# Principes globaux sur la sécurité nationale et le droit à l'information

(« Principes de Tshwane »)

# Principes globaux sur la sécurité nationale et le droit à l'information (« Principes de Tshwane »)

Ces principes globaux sur la sécurité nationale et le droit à l'information, lancés le 12 juin 2013, ont été développés par 22 groupes, dans le cadre d'un processus qui a permis de consulter, au cours de deux ans, plus de 500 experts provenant de plus de 70 pays à travers le monde. Le processus de rédaction s'est terminé lors d'une réunion à Tshwane, en Afrique du Sud, ville qui a donné son nom aux Principes.

**finalisés à Tshwane, Afrique du Sud**
**publiés le 12 juin 2013**

ISBN: 978-1-936133-98-7

Publié par
Open Society Foundations
Open Society Justice Initiative
224 West 57th Street
New York, NY 10019 USA
www.opensocietyfoundations.org

Design par Judit Kovács | Createch Ltd.

# Table des matières

# Introduction

Ces principes ont été élaborés afin de guider les personnes impliquées dans la rédaction, la révision ou la mise en œuvre de lois ou de dispositions liées à l'autorité de l'État à retenir des informations pour des raisons de sécurité nationale ou à punir la divulgation de telles informations.

Ils sont basés sur les lois, normes et bonnes pratiques nationales et internationales, ainsi que sur des publications d'experts.

Ils traitent de la sécurité nationale plutôt que de tous les motifs de rétention d'information. Tous les autres motifs publics de restriction de l'accès à l'information doivent au moins répondre à ces critères.

Ces principes ont été rédigés par 22 organisations et centres universitaires (liste en annexe), en consultation avec plus de 500 experts issus de plus de 70 pays, lors de 14 réunions organisées dans le monde entier par l'Open Society Justice Initiative, et en collaboration avec quatre rapporteurs spéciaux sur la liberté d'expression et/ou de la presse, ainsi que le rapporteur spécial sur le contre-terrorisme et les droits humains :

- le Rapporteur spécial des Nations Unies sur la Liberté d'opinion et d'expression,
- le Rapporteur spécial des Nations Unies sur le Contre-terrorisme et les droits humains,
- le Rapporteur spécial de la Commission africaine sur les droits de l'homme et des peuples (ACHPR) sur la Liberté d'expression et d'accès à l'information,
- le Rapporteur spécial de l'Organisation des États américains sur la Liberté d'expression, et
- le Représentant de l'Organisation pour la Sécurité et la coopération en Europe (OSCE) pour la Liberté de la presse.

# Contexte et raison d'être

La sécurité nationale et le droit de savoir du public sont souvent envisagés comme deux directions opposées. S'il existe parfois des conflits entre la volonté d'un gouvernement de préserver le secret de certaines informations pour des raisons de sécurité nationale et le droit du public à connaître les informations détenues par les autorités publiques, un examen lucide de l'histoire récente suggère que les intérêts légitimes de la sécurité nationale sont, en pratique, mieux protégés lorsque le public est bien informé sur les activités de l'état, y compris celles qui sont entreprises pour protéger la sécurité nationale.

En permettant l'examen de l'action de l'état par le public, l'accès à l'information protège non seulement des abus commis par les représentants du gouvernement, mais permet également au public de jouer un rôle dans l'élaboration des politiques de l'état. Il constitue donc un composant vital pour une sécurité nationale véritable, la participation démocratique et l'élaboration de politiques solides. Afin de protéger le plein exercice des droits humains, il peut être nécessaire, dans certaines circonstances, de préserver le secret de certaines informations afin de protéger les intérêts légitimes de la sécurité nationale.

Il est d'autant plus difficile de trouver le juste équilibre que, dans bien des pays, les tribunaux font preuve de peu d'indépendance et d'une grande allégeance à la volonté des gouvernements lorsque la sécurité nationale est invoquée. Cette déférence est renforcée par les dispositions des lois sur la sécurité de nombreux pays, qui prévoient des exceptions au droit à l'information ainsi qu'aux règles ordinaires concernant les preuves et le droit des accusés, et ce dès lors que le gouvernement présente des preuves minimes, voire la simple conviction qu'il existe un risque pour la sécurité nationale. Pour un gouvernement, invoquer la sécurité nationale de façon abusive peut gravement saper les principales protections institutionnelles contre les abus gouvernementaux : l'indépendance de la justice, l'état de droit, la supervision du législatif, la liberté de la presse et le gouvernement ouvert.

Ces Principes apportent des réponses à ces problématiques de longue date ainsi qu'au fait que, au cours des dernières années, un nombre important d'états du monde entier ont entrepris d'adopter ou de réviser des régimes de classification des informations et d'autres législations connexes. Cette tendance a, quant à elle, été suscitée par différents développements. Le plus important d'entre eux est sans doute l'adoption rapide de lois sur l'accès à l'information depuis la chute du Mur de Berlin. Grâce à elle, au moment de la publication de ces Principes, plus de 5,2 milliards de personnes réparties dans 95 pays du monde bénéficient d'un droit d'accès à l'information, au moins du point de vue de la loi sinon dans la pratique. Les populations de ces pays s'interrogent – souvent pour la première fois – sur l'éventualité du maintien du secret de certaines informations et des conditions dans lesquelles il est envisageable. Parmi les autres développements contribuant à une augmentation de propositions de lois sur le secret, il faut citer la réaction des gouvernements face au terrorisme ou à la menace d'actes terroristes et le souhait de confier à la loi la régulation du secret dans le contexte d'une transition démocratique.

# Préambule

Les organisations et personnes suivantes, impliquées dans la rédaction des présents Principes :

*Rappelant* que l'accès aux informations détenues par l'état est le droit de chaque individu, et donc que ce droit doit être protégé par des lois rédigées avec précision et assorties d'exceptions étroitement définies, en vue de la surveillance de ce droit par des tribunaux indépendants, des organismes parlementaires de supervision et d'autres institutions indépendantes ;

*Reconnaissant* que les états peuvent avoir un intérêt légitime à la retenue de certaines informations, notamment pour des raisons de sécurité nationale, et soulignant qu'il est vital, pour une société démocratique, de trouver un équilibre approprié entre divulgation et conservation des informations, et que cet équilibre est essentiel pour sa sécurité, son progrès, son développement, son bien-être et le plein exercice des droits humains et des libertés fondamentales ;

*Affirmant* qu'il est impératif, pour permettre aux peuples de surveiller la conduite de leur gouvernement et de participer pleinement à une société démocratique, qu'ils aient accès aux informations détenues par les autorités publiques, y compris les informations liées à la sécurité nationale ;

*Remarquant* que ces Principes s'appuient sur le droit et les normes internationales en relation avec le droit du public à accéder aux informations détenues par les autorités et avec d'autres droits humains, sur l'évolution des pratiques étatiques (comme en témoignent, entre autres, les jugements rendus par des cours et tribunaux nationaux et internationaux), sur les principes généraux de droit reconnus par la communauté des nations, et sur des publications d'experts ;

*Gardant à l'esprit* les dispositions pertinentes de la Déclaration universelle des droits humains, le Pacte international relatif aux droits civils et politiques, la Charte africaine sur les droits des hommes et des peuples, la Convention européenne sur les droits humains et la Convention du Conseil de l'Europe sur l'accès aux documents publics ;

*Gardant également à l'esprit* la Déclaration de principes sur la liberté d'expression de la Commission inter-américaine des droits humains, le Modèle inter-américain de loi sur l'accès à l'information, la Déclaration de principes sur la liberté d'expression en Afrique et le Modèle de loi sur l'accès à l'information pour l'Afrique ;

*Rappelant* la Déclaration conjointe de 2004 du Rapporteur spécial des Nations Unies sur la Liberté d'opinion et d'expression, du Représentant de l'OSCE sur la Liberté de la presse et du Rapporteur spécial sur la Liberté d'expression de la Commission inter-américaine sur les droits humains ; les Déclarations conjointes de 2006, 2008, 2009 et 2010 de ces trois experts et du Rapporteur spécial sur la Liberté d'expression et d'accès à l'information de la Commission africaine sur les droits des hommes et des peuples ; la Communication conjointe de décembre 2010 sur WikiLeaks des Rapporteurs spéciaux des Nations Unies et de la Commission inter-américaine, ainsi que le Rapport sur les mesures anti-terroristes et les droits humains, adopté par la Commission de Venise en 2010 ;

*Rappelant en outre* les Principes de Johannesburg sur la Sécurité nationale, la liberté d'expression et l'accès à l'information adoptés par un groupe d'experts réunis par l'Article 19 en 1995, et les Principes de Supervision et de transparence pour les services de sécurité dans une démocratie constitutionnelle élaborés en 1997 par le Centre d'étude sur la sécurité nationale (CNSS) et la Fondation polonaise d'Helsinki pour les droits humains ;

*Remarquant* qu'il existe des principes internationaux – tels que ceux inclus dans le Modèle de loi sur l'accès à l'information en Afrique, les Principes directeurs de l'ONU sur les droits des affaires et les droits humains (« Principes Ruggie »), le Traité sur le commerce des armes, les Directives de l'OCDE relatives aux entreprises multinationales, et le Document de Montreux sur les obligations juridiques pertinentes et les bonnes pratiques pour les États en ce qui concerne les opérations des entreprises militaires et de sécurité privées opérant pendant les conflits armés – qui reconnaissent l'importance cruciale de l'accès à l'information détenues par, ou en rapport avec, des entreprises commerciales dans certaines circonstances, et que certains d'entre eux traitent expressément de la nécessité, pour les entreprises militaires et de sécurité privées opérant dans le secteur de la sécurité nationale, de rendre certaines informations publiques ;

*Notant* que ces Principes ne fournissent pas de norme concrète concernant la collecte de renseignements, la gestion des données personnelles ni le partage de renseignement, sujets traités par les « bonnes pratiques concernant les cadres légaux et institutionnels régissant les services de renseignement et leur supervision » publiés en 2010 par Martin Scheinin, puis par le Rapporteur spécial des Nations Unies sur la promotion et la protection des droits humains et des libertés fondamentales dans le cadre de la lutte contre le terrorisme, à la demande du Conseil des droits de l'homme des Nations Unies ;

*Reconnaissant* l'importance d'un partage efficace du renseignement entre les états, tel que défendu par la Résolution 1373 du Conseil de sécurité de l'ONU ;

*Reconnaissant en outre* que les obstacles à la supervision du public et d'organismes indépendants créés au nom de la sécurité nationale augmentent le risque de conduite illégale, corrompue et frauduleuse tout en rendant sa détection plus difficile ; que les atteintes à la vie privée et aux autres droits individuels ont souvent lieu sous couvert du secret exigé par la sécurité nationale ;

*Inquiets* devant le coût que représente un excès de secret pour la sécurité nationale – obstacle au partage d'informations entre agences gouvernementales et entre alliés, incapacité à protéger les secrets légitimes, incapacité à trouver les informations importantes parmi la masse, collecte répétitive d'informations par de multiples agences et surcharge de travail pour les responsables de sécurité ;

*Soulignant* que les Principes se concentrent sur le droit du *public* à l'information et qu'ils traitent du droit à l'information des détenus, des victimes d'atteintes aux droits humains et autres personnes ayant des besoins d'information critiques dans la seule mesure où ces droits sont étroitement liés au droit du public à l'information ;

