



CONCILIER
DROIT D'ACCÈS
À L'INFORMATION
&
PROTECTION
DES DONNÉES
PERSONNELLES
GUIDE PRATIQUE

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

SOMMAIRE

I. INTRODUCTION	
CE GUIDE, POURQUOI, POUR QUI, COMMENT	4
II. LE CONTEXTE	6
A. LES ENJEUX	7
B. LE CADRE JURIDIQUE PERTINENT	8
1. Une double consécration internationale	
2. Une robuste protection nationale	
3. Concilier droit à l'information et protection des données personnelles : ce qui dit la loi	
a. Généralités	
b. La balance des intérêts	
c. Règles fixes	
d. Mise en œuvre	
III. MARCHE À SUIVRE POUR L'EXAMEN D'UNE DEMANDE D'ACCÈS À UN DOCUMENT CONTENANT DES DONNÉES PERSONNELLES	12
A. EN GÉNÉRAL	13
B. EN DÉTAIL	13
1. Repérer une éventuelle règle fixe	
2. Identifier un éventuel intérêt public (ou privé) prépondérant	
3. Rechercher le consentement de la personne concernée	
4. Tenter d'anonymiser le document requis	
5. Procéder à la pondération des intérêts	
a. Généralités	
b. Facteurs pesant en faveur de la transparence	
c. Facteurs pesant en faveur du secret	
SCHÉMA RÉCAPITULATIF	18
IV. LE MOT DE LA FIN	21

En Tunisie comme ailleurs, la pratique démontre que l'articulation entre le droit d'accès à l'information et la protection des données personnelles ne va pas de soi, tant ces deux principes fondamentaux de tout État démocratique apparaissent antagonistes de prime abord. Il n'est pas simple de les concilier lorsqu'une demande d'accès à un document officiel contient des données personnelles. Les personnes chargées de se prononcer doivent en effet procéder non seulement à une analyse approfondie des circonstances de l'espèce, mais aussi à une délicate balance des intérêts en présence.

Ce guide a pour objectif de faciliter la tâche des agents de la fonction publique en leur donnant les instruments leur permettant de prendre une décision fondée, réfléchie et équilibrée et ce, sans exiger d'eux des connaissances juridiques pointues ni les contraindre à des raisonnements alambiqués. Bien que destiné principalement à l'administration publique, ce document apporte aussi des informations utiles aux personnes qui exercent leur droit d'accès.

Il est également disponible sur les sites web de l'Instance pour l'accès à l'information (INAI) www.inai.tn et de l'Instance nationale de protection des données personnelles (INPDP) www.inpdp.tn

PROGRAMME DE RÉALISATION

Conseil de l'Europe et Union européenne :
Appui aux instances indépendantes en Tunisie (PAII-T)

ÉQUIPE DU PROJET

Anne Boyer-Donnard, Ikram Ben-Sassi, Hela Rezouga

RÉDACTION

Pr. Bertil Cottier.

CONCEPTION GRAPHIQUE ET IMPRESSION

Impact
Tunis, 2022

Cette publication est produite avec le soutien de l'Union européenne et le Conseil de l'Europe dans le cadre du « Projet d'appui aux instances indépendantes en Tunisie ». Ni l'Union européenne, ni le Conseil de l'Europe ne pourront être tenus responsables de l'usage qui pourrait être fait des informations qu'elle contient

I. INTRODUCTION

CE GUIDE, POURQUOI, POUR QUI, COMMENT

La pratique, en Tunisie comme à l'étranger, le démontre à l'envi : l'articulation entre le droit d'accès à l'information et la protection des données personnelles ne va pas de soi, tant ces deux principes fondamentaux de tout État démocratique apparaissent antagonistes de prime abord. À tel point qu'il n'est pas simple de les concilier lorsqu'une demande d'accès à un document officiel contient des données personnelles. Celui qui est appelé à se prononcer doit en effet procéder non seulement à une analyse approfondie des circonstances de l'espèce, mais aussi à une délicate balance des intérêts en présence.

L'objectif du présent guide est de faciliter la tâche des agents de la fonction publique en leur donnant les instruments leur permettant de prendre une décision fondée, réfléchie et équilibrée ; et ce, sans exiger d'eux des connaissances juridiques pointues ni les contraindre à des raisonnements alambiqués. Bien que destiné principalement à l'administration publique, ce document apporte aussi des informations utiles aux personnes qui exercent leur droit d'accès.

