles dans le concept générique de vie privée.

19 « L'accès aux données personnelles peut seulement être accordé si l'intérêt du requérant à obtenir l'information surpasse l'intérêt de la tierce personne à ce qu'elle soit exclue de l'accès à l'information » (traduction non officielle)

[20] Emblématique de cette approche nuancée est le sort réservé à une demande d'accès à la liste des emplois accessoires de fonctionnaires fédéraux : les informations relatives aux cadres supérieurs furent transmises au requérant, celles relatives aux employés subalternes lui furent refusées (Tribunal administratif fédéral, A-6738/2014 du 23 septembre 2015).

> débat public, lorsqu'elle affecte un cercle étendu de personnes ou d'entreprises, lorsqu'elle est indispensable pour comprendre les tenants et aboutissants d'une décision prise ou encore lorsque la santé publique, la sécurité publique ou les finances publiques sont en jeu.[21]

On relèvera enfin l'intéressante initiative du Ministère de la justice britannique qui a établi, à l'intention des unités administratives nationales, un vade-mecum des questions que doit nécessairement se poser l'autorité requise lorsqu'elle procède à une balance des intérêts. En bref, on retiendra que, entre autres, celle-ci doit prêter une grande attention à la manière dont l'information personnelle a été obtenue (source, modalités de collecte notamment), aux attentes en matière de confidentialité de la personne concernée et aux conséquences négatives, pour la personne concernée, qu'auraient une communication.[22]

3.2.2 Evaluation sommaire des deux approches

L'approche abstraite a pour elle la clarté et la prévisibilité : pour chaque type d'information de nature privée, le législateur arbitre lui-même le conflit entre transparence et protection des données. L'autorité requise se prononcera sur l'accessibilité ou non du document requis en fonction de la typologie qui résulte de cet arbitrage. Sa marge d'appréciation est restreinte ; toutefois, si l'information requise ne rentre dans aucune des catégories consacrées par la typologie - soit que le législateur l'a omise, soit qu'il s'agit d'un type jusqu'alors inconnu -, l'autorité requise bénéficiera, exceptionnellement, d'une grande latitude d'interprétation pour combler la lacune.

L'approche concrète a l'avantage de la flexibilité ; basée sur des clauses générales protégeant des intérêts privés définis à grands traits, elle s'adapte à l'imprévu ; de surcroît, elle est plus fine, car la pesée des intérêts implique une prise en compte de l'ensemble des particularités du cas concret. Cette méthode présente en revanche le défaut de laisser une vaste marge d'interprétation à l'autorité requise, marge dont elle peut abuser pour occulter, au nom de la protection de la vie privée, des informations qui l'embarrasserait elle-même ou la mettrait en cause ; c'est l'effet paravent inhérent à la protection des données, un risque dont il a déjà été question plus haut.[23]

3.2.3 Approches hybrides

Désireux de tirer parti des avantages de chacune des deux approches, la plupart des législateurs n'ont pas consacré l'une ou l'autre des approches de manière absolue, mais combiné les deux.

---

[21] David Banisar, The Right to Information and Privacy: Balancing Rights and Managing Conflicts, Washington 2011, p. 20.

[22] U.K. Ministry of Justice (2008), "Freedom of Information Guidance: Exemptions Guidance, Section 40- Personal Information."

[23] Cf. supra 2.1

Le modèle classique est celui de la pesée des intérêts, doublée, dans certains cas, de règles fixes.

- Exemple : l'art. 5 de la loi fédérale allemande sur l'accès à l'information institue généralement une pesée des interdits (cf. supra 3.2.1), mais pose ensuite une interdiction absolue d'accéder à des données sensibles (au sens de l'art. 9 al. 1 du RGPD) sans le consentement de la personne concernée.

Certains législateurs n'ont pas complété la pesée des intérêts par des normes fixes, mais par des présomptions de publicité (plus rarement de secret) ; à chaque fois, la présomption est réfragable.

- Exemple : l'art. 6 de l'ordonnance fédérale suisse sur la transparence présume l'existence d'un intérêt prépondérant à l'accès dans deux cas : lorsque le document requis est en relation avec un événement important pour le grand public (un scandale politique ou une affaire de corruption au sein de l'administration notamment) et lorsque la personne concernée est « liée à une autorité soumise à la loi sur la transparence par un rapport de fait ou de droit qui lui procure des avantages importants ». Cette dernière hypothèse vise tout particulièrement les personnes bénéficiant d'une concession ou d'une autorisation administrative, ainsi que celles qui ont obtenu des aides financières des autorités publiques.