*Reconnaissant* que certaines informations ne devant pas être maintenues secrètes pour des raisons de sécurité nationales peuvent toutefois l'être pour d'autres motifs reconnus par le droit international – relations internationales, équité des procédures judiciaires, droits des parties en procès et droit à la vie privée – en respectant toujours le principe selon lequel l'information ne peut être maintenue secrète que lorsque l'intérêt du public au secret de l'information est nettement plus grand que l'intérêt du public à accéder à cette même information ;

*Souhaitant* fournir des directives concrètes aux gouvernements, aux corps législatifs et réglementaires, aux autorités publiques, aux rédacteurs de législations, aux tribunaux,

aux organismes de surveillance et à la société civile au sujet de certaines problématiques des plus complexes liées à l'intersection entre sécurité nationale et droit à l'information, en particulier celles qui impliquent le respect des droits humains et la transparence démocratique ;

*S'efforçant* d'élaborer des Principes ayant une valeur et une application universelles ;

*Reconnaissant* que les états font face à des défis très variés dans leur effort pour trouver un équilibre entre l'intérêt du public à accéder aux informations et la nécessité du secret pour protéger les intérêts légitimes de la sécurité nationale, et que, si les Principes sont universels, leur application pratique peut devoir satisfaire des réalités locales telles que des systèmes légaux différents ;

*Recommandent* que les organismes appropriés aux niveaux national, régional et international prennent des mesures pour diffuser et discuter ces Principes, et les appuient, les adoptent et/ou les mettent en œuvre dans la mesure du possible, dans l'optique de parvenir progressivement à la concrétisation complète du droit à l'information tel qu'exposé dans le Principe 1.

# Définitions

Dans ces Principes, sauf si le contexte impose une autre signification :

« **Entreprise privée appartenant au secteur de la sécurité nationale** » désigne une personne morale exerçant ou ayant exercé un commerce ou une activité dans le secteur de la sécurité nationale, mais uniquement à titre de sous-traitant, de prestataire de services ou de fournisseur d'installations, de personnel ou de produits incluant, entre autres, de l'armement, de l'équipement ou des renseignements. Cette notion inclut les entreprises militaires et de sécurité privées (EMSP). Elle n'inclut pas les personnes morales ayant la forme d'organisations à but non lucratif ou non gouvernementales.

« **Indépendant** » signifie libre de l'influence, de la direction ou du contrôle du pouvoir exécutif et de toutes les autorités du secteur de la sécurité, à la fois sur les plans institutionnel, financier et opérationnel.

« **Information** » désigne tout original ou toute copie de matériel documentaire, quelles que soient ses caractéristiques physiques, et tout autre matériel tangible ou intangible, quels que soient la forme et le support de sa conservation. Le terme inclut, entre autre, les archives, correspondances, faits, opinions, conseils, mémos, données, statistiques, libres, dessins, plans, cartes, schémas, photographies, enregistrements audio ou vidéo, documents, emails, registres, échantillons, modèles et données conservées sous toute forme électronique.

« **Information d'intérêt public** » désigne les informations qui sont pertinentes ou avantageuses pour le public et pas uniquement pour un intérêt individuel, et dont la divulgation est « dans l'intérêt du public », par exemple parce qu'elles sont utiles à la compréhension des activités du gouvernement par le public.

« **Intérêt légitime de sécurité nationale** » désigne un intérêt dont la finalité authentique et l'impact principal est de protéger la sécurité nationale, en conformité avec le droit international et national. (Les catégories d'informations dont la retenue peut être nécessaire pour protéger un intérêt légitime de la sécurité nationale sont présentées dans le Principe 9.) Un intérêt de sécurité national n'est pas légitime si sa finalité réelle ou son impact principal consiste à protéger un intérêt non lié à la sécurité nationale, par exemple à protéger un gouvernement ou des représentants de l'état d'une situation embarrassante ou de la mise au jour d'un méfait, à dissimuler des informations sur des atteintes aux droits humains, sur d'autres atteintes à la loi ou sur le fonctionnement d'institutions publiques, à renforcer ou à perpétuer un intérêt, un parti ou une idéologie politique en particulier, ou bien à faire taire des protestations légitimes.

« **Sécurité nationale** » n'est pas définie dans ces Principes. Le Principe 2 inclut une recommandation selon laquelle la « sécurité nationale » doit être définie précisément par le droit national, en conformité avec les besoins d'une société démocratique.

« **Autorités publiques** » inclut tous les organismes au sein des branches exécutive, législative et judiciaire à tous les niveaux d'autorité gouvernementale, constitutionnelle et statutaire, y compris les autorités du secteur de la sécurité, ainsi que les organismes non gouvernementaux qui sont la propriété ou sous le contrôle du gouvernement, ou qui servent en tant qu'agents du gouvernement. Les « autorités publiques » incluent également les entités privées ou autres qui assurent des fonctions ou des services publics, ou opèrent avec des fonds ou des bénéfices publics conséquents, mais uniquement dans le cadre de l'exercice de ces fonctions, de la prestation des services ou de l'utilisation des fonds ou bénéfices publics.

« **Personnel public** » ou « **fonctionnaire** » désigne un employé, un prestataire ou un sous-traitant, actuel ou passé, d'une autorité publique, y compris du secteur de la sécurité. Les « personnels publics » et les « fonctionnaires » incluent également les personnes employées par des organismes non gouvernementaux qui sont la propriété ou sous le contrôle du gouvernement, ou bien qui servent en tant qu'agents du gouvernement, ainsi que les employés des entités privées ou autres qui assurent des fonctions ou des services publics, ou opèrent avec des fonds ou des bénéfices publics conséquents, mais uniquement dans le cadre de l'exercice de ces fonctions, de la prestation des services ou de l'utilisation des fonds ou bénéfices publics.

« **Sanction** » désigne toute forme de pénalité ou de détriment et englobe les mesures pénales, civiles et administratives. Le verbe « sanctionner » désigne la mise en application de telle forme de pénalité ou de détriment.

« **Secteur de la sécurité** » est défini de façon à englober : (i) les fournisseurs de sécurité, ce qui inclut, entre autres, les forces armées, la police et autres organismes de maintien de la loi, les forces paramilitaires et les services de renseignement et de sécurité (militaires et civils), et (ii) tous les organismes exécutifs, départements et ministères responsables de la coordination, du contrôle et de la supervision des fournisseurs de sécurité.

# Partie I : Principes généraux

## Principe 1 : Droit à l'information

(a) Chacun a le droit de rechercher, recevoir, utiliser et faire connaître des informations détenues par des autorités publiques ou pour leur compte, ou des informations auxquelles les autorités publiques ont légalement le droit d'accéder.

(b) Les principes internationaux reconnaissent également que les entreprises privées appartenant au secteur de la sécurité nationale, ce qui inclut les entreprises privées militaires et de sécurité, ont la responsabilité de divulguer les informations concernant des situations, des activités ou des conduites pouvant être raisonnablement considérées comme ayant un impact sur l'exercice des droits humains.

(c) Ceux qui sont soumis à une obligation de divulgation d'informations, conformément avec les Principes 1(a) et 1(b) doivent communiquer ces informations sur demande, dans la limite des seules exceptions prévues par la loi et nécessaires pour éviter toute nuisance spécifique et identifiable à des intérêts légitimes, y compris ceux de la sécurité nationale.

(d) Seules les autorités publiques dont les responsabilités spécifiques incluent la protection de la sécurité nationale peuvent utiliser la sécurité nationale comme motif de rétention d'informations.

(e) Tout recours à la sécurité nationale par une entreprise privée pour retenir des informations doit être explicitement autorisé ou confirmé par une autorité publique chargée de la protection de la sécurité nationale.

*Remarque :C'est au gouvernement, et à lui seul, qu'incombe la responsabilité définitive de la sécurité nationale, et donc seul le gouvernement est en position d'affirmer qu'une information ne doit pas être divulguée si elle est susceptible de nuire à la sécurité nationale.*

(f) Les autorités publiques sont également dans l'obligation positive de publier de leur propre initiative certaines informations d'intérêt public.

## Principe 2 : Application de ces Principes

(a) Ces Principes s'appliquent à l'exercice du droit d'accès à l'information tel qu'identifié dans le Principe 1, lorsque le gouvernement affirme ou confirme que la divulgation de telles informations pourrait nuire à la sécurité nationale.

(b) Dans la mesure où la sécurité nationale est l'un des motifs publics les plus puissants pour la restriction d'informations, lorsque les autorités publiques recourent à d'autres motifs publics pour limiter l'accès – relations internationales, ordre public, santé et sécurité publiques, application de la loi, communication future de conseils libres et ouvertes, formulation effective de politique et intérêts économiques de l'état – elles doivent au moins satisfaire les normes concernant l'imposition de restrictions sur le droit d'accès à l'information présentées comme pertinentes dans ces Principes.

(c) Les bonnes pratiques exigent que la sécurité nationale, si elle doit être invoquée pour limiter le droit à l'information, soit précisément définie dans le cadre légal d'un pays, d'une manière conforme aux caractéristiques d'une société démocratique.

## Principe 3 : Critères de restriction du droit à l'information pour des raisons de sécurité nationale

Aucune restriction ne peut être imposée au droit à l'information pour des motifs de sécurité à moins que le gouvernement ne puisse établir ce qui suit : (1) la restriction est (a) prévue par la loi et (b) nécessaire dans une société démocratique (c) pour protéger un intérêt légitime de sécurité nationale ; et (2) la loi prévoit des protections adéquates contre les abus, y compris l'examen rapide, complet, accessible et effectif de la validité

de la restriction par une autorité indépendante de supervision et une revue complète par les tribunaux.

(a) *Prévue par la loi*. La loi doit être accessible, dépourvue d'ambiguïté, étroitement et précisément définie de manière à permettre aux individus de comprendre quelles informations peuvent être retenues, lesquelles doivent être divulguées et quelles actions relatives aux informations sont soumises à des sanctions.

(b) *Nécessaire dans une société démocratique*.

(i) La divulgation de l'information doit présenter un risque réel et identifiable de dommage conséquent à un intérêt légitime de sécurité nationale.

(ii) Le risque de dommage lié à la divulgation doit être supérieur à l'intérêt public d'une divulgation.

(iii) La restriction doit respecter le principe de proportionnalité et doit constituer le moindre moyen disponible de protection contre le dommage.

(iv) La restriction ne doit pas entraver l'essence du droit à l'information.

(c) *Protection d'un intérêt légitime de sécurité nationale*. Les catégories étroites d'informations pouvant être retenues pour des raisons de sécurité nationales doivent être clairement exposées dans la loi.