Le guide opère en deux temps. D'abord il détaille les enjeux, s'attachant notamment à exposer les buts respectifs de la protection des données et du droit à l'information sur les activités étatiques ainsi que les régimes juridiques qui gouvernent ces deux institutions. De la théorie on passe ensuite à la pratique : la deuxième partie du guide s'adresse en effet directement à celui qui est confronté à une demande de consultation de données personnelles, en lui indiquant la marche à suivre pour traiter adéquatement pareille demande. Dans cette perspective didactique, une attention toute particulière est apportée aux facteurs qui doivent être pris en considération tout au long des diverses étapes de la prise de décision.

Le présent guide est le fruit d'une coopération bénéfique entre l'Instance d'accès à l'information (INAI) et l'Instance nationale de protection des données personnelles (INPDP). Ces deux institutions expriment leur gratitude à l'Union européenne et au Conseil de l'Europe : sans leur soutien financier et logistique, cette entreprise éducative et conciliatrice n'aurait pas été portée à terme.



II. LE CONTEXTE

A. Les enjeux

Tant le droit d'accès à l'information que la protection des données sont des piliers incontournables de la démocratie.

Côté transparence, il en va non seulement de la libre circulation et du débat d'idées, mais aussi du contrôle citoyen sur l'État et ses organes. À cet effet, tout un chacun se voit reconnaître un véritable droit à accéder aux documents détenus par les autorités publiques. Inutile de préciser qu'en ces temps où la désinformation rode sur les réseaux sociaux, il est plus que jamais d'importance que la population puisse recueillir des données fiables et complètes sur les activités des autorités.

Côté vie privée, est en jeu le droit de chaque individu à bénéficier d'une sphère personnelle secrète, propre à sauvegarder son intimité et sa personnalité. Mais ce n'est pas tout : il s'agit aussi d'accorder à l'individu la pleine maîtrise sur l'usage qui est fait de ses données personnelles. En d'autres termes, il doit être en mesure de déterminer ce qui doit rester secret et ce qui peut être communiqué. Sphère de confidentialité et droit à l'autodétermination informationnelle contribuent tous deux à la protection de la vie privée.

Apparemment antagonistes, les valeurs fondamentales de transparence des activités des autorités étatiques et de

protection de vie privée sont en fait indissociables et complémentaires. Partant, elles doivent être coordonnées. Ainsi le préambule de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981 (Convention 108), à laquelle la Tunisie est partie depuis 2017, reconnaît « la nécessité de concilier les valeurs fondamentales du respect de la vie privée et de la libre circulation de l'information entre les peuples ».

Réciproquement, la Convention sur l'accès aux documents publics (Convention de Tromsø) du 8 juin 2009, prévoit dans son préambule, une réserve à la communication des documents publics qui porte sur « la protection d'autres droits et intérêts légitimes » et la précise à son article 3 : « ...la vie privée et les autres intérêts privés légitimes ».

L'impératif de coordination est d'autant plus important que droit d'accès et protection des données ont une finalité commune : l'un et l'autre tendent à rendre l'État redevable 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. Dès lors, les règles sur l'accès à l'information et celles sur la protection des données concourent, ensemble mais chacune à sa manière, à la bonne gouvernance des informations détenues par les autorités.

B. Le cadre juridique pertinent

1. Une double consécration internationale

Le droit d'accès à l'information comme la protection de la vie privée sont consacrés par le Pacte international relatif aux droits civils et politiques de 1966. Adopté sous les auspices des Nations Unies et ratifié par la Tunisie en 1969, ce texte à vocation universelle souligne à son article 19 que la liberté d'expression « *comporte la liberté de rechercher des informations* » ; de même, l'article 17 proclame que « *Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation* ».

Également ratifiée par la Tunisie, la Charte africaine des droits de l'homme protège aussi, même si c'est en des termes plus généraux, le droit à l'information, à l'article 9.

2. Une robuste protection nationale

Tant la protection de la vie privée, et dans son prolongement la protection des données personnelles, que le droit d'accès à l'information bénéficient dans le pays d'une légitimité de très haut niveau.