Enfin, il y a lieu de relever que, lors de l'examen de la requête, la pesée des intérêts intervient en dernière étape. Si la requête peut d'emblée être rejetée en raison d'un autre obstacle (une règle fixe, ou un intérêt public prépondérant au secret ou encore la nature inachevée ou interne du document requis), on peut se passer d'entreprendre une opération de pondération, toujours délicate et longue (en particulier si la personne concernée doit être consultée, cf. infra 4).

3.2.4 Forme de la transmission des données requises

Quelques législateurs contraignent le requérant à se contenter de la remise des données requises sous forme de copie sur support papier, interdisant notamment tout accès direct aux bases de données électroniques détenues par les autorités. L'objectif est d'éviter toute exploitation de fichiers qui pourrait mettre en danger la vie privée de la personne concernée.

3.3. Sources juridiques du compromis

Le plus souvent les règles de coordination sont insérées au sein du corpus normatif qui régit la transparence, plus rarement dans celui qui régit la protection des données.

Il est patent que la première option est la plus adéquate, car elle contribue à la cohérence et à la visibilité du régime juridique des restrictions au droit d'accès. Cela dit, pour dissiper tout doute sur les relations entre la publicité des documents administratifs et la protection des données, le

législateur a quelquefois doté la loi sur la protection des données d'un renvoi à la loi sur l'information.

- Exemple : l'art 12 al. 2 de la loi sur la protection des données du canton suisse de Fribourg dispose que : « La communication de données personnelles au public est (…) régie par la législation sur l'information et l'accès aux documents. »

Très rarement, le compromis est régi par des règles ressortissant les unes au régime de la transparence, les autres à celui de la protection des données. C'est notamment le cas en Suisse où le mécanisme de coordination résulte de l'amalgame d'une exception générale de vie privée et d'une norme sur l'anonymisation insérées dans loi fédérale sur la transparence de l'administration (art. 7 et 9) et d'une norme, insérée dans la loi fédérale sur la protection des données, réglant la communication de données personnelles par l'administration (art. 19bis). Inutile de préciser qu'un régime aussi alambiqué ne facilite pas la tâche des autorités d'application.

Qu'il relève du corpus normatif régissant la transparence ou de celui qui régit la protection des données, le mécanisme de coordination peut ressortir d'une combinaison de texte de divers niveaux législatifs. Alors que la norme de conflit consacrant une balance des intérêts est souvent instituée au niveau de la loi formelle, ses modalités de mise en œuvre (détails des règles fixes complémentaires, présomptions de publicité ou de secret notamment) résultent de textes réglementaires : décrets du gouvernement ou circulaires d'un ministère, voire même de textes infra-légaux, telles des recommandations ou des instructions des instances en charge de l'accès aux documents administratifs ou de la protection des données.

- Exemple : La Commission française d'accès aux documents administratifs (CADA) et la Commission nationale informatique et libertés (CNIL) ont publié ensemble, en 2019, un guide sur « L'anonymisation des données ».

On notera enfin que, quelquefois, la balance des intérêts n'a pas été instituée par le législateur mais par la jurisprudence désireuse de tempérer la rigidité d'une exception d'atteinte à la vie privée en cas de communication, formulée en termes absolus par le législateur.

- Exemple : L'art. 6 al. 3 du Décret du Conseil de la Communauté française (Belgique) relatif à la publicité de l'administration de la loi dispose que : L'autorité administrative rejette la demande si la publicité donnée au document porte atteinte à la vie privée. Cette disposition sans nuance a été relativisée par tribunaux : « Par ailleurs, une analyse de la jurisprudence des différentes CADA et du Conseil d'État met en lumière la nécessité de mettre en balance l'intérêt de la publicité pour la partie requérante avec celui de la protection de la vie privée » (Décision de la Commission d'accès aux documents administratifs de la Fédération Wallonie-Bruxelles du 30 juin 2020).

4. Le droit d'être entendu de la personne concernée

4.1. Les options possibles

Les droits que la personne concernée peut ou ne peut pas faire valoir dans le cadre de la procédure d'examen de la requête de consultation est une question à laquelle les législateurs ont répondu très différemment d'un pays à l'autre. Ici la personne concernée est totalement ignorée. Là, elle a le droit d'exprimer son point de vue sur la communicabilité ou non de ses données personnelles ; en revanche, il ne lui appartient pas de se prononcer sur d'éventuels intérêts prépondérants de nature publique ou privée (mais afférents à des tiers).

On relèvera que si certains pays privent la personne concernée de tout droit de s'exprimer, c'est pour ne pas rallonger la procédure. On sait en effet que les requêtes d'accès à l'information doivent être traitées avec célérité (notamment pour tenir compte des besoins de la presse), or la consultation de la personne concernée prend son temps. Et ce, même si la plupart des législations qui accordent un droit de consultation à la personne concernée lui impartissent des délais courts (au maximum deux-trois semaines) pour se prononcer.