*Remarques : Voir plus haut la définition de l'expression « intérêt légitime de sécurité nationale » dans la section des Définitions. Le Principe 3(b) est d'autant plus important si la sécurité nationale n'est pas clairement définie dans la loi comme le recommande le Principe 2.*

*« Intérêt (du) public » n'est pas défini dans ces Principes. Une liste des catégories d'intérêt public particulièrement élevé, devant faire l'objet d'une publication proactive et ne devant jamais faire l'objet de restrictions, est présentée dans le Principe 10. Une liste des catégories de méfaits présentant un intérêt élevé pour le public, et que les fonctionnaires doivent et peuvent divulguer sans craindre de représailles, est présentée dans le Principe 37.*

*Dans la détermination du juste équilibre entre risque de dommage et intérêt public de la divulgation, il est nécessaire de tenir compte de la possibilité de réduire les risques dus à la divulgation, notamment par des moyens exigeant des dépenses raisonnables. À titre d'illustration, la liste suivante présente des facteurs à prendre en compte afin de déterminer si l'intérêt du public est plus fort que le risque de dommage :*

- *facteurs en faveur de la divulgation : la divulgation est raisonnablement susceptible de (a) promouvoir une discussion ouverte des affaires publiques, (b) renforcer la responsabilité et la transparence du gouvernement, (c) contribuer à un débat positif et informé sur des problématiques importantes ou des questions de grand intérêt, (d) promouvoir la supervision effective des dépenses de fonds publics, (e) révéler les motifs d'une décision du gouvernement, (f) contribuer à la protection de l'environnement, (g) révéler des menaces pensant sur la santé ou la sécurité du public, ou (h) révéler des atteintes aux droits humains ou au droit humanitaire international, ou contribuer à en établir les responsabilités.*
- *facteurs en faveur de la rétention : la divulgation est susceptible de présenter un risque réel et identifiable de dommage à un intérêt légitime de sécurité nationale ;*
- *facteurs non pertinents : on peut raisonnablement penser que la divulgation va (a) embarrasser ou décrédibiliser un gouvernement ou un représentant officiel, ou (b) affaiblir un parti ou une idéologie politique.*

*Le fait que la divulgation est susceptible de nuire à l'économie d'un pays est un critère pertinent lorsqu'il s'agit de déterminer si une information doit être retenue pour ce motif, mais ne permet pas de conclure qu'une information doit être retenue pour des raisons de sécurité nationale.*

## Principe 4 : Responsabilité de l'Autorité publique de la détermination de la légitimité d'une restriction

(a) La responsabilité de la démonstration de la légitimité d'une restriction incombe à l'autorité publique qui cherche à retenir l'information.

(b) Le droit à l'information doit être interprété et appliqué largement, et toutes les restrictions doivent être interprétées étroitement.

(c) Pour remplir cette responsabilité, il ne suffit pas à l'autorité publique qu'elle affirme simplement qu'il existe un risque ; elle est dans l'obligation de fournir des raisons spécifiques et substantielles pour appuyer ses affirmations.

*Remarque : Toute personne cherchant à accéder à l'information doit avoir la possibilité de questionner la base déclarée de l'évaluation du risque devant une autorité administrative et une autorité judiciaire, conformément aux Principes 26 et 27.*

(d) En aucun cas la simple assertion, par exemple sous la forme d'un certificat émis par un ministre ou autre représentant officiel déclarant que la divulgation pourrait nuire à la sécurité nationale, ne sera considérée comme définitive en ce qui concerne le point qu'elle défend.

## Principe 5 : Aucune exemption pour les autorités publiques

(a) Aucune autorité publique – qu'il s'agisse du pouvoir judiciaire, de la législature, des institutions de surveillance, des agences de renseignement, des forces armées, de la police, d'autres agences de sécurité, des services du chef de l'État et du gouvernement, ou de services inclus dans les précédents – ne peut être exemptée des exigences de divulgation.

(b) Les informations ne peuvent être retenues pour des raisons de sécurité nationale au seul motif qu'elles ont été générées ou communiquées par un état étranger ou un organisme intergouvernemental, une autorité publique particulière ou une certaine unité au sein d'une autorité.

*Remarque : Concernant les informations produites par un état étranger ou un organisme intergouvernemental, voir le Principe 9 (a)(v).*

## Principe 6 : Accès aux informations pour les organismes de surveillance

Tous les organismes de surveillance, de médiation et d'appel, y compris les cours et tribunaux, doivent avoir accès à toutes les informations, y compris relatives à la sécurité nationale, qui sont nécessaires à l'exercice de leurs fonction, et ce quel qu'en soit le niveau de classification.

*Remarque : Ce principe est approfondi dans le Principe 32. Il ne concerne pas la divulgation d'informations au public par les organismes de surveillance. Les organismes de surveillance doivent préserver le secret de toutes les informations qui ont été légitimement classées, conformément à ces Principes et comme prévu par le Principe 35.*

## Principe 7 : Ressources

Les états doivent consacrer des ressources adéquates et prendre toutes les mesures nécessaires telles que la publication de régulations et la bonne gestion des archives pour assurer la mise en application de ces Principes.

## Principe 8 : États d'urgence

En cas d'état d'urgence menaçant la vie de la nation et proclamé comme tel officiellement et légalement, conformément au droit national et international, un état peut déroger à ses obligation concernant le droit de rechercher, recevoir et faire connaître des informations, seulement dans la mesure strictement requise par les exigences de la situation et tant que la dérogation est conforme aux autres obligations de l'état d'après le droit international, et qu'elle n'implique aucune discrimination d'aucune sorte.

*Remarque : Certains aspects du droit de rechercher, recevoir et faire connaître des informations et des idées sont si fondamentaux pour l'exercice de droits non aliénables, qu'ils doivent toujours être entièrement respectés, y compris lors des périodes d'urgence publique. À titre d'exemple non exhaustif, les informations mentionnées dans le Principe 10 sont de cette nature.*

# Partie II : Informations pouvant être retenues pour des raisons de sécurité nationales, et informations devant être divulguées

## Principe 9 : Informations pouvant être légitimement retenues

(a) Les autorités publiques peuvent limiter le droit du public à accéder à des informations pour des raisons de sécurité nationales, mais seulement si ces limites sont conformes à toutes les autres dispositions de ces Principes, que les informations sont détenues par une autorité publique et qu'elles entrent dans l'une des catégories suivantes :

(i) Informations concernant des programmes, des opérations ou des capacités de défense, pendant toute la période d'utilité opérationnelle des informations.

*Remarque : L'expression « pendant toute la période d'utilité opérationnelle des informations » a pour objet d'exiger la divulgation des informations une fois que celles-ci ne révèlent plus rien qui puisse être utilisé par un ennemi pour comprendre la préparation, les capacités ou les plans d'un état.*

(ii) Informations concernant la production, les capacités ou l'utilisation d'armes ou autres systèmes militaires, y compris les systèmes de communication.

*Remarque : Ces informations incluent les données et inventions technologiques et les informations relatives à leur production, leurs capacités ou leur utilisation. Les informations relatives aux décisions budgétaires concernant des armes ou autres systèmes militaires doivent être rendues publiques. Voir les Principes 10C (3) et 10F. La bonne pratique consiste, pour un état, à maintenir et publier une liste de contrôle des armes, comme l'encourage le Traité sur le commerce des armes au sujet des armes conventionnelles. La bonne pratique consiste également à publier des informations sur les armes, l'équipement et les effectifs des troupes.*

(iii) Informations relatives à des mesures spécifiques de protection du territoire de l'état, des infrastructures critiques ou des institutions essentielles contre les menaces ou l'usage de la force ou du sabotage, et dont l'efficacité dépend de leur secret ;

*Remarque : Les « infrastructures critiques » désignent les ressources, actifs et systèmes stratégiques, qu'ils soient virtuels ou physiques, qui ont un tel caractère vital pour l'état que leur destruction ou leur mise hors service handicaperait la sécurité nationale.*

(iv) Informations liées à, ou dérivées des opérations, sources et méthodes des services de renseignement, dans la mesure où elles concernent des questions de sécurité nationale ;

(v) Informations concernant les questions de sécurité nationales et fournies par un état étranger ou un organisme intergouvernemental avec des attentes expresses de confidentialité, et autres communications diplomatiques dans la mesure où elles concernent des questions de sécurité nationale.

*Remarque : La bonne pratique consiste à consigner ces attentes de confidentialité par écrit.*

*Remarque : Dans la mesure où des informations particulières concernant le terrorisme et les mesures anti-terrorisme sont couvertes par l'une des catégories ci-dessus, le droit du public à y accéder peut être soumis à des restrictions pour des raisons de sécurité nationale, conformément à plusieurs dispositions des Principes, dont celle-ci. Dans le même temps, certaines informations concernant le terrorisme ou les mesures anti-terrorisme peuvent être d'un intérêt particulièrement élevé pour le public : voir par exemple les Principes 10A, 10B et 10H(1).*

(b) La bonne pratique consiste à faire figurer dans le droit national une liste exclusive de catégories d'informations définies de façon au moins aussi étroite que les catégories ci-dessus.

(c) Un état peut ajouter une catégorie à la liste ci-dessus, mais seulement si la catégorie est spécifiquement identifiée et définie de façon étroite, et si la préservation du secret de l'information est nécessaire pour protéger un intérêt légitime de sécurité nationale prévu dans la loi, comme suggéré par le Principe 2(c). En proposant la catégorie, l'état doit expliquer en quoi la divulgation d'informations de cette catégorie pourrait nuire à la sécurité nationale.

## Principe 10 : Catégories d'informations dont l'intérêt public est présumé ou estimé supérieur et devant donc être divulguées

Certaines catégories d'informations – dont celles énumérées plus bas – sont d'un intérêt public particulièrement élevé en raison de leur importance spéciale dans le processus de contrôle démocratique et d'état de droit. En conséquence, on présume fortement que ces informations doivent être publiques et divulguées de façon proactive, et dans certains cas cette présomption est un impératif indiscutable.

Les informations appartenant aux catégories suivantes doivent bénéficier au minimum d'une forte présomption en faveur de la divulgation, et ne peuvent être retenues pour des raisons de sécurité nationale que dans les circonstances les plus exceptionnelles et en conformité avec les autres principes, pour une période strictement limitée seulement, dans le seul cadre de la loi, et uniquement s'il n'existe aucun moyen raisonnable de limiter l'impact négatif d'une divulgation. Dans le cas de certaines sous-catégories d'informations, identifiées ci-dessous comme présentant par nature un intérêt public impératif, le secret au motif de la sécurité nationale ne peut jamais être justifié.

### A. Violations des droits humains et du droit humanitaire international

(1) Il existe un intérêt public impératif pour la divulgation d'informations concernant de graves violations des droits humains ou du droit humanitaire international, telles que les crimes contre le droit international et les violations systématiques ou fréquentes des libertés individuelles et des droits à la sécurité. Ces informations

ne peuvent être retenues pour des raisons de sécurité nationale quelles que soient les circonstances.

(2) Les informations concernant d'autres violations des droits humains ou du droit humanitaire sont soumise à une forte présomption de divulgation et ne peuvent en aucun cas être retenues pour des raisons de sécurité nationale d'une manière qui protège les responsables des violations ou qui empêche une victime d'accéder à un recours effectif.

(3) Lorsqu'un état traverse un processus de justice transitionnelle au cours duquel il est particulièrement chargé d'assurer la vérité, la justice, la réparation et les garanties de non-récidive, il existe un impératif indiscutable de divulgation à la société dans son ensemble de toutes les informations relatives aux atteintes aux droits humains commises sous le régime précédent. Le gouvernement succédant doit immédiatement protéger et préserver l'intégrité des archives contenant les informations dissimulées par le précédent gouvernement, et en assurer la publication sans délai.