D'abord, la constitution de 2022 les consacre expressément. Ainsi l'article

30 dispose que : « *L'État protège la vie privée, l'inviolabilité du domicile et le secret des correspondances, des communications et des données personnelles* ». Quant à l'article 38, il souligne que : « *L'État garantit le droit à l'information et le droit d'accès à l'information* ».

Ensuite et surtout, les diverses modalités d'exercice de ces deux droits fondamentaux sont définies en détail dans deux lois organiques, à savoir dans des textes qui sont hiérarchiquement supérieurs aux lois ordinaires mais qui restent soumis à la supériorité des conventions internationales ratifiées par la République tunisienne : d'une part la *Loi organique 22/2016, relative au droit d'accès à l'information*, d'autre part la *Loi organique 63/2004, portant sur la protection des données à caractère personnel*.

En les faisant bénéficier tous deux d'une consécration constitutionnelle et organique, le droit tunisien met la protection des données et le droit d'accès à l'information sur un pied d'égalité. En cas de conflit, aucune des deux institutions ne l'emporte a priori sur l'autre. En conséquence, ils doivent être conciliés.

Une approche accommodante est d'ailleurs expressément préconisée par le Règlement européen de protection des données (UE 2016/679) ; son article 86 souligne en 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».

3. Concilier droit à l'information et protection des données personnelles : ce qui dit la loi

a. Généralités

Certains pays opèrent cette nécessaire conciliation en établissant, au sein de leur législation sur la transparence des autorités publiques, une liste des types de données personnelles inaccessibles (par exemple, les informations médicales) ou des types de documents inaccessibles (par exemple, les dossiers de candidatures à des emplois publics) ; cette liste négative peut être complétée, à l'inverse, par une liste positive d'informations qui sont obligatoirement publiques (par exemple les audits des entités administratives). Cette technique législative est appelée **méthode des normes fixes**, car le législateur a anticipé le conflit entre droit à l'information et protection des données, suivant la nature des informations en jeu et l'a tranché abstraitement.

D'autres pays ont opté pour une autre méthode de conciliation, plus fine, car tenant compte de la diversité de chaque cas concret : **la balance des intérêts**. Il appartient dans ce cas à l'autorité saisie d'une demande d'accès à un document contenant des données personnelles de pondérer les intérêts en conflit en fonction des circonstances précises de l'espèce.

Les deux méthodes ayant leurs avantages et leurs défauts, le législateur tunisien a opté pour une approche hybride : en règle générale, la méthode de la balance des intérêts prévaut ; toutefois, dans certaines hypothèses bien définies, des normes fixes sont applicables.

b. La balance des intérêts

Le siège de la matière se trouve à l'article 24 de la loi organique 22/2016 relative au droit à l'information. Son premier alinéa érige expressément la vie privée et la protection des données en exceptions à la transparence.

La vie privée est un concept juridique dont les contours sont difficiles à cerner avec précision ; elle a été consacrée par les textes internationaux (Déclaration universelle des droits de l'Homme, Pacte international relatif aux droits civils et politiques). La jurisprudence et la doctrine s'accordent cependant pour affirmer qu'elle englobe, entre autres éléments, les informations ayant trait à la vie familiale d'une personne (mariage, divorce, filiation), à son état de santé, à ses croyances religieuses, à ses opinions politiques, à sa situation financière, à son orientation sexuelle ou encore à des condamnations pénales ou à des sanctions administratives. La jurisprudence détermine au cas par cas et suivant la situation de la personne la limite à fixer entre sa vie privée et sa vie publique.

Quant à la notion de donnée personnelle, elle recouvre « *toutes les informations quelle que soit leur origine ou leur forme et qui permettent directement ou indirectement d'identifier une personne*

physique ou la rendent identifiable » (article 4 de la loi 63/2004). Toute particularité susceptible d'individualiser une personne répond à cette définition. Plus concrètement, ce peut être une particularité physique (amputation d'une jambe,...), physiologique (empreintes digitale, génétique...), sociale (plaques d'immatriculation d'un véhicule ...) ou encore culturelle (coiffure originale...) ainsi que les images de la vidéo-surveillance, les enregistrements audios, les déplacements des personnes et leur géolocalisation, le résultat du profilage et de l'évaluation comportementale des personnes.

La loi 63/2004 ne protège que les données relatives aux personnes physiques (article 4). Si les personnes morales ne peuvent dès lors prétendre à la protection de leurs « données personnelles » en tant que telles, elles jouissent néanmoins d'une sphère de confidentialité au titre de la protection particulière de leurs activités.