4.2. *La valeur juridique du point de vue de la personne concernée*

Le droit d'être consulté est une chose, la portée juridique de la consultation une autre. Le plus souvent, le point de vue de la personne concernée se résume à une opposition sans valeur contraignante que l'autorité requise peut librement rejeter ou faire sienne. Rares sont en effet les juridictions qui donnent à la personne concernée un véritable droit de veto (et encore, dans ce cas, celui-ci est généralement limité à la communication de données sensibles).[24]

Au demeurant, même s'il n'est pas contraignant, le point de vue de la personne concernée n'est pas dénué de tout effet. D'un côté, un avis défavorable à l'admission de la requête apporte des éléments (notamment des précisions sur les circonstances motivant l'opposition) l'autorité devra prendre en considération dans le cadre de la pesée des intérêts ; de l'autre, un avis favorable sera, juridiquement, assimilé à un consentement à la communication des données requises au requérant.

4.3 Exceptions au droit d'être entendu

Enfin, il y a lieu de souligner que le droit d'être entendu n'est pas absolu, mais connaît quelques exceptions légales et/ou jurisprudentielles. Les principales situations déliant l'autorité requise de toute obligation de consulter la personne concernée sont :

- une forte présomption de consentement de la personne concernée à la communication des données personnelles requises ;

[24] Voir sur ce point l'article 6 de la Convention 108+ qui liste les données sensibles.

- des données concernant des employés de la fonction publique ;
- un nombre considérable de personnes concernées à consulter ;
- un intérêt public à la transparence manifestement prépondérant.

5. L'interaction entre autorité de protection des données et autorité de transparence

Concilier protection des données et transparence, c'est aussi définir les relations entre les instances respectives chargées de ces deux domaines afin que l'expertise de l'une puisse profiter à l'autre. Plus concrètement, il s'agit de déterminer dans quelle mesure l'instance chargée de protection des données est associée au traitement de la requête par l'instance chargée de la transparence – étant entendu que cette dernière demeure, en règle générale, l'instance compétente pour se prononcer sur les requêtes portant sur la consultation de données personnelles. Divers modèles ont cours :

- *Le lien organique* : un membre de chacune des deux instances siège également dans l'autre (avec ou sans droit de vote).
  - Exemples : au Maroc, la Commission nationale de contrôle de la protection des données à caractère personnel et la Commission du droit d'accès à l'information sont présidées par la même personne (art. 23 de loi 31-13 relative au droit d'accès à l'information) ; en France, depuis l'adoption de la loi 2016-1321 pour la République numérique le président de la CADA est d'office membre de plein droit de la CNIL et le président de la CNIL d'office membre de la CADA.

- *Le lien procédural* : l'autorité requise doit consulter l'autorité de protection des données lorsque la requête porte sur des données personnelles.
  - Exemple : le mécanisme de la consultation obligatoire a été consacré de façon générale en Italie. Sans entrer dans le détail de sa mise en œuvre, on soulignera que l'autorité de protection des données à 10 jours pour se prononcer et que son préavis n'est pas jamais contraignant.

- *Le partage du pouvoir réglementaire* : les deux instances édictent, à l'intention des autorités requises, des instructions ou des recommandations communes sur la mise en œuvre des mécanismes de compromis.
  - Exemple : Outre le guide commun sur l'anonymisation des données mentionné plus haut (3.3.), la Commission française d'accès aux documents administratifs (CADA) et la Commission nationale informatique et libertés (CNIL) ont publié 2016 un « Guide sur la mise en ligne et la réutilisation des données publiques » et en 2021 une fiche sur « La publication des documents des collectivités territoriales liés à l'exercice de leur pouvoir décisionnaire ».

- *Le partage d'infrastructures* : tout en restant indépendante l'une de l'autre, les deux instances mettent en commun des infrastructures et /ou des ressources matérielles.
  - Depuis 2018, la Commission française d'accès aux documents administratifs (CADA) et la Commission nationale informatique et libertés (CNIL) sont établies dans le même immeuble à Paris. Cette proximité favorise les échanges informels.