*Remarque : Voir le Principe 21(c) concernant le devoir de recherche ou de reconstruction des informations relatives aux violations des droits humains.*

(4) Lorsque l'existence de violations est contestée ou suspectée plutôt qu'établie, ce Principe s'applique aux informations qui, prises hors contexte ou en conjonction avec d'autres informations, permettraient de faire la lumière sur la réalité des allégations de violation.

(5) Ce Principe s'applique aux informations concernant les violations qui ont eu lieu ou sont en train de se produire, et il s'applique de la même façon si les atteintes ont été commises par l'état qui détient les informations ou par une autre entité.

(6) Les informations relatives aux violations couvertes par ce Principe incluent, entre autres, les suivantes :

(a) Une description complète, assortie de tout document à l'appui, des actes ou omissions qui constituent les violations, ainsi que les dates et les circonstances de leur survenue et, le cas échéant, l'emplacement des personnes disparues ou des dépouilles.

(b) L'identité de toutes les victimes, dans les limites du respect de la vie privée et autres droits des victimes, de leurs proches et des témoins, ainsi que les

données agrégées ou autrement anonymisées concernant leur nombre ou des caractéristiques pouvant être pertinentes pour la protection des droits humains.

*Remarque : Le nom et les données personnelles des victimes, de leurs proches et des témoins peuvent être retenus afin de les protéger de tout danger supplémentaire, si les personnes concernées ou, dans le cas de personnes décédées, les membres de leur famille demandent que ces informations soient maintenues secrètes, expressément et de leur plein gré, ou bien si le secret de ces informations est manifestement conforme aux souhaits de la personnes ou aux besoins particuliers de groupes vulnérables. Concernant les victimes de violences sexuelles, un consentement explicite à la divulgation de leur nom et autres données personnelles doit être exigé. Les victimes mineures (moins de 18 ans) ne doivent pas être identifiées publiquement. Ce Principe doit toutefois être interprété en gardant à l'esprit le fait que des gouvernements ont, à différentes époques, dissimulé des violations des droits humains au regard du public en invoquant le droit à la vie privée, y compris justement celui des personnes dont les droits étaient ou avaient été gravement violés, sans égard pour la volonté réelle des individus affectés. Ces écueils ne doivent toutefois pas empêcher la publication de données agrégées ou autrement anonymisées.*

(c) Les noms des agences et des individus qui ont perpétré des violations ou qui ont une part de responsabilité dans les crimes commis, et plus généralement de toutes les unités du secteur de la sécurité présentes au moment des violations ou impliquées d'une quelconque façon, ainsi que ceux de leurs supérieurs et de leurs commandants, et les informations relatives à leur degré de contrôle et leurs prérogatives.

(d) Les informations sur les causes des violations et l'échec de leur prévention.

## B. Protection des libertés individuelles et du droit à la sécurité, de la prévention de la torture et autres mauvais traitements, et du droit à la vie

Les informations couvertes par ce Principe incluent :

(1) Les lois et réglementations qui autorisent la privation de la vie d'une personne par l'état, et les lois et réglementations concernant la privation de liberté et notamment les motifs, les procédures, les transferts, les traitements et les conditions de détention des personnes concernées, en incluant les méthodes d'interrogation. La divulgation de ces lois et réglementations fait l'objet d'un intérêt public impératif.

*Remarques : L'expression « Lois et réglementations » telle qu'elle est utilisée dans le Principe 10 comprend l'ensemble des législations principales et secondaires, statuts, réglementations et ordonnances, ainsi que les décrets et ordres exécutifs publiés par un président, un premier ministre, un ministre ou autre représentant de l'autorité publique, et les décisions de justice ayant force de loi. Les « lois et réglementations » incluent également les règles et interprétations de la loi qui sont considérées comme faisant autorité par les représentants du pouvoir exécutif.*

*La privation de liberté englobe toutes les formes d'arrestation, de détention, d'emprisonnement et d'internement.*

(2) La localisation de tous les lieux de privation de liberté gérés par l'état ou en son nom, ainsi que l'identité de toutes les personnes privées de liberté, les charges qui pèsent sur elles ou les motifs de leur détention, et ce y compris pendant un conflit armé.

(3) Les informations concernant la mort en détention de toute personne, et les informations relatives à tout décès dont un état est responsable : identité des personnes tuées, circonstances de leur mort et localisation de leur dépouille.

*Remarque : En aucun cas ne peuvent être retenues, au motif de la sécurité nationale, des informations dont la non-divulgation entraîne la détention secrète d'une personne, la création et l'utilisation de lieux de détention secrets, ou des exécutions secrètes. Aucune circonstance ne permet non plus que le destin ou la localisation d'une personne privée de liberté par l'état ou avec son autorisation, son soutien ou sa validation, ne soit dissimulé ou refusé aux membres de sa famille ainsi qu'aux autres personnes ayant un intérêt légitime pour le bien-être de cette personne.*

*Le nom et les données personnelles des personnes qui ont été privées de liberté, qui sont décédées en détention ou dont le décès a été provoqué par des agents de l'état, peuvent être maintenus secrets vis-à-vis du public dans le but de protéger le droit à la vie privée des personnes concernées si elles ou les membres de leur famille dans le cas de personnes décédées demandent expressément et volontairement la retenue des informations, et si leur retenue est conforme aux droits humains. L'identité des enfants privés de liberté ne doit pas être communiquée au public. Ces écueils ne doivent toutefois pas empêcher la publication de données agrégées ou autrement anonymisées.*

## C. Structures et pouvoirs du gouvernement

Les informations couvertes par ce Principe incluent, entre autres, les suivantes :

(1) L'existence de toutes les entités militaires, de police, de sécurité et de renseignement, ainsi que leurs sous-unités.

(2) Les lois et réglementations applicables à ces autorités ainsi que leurs organismes de surveillance et leurs mécanismes internes de contrôle, et les noms des représentants officiels qui dirigent ces entités.

(3) Les informations nécessaires pour évaluer et contrôler les dépenses de fonds publics, y compris les budgets globaux, les postes de dépense principaux et les informations de base sur les dépenses de ces entités.

(4) L'existence et les termes des accords bilatéraux et multilatéraux et autres engagements internationaux majeurs pris par l'état en lien avec des questions de sécurité nationale.

## D. Choix du recours à la force militaire ou de l'acquisition d'armes de destruction massive

(1) Les informations couvertes par ce Principe incluent les informations relatives à une décision d'engager des troupes de combat ou d'entreprendre une action militaire, et cela englobe la confirmation de la réalisation de cette action, son envergure et sa portée générales, ainsi qu'une explication de son motif et toute information pouvant prouvé qu'un fait publiquement cité comme motif était erroné.

*Remarque : La référence à l'envergure et la portée « générales » d'une action reconnaît qu'il doit généralement être possible de satisfaire un intérêt public élevé pour l'accès aux informations relatives à la décision d'engager des troupes sans pour autant révéler tous les détails des aspects opérationnels de l'action militaire en question (voir Principe 9).*

(2) La possession ou l'acquisition d'armes nucléaires ou autres armes de destruction massives par un état, sans nécessairement inclure de détails concernant leur fabrication ou leurs capacités opérationnelles, constitue une question d'intérêt public supérieur et ne peut être maintenue secrète.

*Remarque : Ce sous-principe ne doit en aucun cas être lu comme une quelconque validation de l'acquisition de telles armes.*

## E. Surveillance

(1) Le cadre légal général concernant toutes les formes de surveillance ainsi que les procédures à suivre pour autoriser la surveillance, sélectionner les cibles de surveillance et utiliser, partager, conserver et détruire les données interceptées, doivent être accessibles au public.

*Remarque : Ces informations incluent : (a) les lois régissant toutes les formes de surveillance, couvertes ou ouvertes, y compris la surveillance indirecte telle que le profilage et la recherche de données, et les types de mesures de surveillance pouvant être utilisés ; (b) les objectifs autorisés de la surveillance ; (c) le seul de suspicion requis pour initier ou poursuivre une opération de surveillance ; (d) les limitations portant sur la durée des mesures de surveillance ; (e) les procédures visant à autoriser et contrôler l'utilisation de ces mesures ; (f) les types de données personnelles pouvant être recueillies et/ou traitées à des fins de sécurité nationale ; et (g) les critères qui s'appliquent à l'utilisation, la rétention, la suppression et le transfert de ces données.*

(2) Le public doit également avoir accès aux informations concernant les entités autorisées à effectuer des opérations de surveillance et aux statistiques sur l'utilisation de la surveillance.

*Remarques : Ces informations incluent l'identité de toutes les entités gouvernementales recevant chaque année une autorisation spécifique pour la conduite d'opérations de surveillance particulières, le nombre d'autorisations de surveillance accordées chaque année à ces entités, les meilleures informations disponibles concernant le nombre d'individus et le nombre de communications soumises à une surveillance chaque année, ainsi que la présence ou non d'une autorisation spécifique pour ces opérations de surveillance et l'entité gouvernementale qui l'a émise le cas échéant.*

*Le droit du public à l'information ne s'étend pas nécessairement aux faits ou aux détails opérationnels des opérations de surveillance conduites dans le cadre de la loi et conformes aux obligations des droits humains. Ces informations peuvent être maintenues secrètes vis-à-vis du public et des personnes faisant l'objet de la surveillance, au moins jusqu'au terme de la période de surveillance.*

(3) De plus, le public doit être pleinement informé de tous les cas de surveillance illégale. Les informations relatives à ces cas de surveillance doivent être divulguées dans la plus grande mesure possible sans enfreindre le droit à la vie privée des personnes soumises à la surveillance.

(4) Ces Principes couvrent le droit du public à accéder aux informations et ne portent pas préjudice aux autres droits fondamentaux et procéduraux des personnes qui ont fait, ou pensent avoir fait, l'objet d'une surveillance.

*Remarque : La bonne pratique consiste, pour les autorités publiques, à devoir informer les personnes qui ont fait l'objet d'une surveillance couverte (en fournissant, au minimum, des informations sur le type de mesures employées, les dates de surveillance et l'organisme ayant autorisé la surveillance) dans la mesure où cela peut être fait sans compromettre des opérations en cours, des sources ou des méthodes.*

(5) La forte présomption en faveur de la divulgation reconnue par ce Principe ne s'applique pas aux informations uniquement liées à la surveillance des activités des gouvernements étrangers.

*Remarque : Les informations obtenues par la surveillance couverte, notamment sur les activités de gouvernements étrangers, doivent faire l'objet d'une divulgation dans les circonstances identifiées dans le Principe 10A.*

## F. Informations financières

Les informations couvertes par ce Principe incluent les informations suffisantes pour permettre au public de comprendre les finances du secteur de la sécurité ainsi que les règles qui régissent les finances du secteur de la sécurité. Ces informations doivent inclure, entre autres :

(1) Les budgets des départements et des agences ainsi que leurs différents intitulés ;

(2) Les déclarations financières de fin d'année avec les intitulés ;

(3) Les règles de gestion financière et les mécanismes de contrôle ;

(4) Les règles de l'approvisionnement ;

(5) Les rapports rédigés par les institutions de contrôle supérieures et autres organismes responsables de l'examen des aspects financiers du secteur de la sécurité, y compris les résumés des sections classifiées de ces rapports.