Il importe de souligner que les exceptions de protection de données personnelles dans le cadre de l'exercice du droit à l'accès à l'information ne sont que relatives (article 24 al. 2 de la loi 22/2016) ; elles peuvent en effet être écartées si, en l'espèce, l'intérêt public à la communication du document contenant des informations personnelles l'emporte sur l'intérêt privé de la personne concernée au maintien du secret. Exemples tirés de la jurisprudence de l'Instance d'accès à l'information :

Décision 51/2018 : l'intérêt général à connaître les tenants et aboutissants de graves malversations (corruption

notamment) dans le service public du sport l'a emporté sur l'intérêt des protagonistes à ce que leur identité ne soit pas révélée.

Décision 92/2018 : priorité a été donnée à l'intérêt général à assurer une pleine transparence sur les procédures de recrutement d'enseignants sur l'intérêt privé des candidats à ce que leurs données personnelles demeurent confidentielles. Dans ce cas, c'est la nécessité de démontrer au public la loyauté et l'impartialité de ces procédures qui a prévalu.

En revanche, si l'intérêt privé à la confidentialité des données personnelles pèse plus lourd dans la balance, celles-ci ne seront pas communiquées. L'article 47 de la loi 63/2004 interdit en effet expressément de porter des données personnelles à la connaissance de tiers sans le consentement écrit de la personne concernée. Exemples pratiques :

Décision INAI 331/2019 : accès aux listes nominatives des enseignants universitaires adhérents à des syndicats de l'enseignement supérieur refusé au motif que leur communication violerait la liberté syndicale des enseignants.

Décision INAI 351/2019 : absence d'intérêt public à communiquer les coordonnées bancaires et la nature des relations bancaires d'une cliente étrangère de la Banque centrale de Tunisie.

Reste que le document requis ne demeurera pas pour autant inaccessible.

Conformément à l'article 27 de la loi 22/2016, qui concrétise le principe général de proportionnalité en prescrivant la minimisation du secret, il sera communiqué au requérant, mais en partie seulement. Autrement dit, sans les données personnelles qui doivent demeurer secrètes lesquelles auront été au préalable occultées par caviardage, effacement ou suppression.

c. Règles fixes

L'article 26 de la loi 22/2016 pose deux règles fixes en faveur de la transparence. La première vise « les informations dont la divulgation est nécessaire en vue de dévoiler des violations graves aux droits de l'Homme ou des crimes de guerre ou les investigations y liées ou la poursuite de ses auteurs » ; la seconde répond à la nécessité de parer à une menace grave pour la santé, la sécurité ou l'environnement.

Cette même loi institue à son article 25 une règle fixe en faveur du secret cette fois : l'identité d'un dénonciateur ou d'un lanceur d'alerte ne doit en aucun cas être révélée. Il importe en effet de mettre ces personnes à l'abri de mesures de rétorsion ou d'actes de vengeance ; partant, il n'y aura lieu de procéder à une communication partielle du document requis en application de l'article 27 (cf. supra b) que si les informations susceptibles d'identifier directement ou indirectement la personne concernée ont été dans leur ensemble masquées (décisions de l'INAI 197/2018 et 297/2019)

La loi organique 22/2016 n'a pas l'exclusivité des règles fixes. Plusieurs règles de ce type - la plupart imposant

le secret - ont été posées par législateur dans d'autres textes législatifs.

d. Mise en œuvre

Les deux lois organiques instituent, chacune pour son domaine, un organe spécifique chargé de conseiller et surveiller leur mise en œuvre respective : la mise en œuvre de la loi 63/2004 a été confiée à l'Instance nationale de protection des données personnelles (INPDP), celle de la loi 22/2016 à l'Instance d'accès à l'information (INAI). L'INAI est aussi autorité de recours contre les décisions prises par les entités déterminées par la loi.

En cas de recours contre une décision de refus d'accorder l'accès à un document contenant des données personnelles, il appartient à l'INAI (et non à l'INPDP) de se prononcer (article 30 et 37 de la loi 22/2016). Et ce, même si le refus est motivé par un risque sérieux d'atteinte à la vie privée ou à la protection des données en cas de communication du document.