On rappellera enfin que de nombreux pays (entre autres l'Allemagne, le Canada, le Royaume-Uni, la Slovénie, la Serbie et la Suisse) ont fusionné l'instance de protection d'accès à l'information avec l'instance de protection des données ; une synergie motivée par le fait que les deux domaines ressortissent au statut de l'information publique (cf. supra 2.2). Il y a quelques années le gouvernement français a envisagé de procéder à une pareille fusion ; il a finalement renoncé à ce projet au vu des pouvoirs différents des deux instances (la CADA ne peut émettre que des recommandations alors que la CNIL peut ordonner des mesures contraignantes) ainsi qu'à leur culture administrative divergente.[25]

Quoi qu'il en soit, il a été souligné que dans les pays qui n'ont pas fusionné les deux instances, celles-ci coopèrent étroitement : *« It is therefore necessary that personal data protection supervisory bodies and FOI bodies, in states which has both types of supervisory bodies, work together and are coordinated. »*[26]

6. Le droit tunisien en comparaison

Le droit à l'information et le droit de la protection des données étant en Tunisie d'égale valeur - tous deux ont été consacrés par des lois organiques[27], le législateur ne pouvait pas faire l'économie d'un mécanisme de conciliation. A défaut, les données personnelles auraient par principe échappé à la transparence ; l'art. 47 de la loi 2004/63 portant sur la protection des données à caractère personnel interdit en effet expressément de communiquer des données personnelles à des tiers sans le consentement écrit de la personne concernée.

---

[25] Sur les avantages et les désavantages d'une autorité commune de protection des données et de transparence des documents administratifs, voir N. Musar et B. Cottier, *Comparative study of different appeal and control mechanisms regarding access to public information in six Council of Europe member states*, Council of Europe, Strasbourg 2017.

[26] *Human Dynamics Consulting, Legal balance of interests between transparency of public life and data protection* (project soutenu par l'UE), p. 8. (traduction non officielle : "Il est ainsi nécessaire que, dans les États qui ont ces deux types d'organes des contrôle, les organes de protection des données personnelles et les organes chargés de la liberté de l'information travaillent ensemble et soient coordonnés. »)

[27] Le premier par la loi organique 2016/22 relative au droit à l'information, le second par la loi organique 2004/63 portant sur la protection des données à caractère personnel. On notera qu'en Tunisie, comme dans la plupart des pays qui connaissent aujourd'hui et la transparence et la protection des données, cette dernière a précédé dans le temps le droit à l'information.

Institué par les art. 24 à 27 de la loi organique 2016/22 relative au droit à l'information, ce nécessaire mécanisme de conciliation est centré sur une balance des intérêts de présence. Ainsi, l'art. 24 al. 1 érige expressément la protection des données en exception à la transparence (et ce, en sus de l'exception générale de protection de la vie privée). Cette exception spécifique est cependant relative ; elle peut en effet être renversée en cas d'intérêt public prépondérant à l'accessibilité (art. 24 al. 2). Si toutefois l'intérêt de personne concernée au maintien du secret prévaut, l'information personnelle requise ne sera pas communiquée. Le document qui la contient ne demeurera pas pour autant inaccessible : il sera transmis au requérant, mais sans l'information personnelle qui doit rester secrète, laquelle aura été au préalable occultée par caviardage ou effacement (art. 27).

Ce mécanisme de conciliation de type concret est complété par quelques rares règles fixes additionnelles ; l'art. 26 en pose deux en faveur de la transparence (crimes graves contre l'Humanité, atteintes graves à la santé et à l'environnement) et l'art. 25 en institue une en faveur du secret (identité du dénonciateur).

On relèvera enfin que le législateur a eu souci de favoriser les échanges entre l'Instance nationale d'accès à l'information et l'Instance nationale de protection des données : la première doit accueillir, en tant que membre de plein droit, un représentant senior de la seconde (art. 41 de la loi organique 2016/22). L'interaction pourrait ne pas en rester là : les deux instances ont en effet manifesté leur intention de développer ensemble une liste exemplaire de facteurs susceptibles de peser lourd dans la balance des intérêts.

7. Conclusion

Arrivé au terme de ce bref état des lieux, il convient de souligner que le droit comparé met en évidence trois constantes :

- si la protection des données n'est nulle part un motif en soi suffisant pour rejeter une requête d'accès, elle est néanmoins un facteur appelé à jouer un rôle plus ou moins important en fonction des circonstances concrètes de la requête ;

- l'anonymisation est une mesure qui est largement préconisée pour concilier concrètement l'intérêt à la transparence et l'intérêt à la protection de la vie privée ; cette mesure atteint toutefois sa limite lorsque le requérant cherche précisément à s'informer sur une personne déterminée ;

- le législateur, la jurisprudence ou encore les instances d'accès à l'information et de protection des données (conjointement ou indépendamment) ont cherché à définir certains types de données personnelles qui, dans tous les cas, doivent être considérées comme accessibles (ou à tout le moins sont présumés l'être) ou, mais plus rarement,

strictement confidentielles. Entrent souvent dans la première catégorie les informations relatives à des personnalités publiques (à commencer par les dirigeants et les hauts fonctionnaires) et celles qui font état d'avantages concédés par l'administration aux administrés (subventions, concessions, contrats administratifs en particulier). La seconde catégorie est notamment composée de données dites sensibles.