## G. Transparence en matière d'infractions constitutionnelles et statutaires et autres abus de pouvoir

Les informations couvertes par ce Principe incluent les informations relatives à l'existence, la nature et l'envergure des infractions constitutionnelles et statutaires et des autres abus de pouvoir commis par les autorités publiques ou leur personnel.

## H. Santé publique, sécurité publique et environnement

Les informations couvertes par ce Principe incluent :

(1) En cas de menace imminente ou actuelle pour la santé publique, la sécurité publique ou l'environnement, toutes les informations pouvant permettre au public de comprendre ou de prendre des mesures pour prévenir ou réduire les risques liés à cette menace, que celle-ci soit due à des causes naturelles ou à des activités humaines, y compris des actions de l'état ou d'entreprises privées.

(2) D'autres informations, régulièrement actualisées, sur l'exploitation des ressources naturelles, la pollution et les inventaires d'émissions, l'impact environnemental des grands travaux publics et des opérations d'extraction majeures en projet ou en cours, ainsi que les évaluations des risques et les plans de gestion des installations particulièrement dangereuses.

# Partie III.A : Règles concernant la classification et la déclassification des informations

## Principe 11 : Devoir de fournir les motifs de la classification des informations

(a) Qu'un état dispose ou non d'un processus formel pour la classification des informations, les autorités publiques sont obligées de fournir les motifs de la classification des informations.

*Remarque : La « Classification » est le processus par lequel des documents contenant des informations sensibles sont examinés afin qu'une marque puisse leur être attribuée, définissant qui peut y accéder et dans quelles conditions il doit être manipulé. La bonne pratique consiste à mettre en place un système formel de classification, afin de réduire la place de l'arbitraire et tout excès de secret.*

(b) Les raisons doivent indiquer la catégorie des informations parmi les catégories étroites énumérées dans le Principe 9 et décrire les dommages pouvant résulter d'une divulgation, leur degré de gravité et la probabilité qu'ils se concrétisent.

(c) Si différents niveaux de classification sont employés, ils doivent correspondre au degré de gravité et à la probabilité indiqués dans la justification.

(d) Lorsque des informations sont classifiées, (i) un marquage de protection doit être apposé au document, indiquant le niveau éventuel de la classification et sa durée

maximale, et (ii) une déclaration doit être incluse, justifiant la nécessité de classifier à ce niveau et pendant la période indiquée.

*Remarque : On encourage à fournir une déclaration justifiant chaque décision de classification parce que cela contraint les représentants officiels à porter attention aux dommages spécifiques pouvant résulter de la divulgation, et parce que cela facilite le processus de déclassification et de divulgation. Le marquage paragraphe par paragraphe favorise encore plus la cohérence de la divulgation des portions non classifiées des documents.*

## Principe 12 : Accès du public aux règles de classification

(a) Le public doit avoir l'opportunité de commenter les procédures et les normes régissant la classification avant leur prise d'effet.

(b) Le public doit avoir accès aux procédures écrites et aux normes régissant la classification.

## Principe 13 : Autorité de classification

(a) Seuls les agents officiels autorisés ou désignés, tels que définis par la loi, sont habilités à classifier des informations. Si un agent officiel non habilité pense qu'une information doit être classifiée, l'information peut être considérée classifiée pendant une période brève et expressément définie jusqu'à ce qu'un agent officiel habilité ait examiné la recommandation de classification.

*Remarque : En l'absence de dispositions légales contrôlant l'autorité de classification, la bonne pratique consiste à spécifier au moins cette autorité de délégation dans une réglementation.*

(b) L'identité de la personne responsable d'une décision de classification doit être traçable ou indiquée dans le document, à moins que des raisons impératives ne justifient que son identité ne soit dissimulée, et ce à des fins de transparence.

(c) Les agents officiels désignés par la loi doivent attribuer une autorité de classification au plus petit nombre possible de cadres subordonnés permettant l'efficacité de l'administration.

*Remarque : La bonne pratique consiste à publier des informations sur le nombre de personne ayant l'autorité requise pour classifier des informations et le nombre de personnes ayant accès aux informations classifiées.*

## Principe 14 : Faciliter la remise en question interne de la classification

Le personnel public, y compris le personnel affilié au secteur de la sécurité, qui pense que des informations ont été classifiées sans justification, peut remettre en question leur classification.

*Remarque : Les membres du personnel du secteur de la sécurité se distinguent en ce qu'ils doivent être particulièrement encouragés à remettre en question la classification, étant donnée l'importance de la culture du secret qui règne dans les agences de sécurité, le fait que la plupart des pays n'ont pas établi ni désigné d'organisme indépendant pour recevoir les réclamations du personnel de sécurité, et que la divulgation d'informations de sécurité entraîne souvent des pénalités plus graves que celle d'autres informations.*

## Principe 15 : Devoir de préserver, gérer et maintenir les informations de sécurité nationale

(a) Les autorités publiques ont le devoir de préserver, gérer et maintenir les informations dans le respect des normes internationales.[I] Les informations ne peuvent être exemptées de préservation, de gestion et de maintenance qu'en conformité avec la loi.

(b) Les informations doivent être correctement maintenues. Les systèmes d'archivage doivent être cohérents, transparents (sans révéler d'informations légitimement classifiées) et complets, de façon à ce que des demandes d'accès spécifiques per-

1. Documents de référence : Conseil international sur les archives (ICA), *Principes d'accès aux archives* (2012) ; ICA, *Déclaration universelle sur les archives* (2010 ; avec l'appui de l'UNESCO); Conseil de l'Europe, *Recommandation No R(2000)13 sur une politique européenne d'accès aux archives* (2000) ; Antonio González Quintana, ICA, *Politique d'archivage pour la protection des droits humains: version actualisée et plus complète du rapport préparé par l'UNESCO et le Conseil international sur les archives (1995), concernant la gestion des archives des services de sécurité d'état des anciens régimes répressifs* (2009).

mettent de localiser toutes les informations pertinentes, même si celles-ci ne sont pas divulguées.

(c) Chaque organisme public doit créer, publier, réviser et actualiser régulièrement une liste détaillée et exacte des dossiers classifiés qu'il détient, à l'exception des documents exceptionnels, le cas échéants, dont l'existence-même peut être légitimement tenue secrète conformément au Principe 19.

*Remarque : La bonne pratique consiste à mettre à jour ces listes une fois par an.*

## Principe 16 : Limitation dans le temps de la classification

(a) Les informations peuvent être tenues secrètes pour des raisons de sécurité nationale uniquement pour la durée nécessaire à la protection d'un intérêt légitime de sécurité nationale. Les décisions de classification des informations doivent être révisée régulièrement afin d'assurer le respect de ce Principe.

*Remarque : La bonne pratique consiste à ce qu'un statut exige cette révision au moins tous les cinq ans. Plusieurs pays imposent une révision selon des intervalles plus courts.*

(b) Le responsable de la classification doit indiquer la date, les conditions ou l'événement qui déterminera la fin de la classification.

*Remarque : La bonne pratique consiste à soumettre à des révisions régulières cette date d'échéance ou bien les conditions ou l'événement permettant de déclassifier les informations.*

(c) Aucune information ne peut rester classifiée indéfiniment. La période maximale présumée de classification pour des raisons de sécurité nationale doit être établie par la loi.

(d) Les informations ne peuvent être retenues au-delà de l'échéance présumée qu'en cas de circonstances exceptionnelles, conformément à une nouvelle décision de classification prise par un autre décideur et définissant une nouvelle date d'échéance.

## Principe 17 : Procédures de déclassification

(a) La législation nationale doit identifier la responsabilité du gouvernement dans la coordination, la supervision et l'exécution des activités de déclassification du gouvernement, y compris la consolidation et l'actualisation régulière des directives de déclassification.

(b) Des procédures doivent être mises en place pour identifier les informations classifiées d'intérêt public en vue d'une déclassification prioritaire. Si des informations d'intérêt public, entrant notamment dans l'une des catégories énumérées au Principe 10, sont classifiées en raison d'une sensibilité exceptionnelle, elles doivent être déclassifiées aussi rapidement que possible.

(c) La législation nationale doit établir des procédures pour la déclassification *en bloc*.

(d) La législation nationale doit identifier des périodes fixes de déclassification automatique pour les différentes catégories d'informations classifiées. Pour minimiser la charge de la déclassification, les archives doivent être automatiquement déclassifiées sans examen à chaque fois que cela est possible.

(e) La législation nationale doit définir une procédure accessible et publique de demande de déclassification de documents.

(f) Les documents déclassifiés, ce qui inclut ceux qui ont été déclassifiés par une cour, un tribunal ou autre corps de surveillance, de médiation ou d'appel, doivent être divulgués de façon proactive ou rendus publiquement accessibles (par exemple, par une harmonisation avec la législation sur le archives nationales, sur l'accès à l'information ou les deux).

*Remarque : Ce Principe est sans préjudice pour la disposition concernant les autres motifs de retenue exposés dans le paragraphe 15 du Préambule.*

*Remarque : On notera les bonnes pratiques supplémentaires ci-dessous :*

- *étude régulière de l'utilisation des nouvelles technologies dans les processus de déclassification ;*
- *consultation régulière de personnes possédant une expertise professionnelle en matière de processus d'établissement des priorités de déclassification, concernant à la fois la déclassification automatique et en bloc.*

# Partie III.B : Règles relatives au traitement des demandes d'information

## Principe 18 : Devoir de considérer des demandes même lorsque les informations sont classifiées

Le fait que des informations soient classifiées n'est pas décisif dans la détermination de la réponse à donner à une demande les concernant. L'autorité publique qui détient les informations doit considérer la requête conformément à ces Principes.

## Principe 19 : Devoir de confirmer ou de nier

(a) Lors de la réception d'une demande d'informations, une autorité publique doit confirmer ou nier qu'elle possède les informations demandées.

(b) Si une juridiction autorise, dans des circonstances extraordinaires, que l'existence-même d'une information particulière soit classifiée conformément au Principe 3, alors le refus de confirmer ou nier l'existence de l'information en réponse à une demande doit s'appuyer sur la démonstration que la simple confirmation ou négation de l'existence de l'information présenterait un risque grave en lien avec une catégorie d'informations particulière qui, selon une loi ou une réglementation nationale, exige un traitement exceptionnel.

## Principe 20 : Devoir de fournir les motifs de refus par écrit

(a) Si une autorité publique décline tout ou partie d'une demande d'informations, elle doit expliquer par écrit les raisons spécifiques du refus, conformément aux Principes 3 et 9, dans les délais prescrits par la loi pour le traitement des demandes d'informations.

*Remarque : Voir le Principe 25 qui exige que le délai de réponse soit stipulé dans la loi.*

(b) L'autorité doit également fournir au demandeur suffisamment d'informations sur les agents officiels ayant autorisé la non-divulgation et sur le processus suivi – à moins que cela ne consiste également à divulguer des informations classifiées – ainsi que sur les moyens de recours, afin que la personne soit en mesure de vérifier la conformité de l'autorité à la loi.