Cela dit, le législateur a eu souci d'assurer une prise en compte adéquate des intérêts afférents à la vie privée et à la protection des données au sein de l'INAI : un représentant senior de l'INPDP fait de droit partie de l'INAI ; à ce titre, il participe notamment aux délibérations portant sur des affaires mettant en jeu ces intérêts (article 41 de la loi 22/2016) bien que les modalités et les critères de sa nomination soient discutables.

III. MARCHE À SUIVRE POUR L'EXAMEN D'UNE DEMANDE D'ACCÈS À UN DOCUMENT CONTENANT DES DONNÉES PERSONNELLES



A. En général

La présente marche à suivre se présente sous la forme d'une check list en cinq étapes :

- **1^{ère} étape** : existe-il une norme fixe pertinente applicable au cas d'espèce ?
- **2^{ème} étape** : un intérêt prépondérant, public ou privé (autre que la vie privée ou la protection des données personnelles), s'oppose-t-il à la consultation du document requis ?
- **3^{ème} étape** : la personne concernée consent-elle à la consultation de ses données personnelles ?
- **4^{ème} étape** : la consultation du document requis sous forme anonymisée est-elle envisageable ?
- **5^{ème} étape** : pondération des intérêts en présence.

En cas de réponse à la question posée permettant une décision, la procédure d'examen de la requête d'accès prend fin à ce stade ou elle se poursuit à l'étape suivante, selon le cas.

Les cinq étapes doivent être impérativement franchies dans l'ordre indiqué, car il convient de minimiser les démarches autant que faire se peut et de ne procéder qu'en dernier ressort à la délicate et complexe pondération entre l'intérêt au secret de la personne concernée et l'intérêt du requérant à la publicité.

Enfin, il y a lieu de signaler que la présente marche à suivre ne prend pas en compte un cas de figure très particulier : l'accès à ses propres

données. Instrument de maîtrise de la personne concernée sur l'usage qui est fait de ses données, ce droit d'accès spécial ressort de la législation sur la protection des données. Les modalités de sa mise en œuvre (notamment les exceptions au droit d'accès et la procédure qui gouverne sa réalisation) sont en effet régies par les articles 32 à 41, et 54 de la loi 63/2004. En outre, l'autorité de recours contre un refus d'accès n'est plus l'INAI, mais l'INPDP.

Reste le problème des demandes d'accès qui visent des documents mixtes, à savoir qui contiennent à la fois des données personnelles du requérant et des données personnelles de tiers et/ou des données non-nominatives. La solution dépend de la possibilité ou non de désagréger les données en jeu. Si les données propres au demandeur peuvent aisément être dissociées, l'accès à celles-ci sera régi par la législation sur la protection des données alors que l'accès aux autres données sera régi par la législation sur la transparence. Si, en revanche la dissociation n'est pas possible, la législation sur la protection des données régira l'accès à l'ensemble du document.

B. En détail

1. Repérer une éventuelle règle fixe

La première étape est relativement aisée, puisqu'elle consiste à rechercher une éventuelle règle fixe directement applicable au cas d'espèce, règle qui ordonnerait d'entrée de cause soit

la communication, soit le secret de l'information requise. La recherche ne peut se borner à l'examen de la loi 22/2016. On rappellera en effet que les trois règles fixes contenues dans ce texte ne sont pas les seules ; des lois spéciales peuvent consacrer d'autres règles fixes (cf. supra II.B.3.c).

Comme l'a souligné l'INAI dans ses décisions 197/2018 et 195/2019, une règle fixe est de nature absolue. En présence d'un état de fait qui réunit toutes les conditions d'application posées par la règle fixe, l'autorité requise est privée de marge d'appréciation ; elle doit alors purement et simplement donner suite à la requête d'accès ou la rejeter (suivant la teneur positive ou négative de la règle fixe applicable). Le législateur ayant arbitré lui-même le conflit entre transparence et protection de la vie privée, aucun autre facteur tendant soit à la communication, soit au secret ne peut être pris en considération.

2. Identifier un éventuel intérêt public (ou privé) prépondérant

La protection de la vie privée et des données personnelles ne sont pas les seuls intérêts justifiant le rejet d'une demande d'accès à un document officiel. L'article 24 al. 1 de la loi 22/2016 en énumère cinq autres. Trois sont de nature publique : la défense, la sécurité nationale et les relations internationales ; deux de nature privée : la propriété intellectuelle et les secrets des affaires. Dérogeant au principe fondamental de transparence des activités étatiques, ces exceptions

doivent toutes être interprétées restrictivement.

C'est ainsi qu'elles n'entrent en ligne de compte que si la communication du document requis pourrait causer une atteinte grave à l'un des cinq intérêts mentionnés ci-dessus. Qui plus est, la nécessité de préserver le secret doit l'emporter sur l'intérêt du requérant à prendre connaissance du document requis.

S'il s'avère en l'espèce que tel est le cas, la demande d'accès sera rejetée.

3. Rechercher le consentement de la personne concernée

En vertu du principe directeur de l'autodétermination informationnelle (cf. supra II.A.), il appartient à la personne concernée de se déterminer sur l'usage qui sera fait de ses données. En conséquence, si elle consent au traitement envisagé, celui-ci peut être entrepris ; encore faut-il que la personne concernée ait été dûment informée des tenants et aboutissants de ce traitement. Rapportée à notre problématique, cette ligne de conduite ouvre la voie à la communication des données personnelles requises en cas de consentement de la personne concernée.

Si la personne concernée avait déjà consenti à la communication des données personnelles en question avant le dépôt de la requête de consultation, le document requis serait remis sur le champ ; il en va de même si la personne concernée avait elle-même rendu ces

données publiquement accessibles à tout un chacun (par exemple, si elle les avait mises en ligne sur son site internet personnel). À défaut d'un consentement préalable, expresse ou déduit des circonstances sans équivoque, contact sera pris avec la personne concernée pour lui demander si elle consent à la communication.

Pour être valable, le consentement doit avoir été donné conformément aux conditions posées par les articles 27 à 31 de la loi 63/2004 ; en particulier, il doit être exprès et écrit. Si les données requises concernent un enfant, il appartient à son tuteur et au juge de la famille de se prononcer. Dans tous les cas, il convient d'informer clairement la personne dont le consentement est exigé des circonstances de la requête d'accès, notamment de l'identité du requérant ; cette démarche doit être entreprise rapidement afin de respecter le délai de traitement des requêtes d'accès qui est de 20 jours (article 14 al. 1 de la loi 22/2016). Le silence de la personne concernée, pourtant dûment notifiée, vaut consentement implicite (application par analogie de l'article 20 de la loi 22/2016 qui régit le silence du tiers qui a fourni des informations confidentielles à l'autorité requise, cf. la fin du paragraphe suivant).

Il existe aussi une autre procédure permettant de dépasser le refus de la personne concernée de permettre la communication de ces données personnelles qui a été prévue par l'article 47 paragraphe 2 de la loi organique numéro 2004-63 et qui dispose que « *L'Instance peut autoriser la communication des données à caractère personnel en cas du refus, écrit et*

explicite, de la personne concernée, de ses héritiers ou de son tuteur lorsqu'une telle communication s'avère nécessaire pour la réalisation de leurs intérêts vitaux, ou pour l'accomplissement des recherches et études historiques ou scientifiques, ou encore en vue de l'exécution d'un contrat auquel la personne concernée est partie et ce, à condition que la personne à qui les données à caractère personnel sont communiquées s'engage à mettre en œuvre toutes les garanties nécessaires à la protection des données et des droits qui s'y rattachent conformément aux directives de l'Instance, et d'assurer qu'elles ne seront pas utilisées à des fins autres que celles pour lesquelles elles ont été communiquées ».

Le refus de consentir à la communication de données personnelles n'entraîne pas pour autant le rejet de la demande d'accès. Ces données pourront être communiquées, nonobstant le refus, si à la suite d'une balance des intérêts en présence, leur publication répond à un intérêt prépondérant (cf. ci-dessous 5). Fait exception le cas de figure des informations confidentielles librement fournies par un tiers à l'autorité requise : le refus de consentement a, dans cette hypothèse très particulière, valeur contraignante (article 20 al. 1 in fine de la loi 22/2016).