## Principe 21 : Devoir de retrouver ou reconstruire les informations manquantes

(a) Lorsqu'une autorité publique n'est pas en mesure de localiser des informations en réponse à une demande, et que les archives contenant ces informations auraient dues être maintenues, collectées ou produites, l'autorité doit fournir des efforts raisonnables pour retrouver ou reconstruire les informations manquantes en vue d'une possible divulgation au requérant.

*Remarque : Ce Principe s'applique aux informations qui ne peuvent être localisées pour quelque raison que ce soit, par exemple parce qu'elles n'ont jamais été recueillies, parce qu'elles ont été détruites ou parce qu'elles sont intraçables.*

(b) Un représentant de l'autorité publique doit être contraint d'indiquer, sous serment et dans un délai raisonnable défini par un statut, l'ensemble des procédures entreprises pour essayer de retrouver ou de reconstruire les informations, de façon à ce que ces procédures puissent faire l'objet d'un examen judiciaire.

*Remarque : Lorsque des informations dont la conservation est exigée par la loi sont introuvables, le dossier doit être transmis à la police ou aux autorités administratives en vue d'une enquête. Les résultats de cette enquête doivent être rendus publiques.*

(c) Le devoir de retrouver ou de reconstruire les informations revêt une importance décisive (i) lorsque les informations concernent des allégations de violations graves ou systématiques des droits humains, et/ou (ii) pendant la transition vers un gouvernement de type démocratique après un régime caractérisé par de nombreuses violations des droits humains.

## Principe 22 : Devoir de divulguer des parties de documents

Les exemptions de divulgation s'appliquent uniquement aux informations spécifiques et non à l'intégralité des documents ou autres supports. Seules les informations spécifiques pour lesquelles la validité de la restriction a été démontrée (« informations exemptées ») peuvent être retenues. Lorsqu'un document contient à la fois des informations exemptées et non exemptées, les autorités publiques ont l'obligation d'extraire et de divulguer les informations non exemptées.

## Principe 23 : Devoir d'identifier les informations retenues

Une autorité publique qui détient des informations qu'elle refuse de communiquer doit identifier ces informations en étant aussi spécifique que possible. Au minimum, l'autorité doit indiquer la quantité d'informations qu'elle refuse de divulguer, en donnant par exemple une estimation du nombre de pages.

## Principe 24 : Devoir de fournir les informations sous les différentes formes disponibles

Dans la mesure du possible, les autorités publiques doivent fournir les informations sous la forme préférée par le demandeur.

*Remarque : Cela couvre par exemple l'obligation des autorités publiques à prendre des mesures appropriées pour fournir les informations aux personnes porteuses de handicaps sous des formats et des supports technologiques accessibles, dans le respect des délais et sans frais supplémentaire, conformément à la Convention des Nations Unies sur les personnes porteuses de handicaps.*

## Principe 25 : Délais de réponse aux demandes d'informations

(a) Les délais de réponse aux demandes – qui doivent englober l'examen de son contenu, une revue interne, une décision par un organisme indépendant si disponible et un examen judiciaire – doivent être établis par la loi et être aussi courts que possible.

*Remarque : Au vu des dispositions de la plupart des lois sur l'accès à l'information, on considère que la bonne pratique consiste à prescrire vingt jours ouvrés ou moins comme délai de réponse substantielle. Lorsque les délais de traitement des demandes ne sont pas prescrits par la loi, ils ne doivent pas dépasser 30 jours pour une demande ordinaire. La loi peut prévoir des délais différents afin de tenir compte des différents volumes et niveaux de complexité et de sensibilité des documents.*

(b) Des délais raccourcis doivent être appliqués lorsqu'il est prouvé que les informations sont requises avec urgence, par exemple lorsque les informations sont nécessaires pour protéger la vie ou la liberté d'une personne.

## Principe 26 : Droit de faire examiner la décision de retenue des informations

(a) Un requérant a le droit de demander qu'un refus de divulgation d'informations ou un autre aspect de sa demande soit examiné rapidement et à faible coût par une autorité indépendante.

*Remarque : Un refus peut se manifester sous la forme d'un refus implicite ou silencieux. Les aspects pouvant faire l'objet d'un examen par une autorité indépendante incluent les frais, les délais et le format des informations.*

(b) L'autorité indépendante doit avoir la compétence et les ressources nécessaires pour assurer un examen effectif, ce qui inclut un accès complet à toutes les informations pertinentes, y compris celles qui sont classifiées.

(c) Une personne doit pouvoir obtenir un examen indépendant et effectif de tous les aspects pertinents par un tribunal compétent.

(d) Lorsqu'une cour prononce un jugement selon lequel la retenue de certaines informations est fondée, elle doit rendre publiques les raisons factuelle et son analyse légale par écrit, excepté en cas de circonstances extraordinaires, et conformément au Principe 3.

# Partie IV : Aspects judiciaires de la sécurité nationale et du droit à l'information

## Principe 27 : Principe général de surveillance judiciaire

(a) L'invocation de la sécurité nationale ne peut servir à fragiliser le droit fondamental à un procès équitable par une cour compétente, indépendante et impartiale établie par la loi.

(b) Lorsqu'une autorité publique cherche à retenir des informations au motif de la sécurité nationale lors d'une procédure judiciaire, un tribunal doit avoir le pouvoir d'examiner les informations afin de déterminer si elles doivent ou non être maintenues secrètes. Un tribunal ne doit pas rejeter une contestation du secret sans examiner les informations.

*Remarque : Conformément au Principe 4(d), le tribunal ne doit pas s'appuyer sur des résumés ou des affidavits affirmant simplement la nécessité du secret sans fournir de preuves à l'appui de cette affirmation.*

(c) Le tribunal doit veiller à ce qu'une personne demandant un accès puisse, dans la mesure du possible, connaître et contester les arguments avancés par le gouvernement pour retenir les informations.

(d) Un tribunal doit conclure à la légalité et la légitimité de l'allégation d'une autorité publique, et il doit contraindre à la divulgation ou ordonner un dédommagement

approprié en cas de divulgation partielle ou de non-divulgation, et cela inclut l'annulation des frais de procédure.

(e) Le tribunal doit évaluer indépendamment si l'autorité publique a invoqué des raisons valables de non-divulgation ; la classification ne doit pas être considérée comme argument définitif contre la divulgation des informations. De la même façon, le tribunal doit évaluer la nature des dommages allégués par l'autorité publique, leur probabilité et l'intérêt publique de la divulgation, en accord avec les normes définies dans le Principe 3.

## Principe 28 : Accès du public aux procédures judiciaires

(a) L'invocation de la sécurité nationale ne doit pas servir à fragiliser le droit fondamental du public à accéder à des procédures judiciaires.

(b) Les jugements de cour – qui exposent l'ensemble des ordres de la cour, les conclusions essentielles, les preuves et l'argumentaire légal – doivent être rendus publics, excepté lorsque l'intérêt d'enfants de moins de dix-huit ans impose un autre traitement.

*Remarques : Le droit international n'autorise aucune dérogation pour raison de sécurité nationale à l'obligation de prononcer les jugements publiquement.*

*Les comptes-rendus des procès de tribunaux pour enfants ne doivent pas être rendus publics. Les comptes-rendus d'autres procédures judiciaires impliquant des enfants doivent généralement dissimuler le nom des enfants de moins de dix-huit ans et toute autre information pouvant permettre de les identifier.*

(c) Le droit du public d'accéder à la justice doit inclure un accès public rapide (i) à l'argumentaire judiciaire, (ii) aux informations concernant l'existence et l'avancement des affaires, (iii) aux arguments écrits soumis à la cour, (iv) aux auditions et aux procès, et (v) aux preuves formant la base d'une condamnation, à moins qu'une dérogation ne soit justifiée conformément aux présents Principes.

*Remarque : Le droit international concernant les critères de procès équitable permettent aux tribunaux d'exclure tout ou parti du public d'une audition pour des raisons de sécurité nationale au sein d'une société démocratique, ainsi que pour des raisons morales ou*

*d'ordre public, dans l'intérêt des vies privées des parties, ou pour éviter tout préjudice aux intérêts de la justice, à condition que ces restrictions soient, dans tous les cas, nécessaires et proportionnées.*

(d) Le public doit avoir la possibilité de contester toute allégation faite par l'autorité publique selon laquelle une restriction de l'accès du public aux procédures judiciaires est rendue strictement nécessaire par des raisons de sécurité nationale.

(e) Lorsqu'une cour prononce un jugement selon lequel une restriction à l'accès libre aux procédures judiciaires est fondée, elle doit rendre publiques les raisons factuelle et son analyse légale par écrit, excepté en cas de circonstances extraordinaires, conformément au Principe 3.

*Remarques : Ce Principe n'a pas pour intention de modifier le droit existant d'un état concernant les procédures préliminaires auxquelles le public n'a généralement pas accès. Il s'applique uniquement lorsque le processus judiciaire autoriserait normalement l'accès du public et que la tentative de refus d'accès s'appuie sur l'invocation de la sécurité nationale.*

*Le droit du public à accéder aux procédures et au matériel judiciaire dérive de l'importance de l'accès pour la promotion (i) de l'équité et de l'impartialité réelles et perçues des procédures judiciaires, (ii) de la conduite appropriée et plus honnête des parties et (iii) de la pertinence accrue du commentaire public.*

## Principe 29 : Accès des parties à l'information dans le cadre d'une procédure pénale

(a) La cour ne peut interdire à un accusé d'assister à son procès pour des raisons de sécurité nationale.

(b) En aucun cas une condamnation ou une privation de liberté ne peut être basée sur des preuves que l'accusé n'a pas eu l'opportunité d'examiner et de réfuter.

(c) Dans l'intérêt de la justice, une autorité publique doit divulguer à l'accusé et à son avocat les charges qui pèsent contre lui et toutes les informations nécessaires pour assurer un procès équitable, que les informations soient ou non classifiées, conformément aux Principes 3 à 6, 10, 27 et 28, en tenant compte de l'intérêt public.

(d) Lorsque l'autorité publique refuse de divulguer des informations nécessaires à la tenue d'un procès équitable, la cour doit suspendre ou lever les charges.

*Remarque : Les autorités publiques ne peuvent pas utiliser des informations à leur avantage si elles en allèguent le secret, bien qu'elles puissent décider de maintenir les informations secrètes et d'en subir les conséquences.*

*Remarque : Les Principes 29 et 30 sont inclus dans ces Principes relatifs à l'accès du public à l'information, dans la mesure où l'examen judiciaire et les divulgations connexes faites dans le contexte d'une surveillance judiciaire sont souvent d'importants moyens de divulgation publique d'informations.*

## Principe 30 : Accès des parties à l'information dans le cadre d'une procédure civile

(a) Toutes les allégations de rétention d'informations par une autorité publique dans le cadre d'une procédure civile doivent être examinées conformément aux Principes 3 à 6, 10, 27 et 28, en tenant compte de l'intérêt public.

(b) Les victimes de violations des droits humains ont droit à des réparations effectives, qui incluent la divulgation publique des abus subis. Les autorités publiques ne doivent pas retenir d'informations liées à leurs allégations d'une façon qui contredise ce droit.

(c) Le public a également droit aux informations concernant les violations graves des droits humains et du droit humanitaire international.

# Partie V : Organismes supervisant le secteur de la sécurité

## Principe 31 : Établissement des organismes indépendants de surveillance

S'ils ne l'ont pas déjà fait, les états doivent mettre en place des organismes de surveillance chargés de superviser les entités du secteur de la sécurité, leurs opérations, leurs réglementations, leurs politiques, leurs finances et leur administration. Ces organismes de surveillance doivent être indépendants des institutions qu'ils sont chargés de superviser sur les plans institutionnel, opérationnel et financier.

## Principe 32 : Accès sans restrictions aux informations nécessaires à l'exécution d'un mandat

(a) Les organismes indépendants de surveillance doivent bénéficier d'un accès légalement garanti à toutes les informations nécessaires à l'exécution de leur mandat. Il ne doit y avoir aucune restriction à cet accès, quel que soit le niveau de classification ou de confidentialité des informations, dès lors que les exigences raisonnables d'accès de sécurité sont satisfaites.

(b) Les informations auxquelles les organismes de surveillance doivent avoir accès incluent, entre autres :

(i) l'ensemble des documents, technologies et systèmes en possession des autorités du secteur de la sécurité, quels qu'en soient la forme ou le support, et qu'ils aient ou non été créés par cette autorité ;

(ii) les locaux, objets et installations physiques ;

(iii) les informations détenues par les personnes que les superviseurs considèrent pertinentes pour l'exécution de leur mandat.

(c) Les obligations du personnel public à maintenir le secret ou la confidentialité de certaines informations ne doit pas les empêcher de fournir ces informations aux institutions de surveillance. La communication de ces informations ne doit pas être considérée comme une infraction aux lois ou aux contrats imposant ces obligations.

## Principe 33 : Pouvoirs, ressources et procédures nécessaires pour assurer l'accès à l'information

(a) Les organismes indépendants de surveillance doivent disposer de pouvoirs légaux adéquats leur permettant de consulter et d'interpréter toutes les informations pertinentes qu'ils estiment nécessaires à l'exercice de leur mandat.

(i) Au minimum, ces pouvoirs doivent inclure le droit d'interroger les membres actuels et précédents de la branche exécutive des autorités publiques, ainsi que leurs employés et leurs sous-traitants, de demander et examiner les registres utiles et d'inspecter les locaux et installations physiques.

(ii) Les organismes indépendants de surveillance doivent également avoir le pouvoir d'assignation à l'égard des personnes et des registres, et celui de recevoir des témoignages sous serment ou déclaration sur l'honneur des personnes considérées comme étant en possession d'informations pertinentes pour l'exercice de leur mandat, avec la pleine coopération des agences de maintien de la loi si les circonstances l'exigent.

(b) Les organismes indépendants de surveillance doivent, dans le traitement des informations et des témoignages, tenir compte, entre autres, des lois en vigueur sur la vie privée ainsi que des protections contre l'auto-incrimination et des autres exigences de procédure prévues par la loi.

(c) Les organismes indépendants de surveillance doivent avoir accès aux ressources financières, technologiques et humaines nécessaires à l'identification, la consultation et l'analyse des informations utiles à l'exercice de leurs fonctions.

(d) La loi doit exiger des institutions du secteur de la sécurité qu'elles apportent aux organismes indépendants de surveillance la coopération qu'ils demandent pour consulter et interpréter les informations nécessaires à l'exercice de leurs fonctions.

(e) La loi doit exiger des institutions du secteur de la sécurité qu'elles communiquent aux organismes indépendants de surveillance, de leur propre initiative et sans délai inutile, les catégories d'informations que les superviseurs considèrent nécessaires à la réalisation de leur mandat. Ces informations doivent inclure, entre autres, les possibles violations de la loi et des droits humains.

## Principe 34 : Transparence des organismes indépendants de surveillance

### A. Conditions d'application des lois sur l'accès à l'information

Les lois régissant l'exercice du droit du public à accéder aux informations détenues par les autorités publiques doivent s'appliquer aux organismes de surveillance du secteur de la sécurité.

### B. Rapports

(1) La loi doit exiger les organismes indépendants de surveillance à produire des rapports périodiquement, et les faires disponibles au public. Ces rapports doivent inclure, au minimum, des informations sur l'organisme, y compris son mandat, ses membres, son budget, et ses activités générales.

*Remarque : Ces rapports doivent également inclure des informations sur le mandat, la structure, le budget et les activités générales de toute institution du secteur de la sécurité qui ne rend pas ces informations publiques de sa propre initiative.*

(2) Les organismes indépendants de supervision doivent également fournir des versions publiques de leurs rapports faisant suite à des études et des enquêtes thématiques ou spécifiques, et ils doivent produire autant d'informations que possible sur les sujets d'intérêt public, notamment ceux qui sont énumérés dans le Principe 10.

(3) Dans leurs rapports publics, les organismes indépendants de surveillance doivent respecter le droit des individus concernés, y compris la protection de leur vie privée.

(4) Les organismes indépendants de supervision doivent donner aux institutions soumises à leur supervision l'opportunité d'examiner, dans des délais raisonnables, tous les rapports destinés à être rendus publics afin de leur permettre de signaler toute inquiétude concernant l'inclusion d'informations susceptibles d'être classifiées. La décision finale concernant les informations à publier revient à l'organisme de supervision.

### C. Portée et accessibilité

(1) Le fondement légal des organismes de surveillance, de leurs mandats et de leurs pouvoirs doit être disponible publiquement et facilement accessible.

(2) Les organismes indépendants de supervision doivent mettre en place des mécanismes et des facilités à destination des personnes illettrées, parlant une langue minoritaire ou porteuse d'un handicap visuel ou auditif, afin qu'elles puissent accéder aux informations relatives à leurs travaux.

(3) Les organismes indépendants de surveillance doivent proposer un choix de mécanismes librement accessibles permettant aux membres du public, y compris aux personnes résidant dans des régions isolées, d'entrer en contact avec eux et, dans le cas des organismes chargés de traiter des plaintes, de déposer une plainte ou de signaler un problème.

(4) Les organismes indépendants de surveillance doivent disposer de mécanismes capables de préserver efficacement la confidentialité des plaintes et l'anonymat des plaignants.

## Principe 35 : Mesures de protection des informations traitées par les organismes de surveillance du secteur de la sécurité

(a) La loi doit exiger des organismes indépendants de surveillance qu'ils mettent en place toutes les mesures nécessaires pour protéger les informations en leur possession.

(b) Les législatures doivent avoir le pouvoir de décider si (i) les membres des comités législatifs de supervision et (ii) les dirigeants et membres des organismes indépendants de surveillance non législatifs doivent être soumis à des contrôles de sécurité avant leur nomination.

(c) Lorsqu'un contrôle de sécurité est requis, il doit être effectué (i) dans de brefs délais, (ii) conformément aux principes établis, (iii) indépendamment de tout parti-pris ou motivation politique, et (iv) autant que possible par une institution qui n'est pas soumise à la supervision de l'organisme dont les membres sont contrôlés.

(d) Dans la limite des Principes des Parties VI et VII, les membres du personnel des organismes indépendants de surveillance qui divulguent des informations classifiées ou des contenus confidentiels en dehors des mécanismes ordinaires de rapport de l'organisme, doivent faire l'objet de poursuites administratives, civiles ou criminelles appropriées.

## Principe 36 : Autorité de la législature à rendre des informations publiques

La législature doit avoir le pouvoir de divulguer toute information au public, y compris les informations que le pouvoir exécutif prétend avoir le droit de retenir pour des raisons de sécurité nationale, si elle considère approprié de le faire conformément à des procédures qu'elle doit établir.

# Partie VI : Divulgation d'intérêt public par le personnel public

## Principe 37 : Catégories de méfaits

La divulgation d'informations par le personnel public, quelle qu'en soit la classification, mettant en évidence des méfaits entrant dans l'une des catégories suivantes doit être considérée comme une « divulgation protégée » si elle satisfait les conditions exposées dans les Principes 38 à 40. Une divulgation protégée peut être en rapport avec des méfaits s'étant produits, se produisant actuellement ou susceptibles de se produire.

(a) crimes;

(b) violations des droits humains;

(c) violations du droit humanitaire international;

(d) corruption;

(e) menaces pour la santé et la sécurité du public ;

(f) danger pour l'environnement ;

(g) abus de pouvoir à un office public ;

(h) erreur judiciaire ;

(i) mauvaise gestion ou gaspillage des ressources ;

(j) représailles suite à la divulgation de l'une des catégories de méfaits ci-dessus ;

(k) dissimulation délibérée d'un cas entrant dans l'une des catégories ci-dessus.

## Principe 38 : Raisons, motifs et preuves concernant la divulgation d'informations mettant des méfaits en évidence

(a) Comme défini dans le Principe 41, la loi doit protéger des représailles les personnels publics qui divulguent des informations mettant des méfaits en évidence, que lesdites informations soient classifiées, confidentielles ou non, dès lors que, au moment de la divulgation :

(i) l'auteur de la divulgation a des motifs raisonnables de croire que les informations divulguées tendent à mettre en évidence des méfaits qui entrent dans l'une des catégories définies dans le Principe 37 ;

(ii) la divulgation est conforme aux conditions définies dans les Principes 38 à 40.

(b) La motivation de la divulgation protégée n'est pas un critère, excepté si la divulgation s'avère délibérément fausse.

(c) L'auteur d'une divulgation protégée ne doit pas être contraint de fournir des données probantes ou de porter la responsabilité de la preuve en relation avec la divulgation.

## Principe 39 : Procédures de divulgation protégée et de réponse, en interne ou auprès d'un organisme de surveillance

### A. Divulgations internes

La loi doit exiger des autorités publiques qu'elles établissent des procédures internes et désignent des personnes chargées de recevoir les divulgations protégées.

### B. Divulgations auprès d'organismes indépendants de surveillance

(1) Les états doivent également établir ou identifier des organismes indépendants chargés de recevoir les divulgations protégées et d'enquêter à leur sujet. Ces organismes

doivent être indépendant, sur les plans institutionnel et opérationnel, du secteur de la sécurité et des autres autorités desquelles peuvent provenir des divulgations, ce qui inclut le pouvoir exécutif.

(2) Le personnel public doit être autorisé à procéder à des divulgations protégées auprès d'organismes indépendants de surveillance ou d'un autre organisme ayant autorité pour procéder à une enquête, et ce sans avoir d'abord à le faire en interne.

(3) La loi doit garantir aux organismes indépendants de surveillance l'accès à toutes les informations utiles et leur confier les pouvoirs d'enquête nécessaires pour appuyer cet accès. Ces pouvoirs doivent inclure le pouvoir d'assignation et le pouvoir de demander un témoignage sous serment ou déclaration sur l'honneur.