4. Tenter d'anonymiser le document requis

Concrétisant le principe de minimisation du secret posé par l'article 27 de la loi 22/2016 (cf. supra II.B.3.b), l'anonymisation est une opération

qui consiste à éliminer les données permettant d'identifier la personne concernée, soit directement (nom, numéro de contribuable ou d'assuré...), soit indirectement (caractéristiques physiques ou corrélation d'informations contextuelles). Généralement, pareille élimination des identifiants s'effectue par caviardage ou par leur suppression pure et simple dans une copie du document requis. Dépourvu de données personnelles, le document requis peut alors être communiqué 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 main l'intégralité du document requis ; le cas échéant, il pourra recourir contre ce qui doit être considéré comme un accès partiellement refusé (article 29 de la loi 22/2016).

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,
- le travail nécessaire à l'élimination de tous les identifiants (notamment indirects) est considérable ou vain tant les données personnelles et les données non nominatives sont enchevêtrées, ou encore,
- à chaque fois que le requérant souhaite expressément consulter des documents afférents à une ou des personnes nommément désignées.

Dans ces trois hypothèses, une anonymisation n'entre plus en considération ; l'autorité requise n'a alors d'autre choix que de procéder à une balance des intérêts en présence.

5. Procéder à la pondération des intérêts

a. Généralités

Si elle prescrit une balance des intérêts en présence, la loi 22/2016 ne donne aucune indication quant aux critères de pondération qui peuvent entrer en considération, encore moins sur leur poids respectif. La liste de ces critères établie par le présent guide est donc exemplaire ; elle se fonde sur la jurisprudence tunisienne et sur des arrêts de référence d'instances internationales ou étrangères.

On ne répétera jamais assez que les facteurs mentionnés ci-dessous, même si certains d'entre eux peuvent peser lourd dans la balance, n'emportent pas la décision du fait de leur simple présence dans le cas d'espèce. Il n'y a jamais d'automatisme : tout dépend des circonstances concrètes qui doivent être *analysées et pondérées* avec grand soin.

b. Facteurs pesant en faveur de la transparence

- l'intérêt du public à être mis au courant de malversations commises dans la gestion des biens publics (corruption, détournement de fonds, octroi d'avantages indus, pour ne citer que les fraudes les plus courantes) ou de dysfonctionnements au sein de

l'administration des services publics (politiques publiques aberrantes, mesures inefficaces, inactions dommageables...);

- l'intérêt public à l'impartialité des marchés publics ou des concours pour des emplois publics ;

- le document requis concerne un événement qui suscite un *grand intérêt* dans le public (élections nationales par exemple) ou a causé une grande émotion dans une large partie de la population (grave accident...);

- le rôle *prééminent* joué par la personne concernée dans la société : plus ses fonctions ou sa position hiérarchique sont élevées, plus elle devra tolérer des révélations sur son comportement en public, mais aussi en privé. Au contraire des subalternes, les élus, les magistrats et les hauts fonctionnaires sont tout particulièrement exposés à la publicité du fait de la grande confiance placée en eux par la population ;

- l'existence d'un *rapport privilégié* avec les autorités publiques ; ce rapport peut résulter d'un emploi dans la fonction publique (à cet égard, les promotions ou les révocations sont particulièrement délicates), de la délégation de pouvoirs de puissance publique, du bénéfice d'une concession de service public ou encore de l'octroi de subventions publiques ou d'autres avantages de nature économique ou fiscale.

c. Facteurs pesant en faveur du secret

- la nature sensible des données ; les données sensibles forment une catégorie de données personnelles

que la loi 63/2004 fait bénéficier d'une protection accrue en raison de leur caractère intime (article 14) ; entrent dans cette catégorie les données qui concernent l'origine raciale ou génétique, les convictions religieuses, les opinions politiques, philosophiques ou syndicales, ou la santé ;

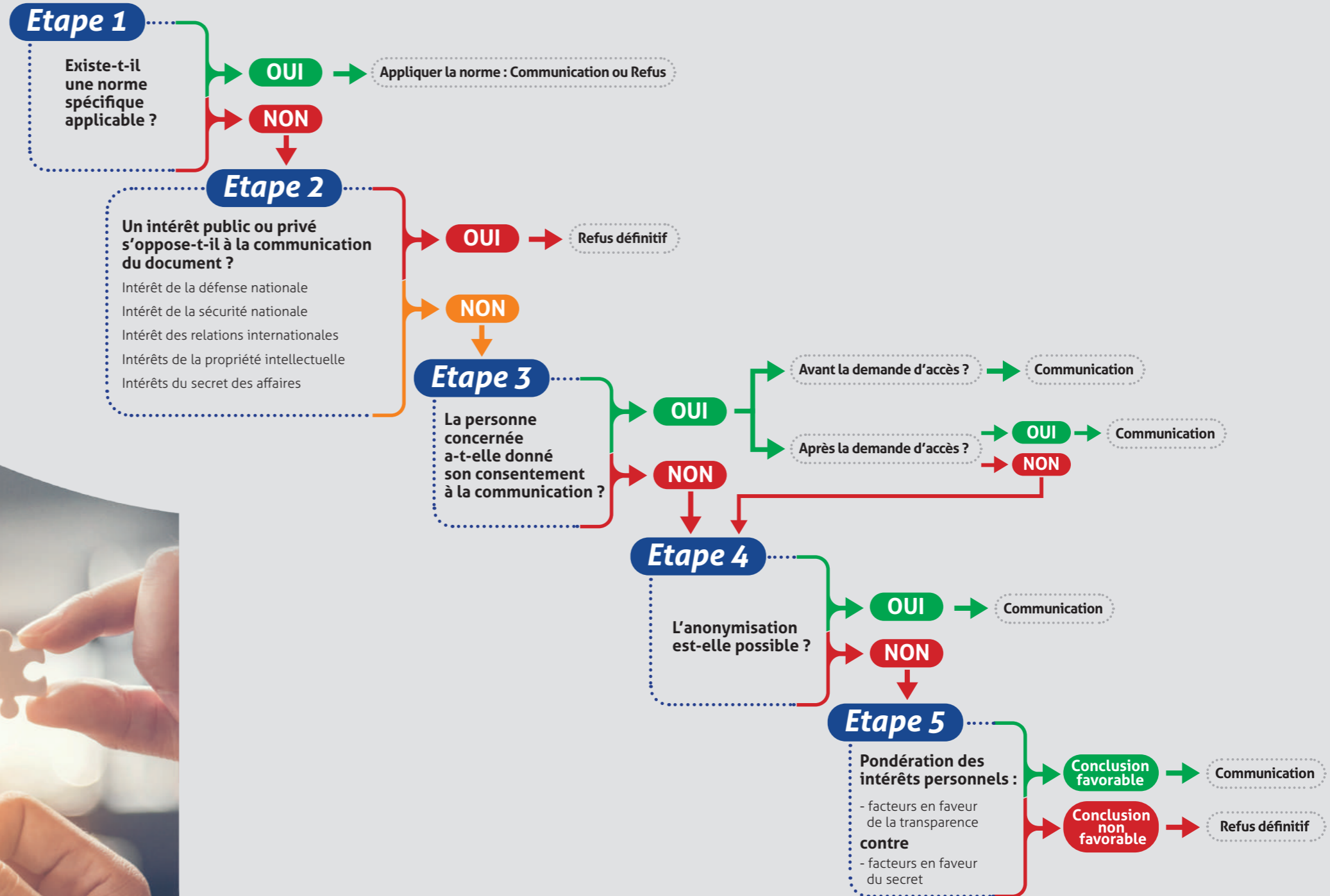
- les attentes élevées de la personne concernée en matière de confidentialité ; c'est le cas notamment des certificats médicaux, des évaluations de performances professionnelles ou des appréciations sur les qualités morales, des notes d'examens ou encore des sanctions administratives ou disciplinaires ;

- la vulnérabilité de la personne concernée ; les enfants, les personnes âgées, les personnes vivant dans la précarité, les personnes souffrant d'un handicap physique ou psychique, les victimes de sévices voient leur vie privée hautement sauvegardée;

- l'intensité de l'atteinte à la personnalité en cas de divulgation. Cette intensité peut résulter de la nature des plus intimes aspects de l'information (santé, orientation sexuelle, statut familial), mais aussi d'une éventuelle publication ultérieure à large échelle (par exemple dans des médias de grand tirage ou sur les réseaux sociaux).

À l'instar des autres exceptions à la transparence instituées par l'article 24 de la loi 22/2016 (cf. supra b), il importe que l'atteinte à la vie privée que pourrait causer la communication des données personnelles soit d'une certaine gravité. La personne concernée doit supporter des conséquences quelque peu désagréables ou embarrassantes.

SCHÉMA RÉCAPITULATIF



IV. LE MOT DE LA FIN