## C. Obligations des unités internes et des organismes indépendants de surveillance recevant des divulgations

Si une personne procède à une divulgation protégée telle que définie dans le Principe 37, à l'interne ou auprès d'un organisme indépendant de surveillance, l'entité dépositaire est dans l'obligation de :

(1) faire une enquête sur les allégations de méfaits et prendre des mesures rapides en vue de résoudre les problèmes dans un délai spécifié par la loi ou, après consultation de l'auteur de la divulgation, la porter à la connaissance d'un organisme ayant l'autorité et la compétence pour procéder à l'enquête ;

(2) protéger l'identité du personnel public qui cherche à faire une déposition confidentielle ; les dépositions confidentielles doivent être considérées pour leur contenu ;

(3) protéger les informations divulguées et le fait qu'une divulgation a été faite, excepté dans le cas où la divulgation des informations est nécessaire pour remédier au méfait ;

(4) informer l'auteur de la divulgation de l'avancement et des conclusions de l'enquête et, dans la mesure du possible, des mesures prises ou des recommandations faites.

## Principe 40 : Protection des divulgations publiques

Comme défini dans le Principe 41, la loi doit protéger des représailles les divulgations publiques d'informations concernant des méfaits tels que définis dans le Principe 37, si la divulgation répond aux critères suivants :

(a) (1) La personne a procédé à une divulgation identique ou très similaire auprès d'une unité interne et/ou d'un organisme indépendant de surveillance et :

(i) l'organisme auprès de qui la divulgation a été faite a refusé d'enquêter sur la divulgation de façon appropriée et conforme aux normes internationales en vigueur, ou n'y est pas parvenu ; ou

(ii) la personne n'a pas reçu de résultats raisonnables et appropriés dans un délai raisonnable et défini par la loi.

OU

(2) La personne a des motifs raisonnables de penser qu'il existe un risque significatif qu'une divulgation interne et/ou auprès d'un organisme indépendant de surveillance entraîne la destruction ou la dissimulation des preuves, des interférences avec des témoins ou des représailles à l'encontre de la personne ou d'un tiers ;

OU

(3) Il n'existe pas d'unité interne ou d'organisme indépendant de surveillance susceptible de recueillir la divulgation ;

OU

(4) La divulgation est liée à un acte ou une omission représentant une menace grave et imminente pour la vie, la santé et la sécurité de personnes, ou pour l'environnement.

ET

(b) L'auteur de la divulgation n'a divulgué que les informations raisonnablement nécessaires pour mettre le méfait en évidence ;

*Remarque : Si, au cours de la divulgation d'informations mettant un méfait en évidence, une personne divulgue également des documents qui ne sont pas nécessaires pour en prouver l'existence, la personne doit néanmoins être protégée de toutes représailles à moins*

*que les dommages liés à la divulgation ne soient plus important que l'intérêt public de la divulgation.*

ET

(c) L'auteur de la divulgation a des motifs raisonnables de penser que l'intérêt public de la divulgation des informations est supérieur aux dommages qu'elle pourrait causer au public.

*Remarque : Le concept de « motifs raisonnables de penser » est évalué à la fois objectivement et subjectivement. La personne doit réellement avoir cette conviction (critère subjectif) et il doit être raisonnable pour elle d'avoir pensé cela (critère objectif). En cas de contestation, la personne peut être amenée à défendre le caractère raisonnable de sa conviction et, en dernier recours, il revient à un tribunal indépendant de déterminer si ce critère est satisfait et permet donc de considérer la divulgation comme protégée.*

## Principe 41 : Protection contre les mesures de représailles après la divulgation d'informations mettant des méfaits en évidence

### A. Immunité civile et pénale en cas de divulgation protégée

Conformément aux Principes 37 à 40, l'auteur d'une divulgation ne doit pas faire l'objet de :

(1) Poursuites pénales, ce qui inclut, entre autres, les poursuites pour la divulgation d'informations classifiées ou autrement confidentielles ;

(2) Poursuites civiles liées à la divulgation d'informations classifiées ou autrement confidentielles, ce qui inclut, entre autres, les tentatives de réclamations de dommages et les poursuites pour diffamation.

### B. Interdiction des autres formes de représailles

(1) La loi doit interdire toutes représailles à l'encontre d'une personne ayant fait, soupçonnée d'avoir fait, ou susceptible de faire une divulgation entrant dans le cadre des Principes 37 à 40.

(2) Les formes interdites de représailles incluent, entre autres :

(a) Les mesures ou sanctions administratives telles que, entre autres : courrier de blâme, enquête en représailles, rétrogradation, mutation, changement de fonctions, refus de promotion, licenciement, mesures susceptibles de ou visant à nuire à la réputation de la personne, ou suspension ou révocation d'une autorisation de sécurité ;

(b) Les agressions et le harcèlement physiques ou psychologiques ; ou

(c) La menace du recours à l'une des mesures ci-dessus.

(3) Les mesures prises à l'encontre de personnes autres que l'auteur de la divulgation peuvent, dans certaines circonstances, constituer des représailles interdites.

## C. Enquête en cas de représailles par un organisme indépendant de surveillance et les autorités judiciaires

(1) Toute personne doit avoir le droit de signaler à un organisme indépendant de supervision et/ou à une autorité judiciaire toute mesure ou menace de représailles en lien avec des divulgations protégées.

(2) Les organismes indépendants de surveillance doivent être contraints à enquêter sur les signalements et les menaces de représailles. Ces organismes doivent également avoir la possibilité d'initier des enquêtes en l'absence de signalement de représailles.

(3) Les organismes indépendants de supervision doivent disposer des pouvoirs et des ressources nécessaires pour procéder à une enquête effective suite à toute allégation de représailles, y compris le pouvoir d'assigner des personnes et des documents, et de recueillir des témoignages sous serment ou déclaration sur l'honneur.

(4) Les organismes indépendants de surveillance doivent faire tout ce qui est en leur pouvoir pour veiller à ce que les procédures en lien avec des allégations de représailles soient équitables et conformes aux normes de procédure.

(5) Les organismes indépendants de surveillance doivent avoir le pouvoir d'exiger que l'autorité publique concernée prenne des mesures de remédiation ou de rétablissement telles que, entre autres, la réintégration, la réaffectation et/ou le remboursement des frais juridiques, des autres coûts raisonnables, des arriérés de salaire

et d'avantages, des frais de déplacement et/ou le versement d'indemnités compensatoires.

(6) Les organismes indépendants de surveillance doivent également avoir le pouvoir d'empêcher une autorité publique de prendre des mesures de représailles.

(7) Ces organismes doivent procéder à l'enquête sur le signalement de représailles dans des délais raisonnables et définis par la loi.

(8) Ils doivent informer les personnes concernées au minimum de la fin de l'enquête et, dans la mesure du possible, des mesures prises ou des recommandations faites.

(9) Les personnes peuvent également faire appel, auprès d'une autorité judiciaire, de la décision de l'organisme indépendant de surveillance si celui-ci a conclu que es mesures ayant fait suite à la divulgation ne constituaient pas des représailles, ainsi que des mesures de remédiation ou de rétablissement décidées par l'organisme de surveillance.

## D. Responsabilité de la preuve

Si une autorité publique prend des mesures à l'encontre d'une personne, c'est l'autorité qui doit apporter la preuve que les mesures n'avaient pas de lien avec la divulgation.

## E. Non-renonciation aux droits et recours

Les droits et recours prévus par les Principes 37 à 40 ne peuvent être annulés ou limités par aucun accord, aucune politique, aucune forme ni condition d'emploi, ce qui couvre également les accords d'arbitrage avant conflit. Toute tentative d'annulation ou de limitation de ces droits et recours doit être considérée comme nulle.

## Principe 42 : Encourager et faciliter les divulgations protégées

Les états doivent encourager les membres du personnel public à procéder à des divulgations protégées. Afin de faciliter ces divulgations, les états doivent exiger de toutes les autorités publiques qu'elles produisent des directives donnant effet aux principes 37 à 42.

*Remarque : Ces directives doivent fournir, au minimum : (1) des conseils concernant les droits et/ou les responsabilités associés à la divulgation des méfaits ; (2) les types d'informations qui doivent ou peuvent être divulguées ; (3) les procédures requises pour procéder à ces divulgations ; et (4) les protections prévues par la loi.*

## Principe 43 : Défense de l'intérêt public pour le personnel public

(a) À chaque fois que le personnel public peut faire l'objet de poursuites pénales ou civiles ou de sanctions administratives en lien avec la divulgation d'informations non protégées par ces Principes, la loi doit prévoir la défense de l'intérêt public si l'intérêt public de la divulgation des informations en question est supérieur à l'intérêt public de leur secret.

*Remarque : Ce Principe s'applique à toutes les divulgations d'informations qui ne sont pas déjà protégées, soit parce que les informations n'entrent pas dans l'une des catégories décrites dans le Principe 37, soit par ce que la divulgation contient des informations qui entrent dans l'une des catégories décrites dans le Principe 37 mais n'a pas été faite conformément aux procédures décrites dans les Principes 38 à 40.*

(b) Pour décider si l'intérêt public de la divulgation est supérieur à l'intérêt public du secret, les autorités de procuration et judiciaires doivent examiner :

(i) si l'étendue de la divulgation était raisonnablement nécessaire pour divulguer les informations d'intérêt public ;

(ii) la portée et la probabilité des dommages pour l'intérêt public entraînés par la divulgation ;

(iii) si la personne avait des motifs raisonnables de croire que la divulgation était d'intérêt public ;

(iv) si la personne a tenté de procéder à une divulgation protégée par le biais de procédures internes et/ou auprès d'un organisme indépendant de surveillance et/ou au public, en conformité avec les procédures décrites dans les Principes 38 à 40 ;

(v) l'existence de circonstances impératives justifiant la divulgation.

*Remarque : Toute loi prévoyant des sanctions pénales pour la divulgation non autorisée d'informations doit être conforme au Principe 46(b). Ce Principe n'a pas pour intention de limiter les droits de liberté d'expression déjà à disposition du personnel public ni de toute autre protection accordée par les Principes 37 à 42 et 46.*

# Partie VII : Limites aux mesures visant à sanctionner ou restreindre la divulgation d'informations au public

## Principe 44 : Protection contre les sanctions pesant sur les divulgations raisonnables faites de bonne foi par des responsables de l'information

Les personnes chargées de répondre aux demandes d'informations émises par le public ne doivent pas être sanctionnées pour avoir communiqué des informations qu'elles considéraient, raisonnablement et en toute bonne foi, pouvoir divulguer conformément à la loi.

## Principe 45 : Sanctions pour la destruction ou le refus de divulguer des informations

(a) Le personnel public doit être exposé à des sanctions pour avoir détruit ou altéré volontairement des informations dans l'intention d'empêcher le public d'y accéder.

(b) Si un tribunal ou un organisme indépendant a demandé la divulgation de certaines informations, et que les informations ne sont pas divulguées dans un délai

raisonnable, l'agent et/ou l'autorité publique responsables de la non-divulgation doivent être exposés aux sanctions appropriées, sauf appel conforme aux procédures décrites par la loi.

## Principe 46 : Limites aux sanctions pénales pour la divulgation d'informations par le personnel public

(a) La divulgation d'informations par le personnel public, même si elle n'est pas protégée par la Partie IV, ne doit pas être exposée à des sanctions pénales, bien qu'elle puisse donner lieu à des sanctions administratives telles que la pertes d'autorisations de sécurité voire un licenciement.

(b) Si la loi prévoit néanmoins des sanctions pénales pour la divulgation non autorisée d'informations au public ou bien à certains individus dans l'intention de rendre les informations publiques, les conditions suivantes doivent s'appliquer :

(i) Les sanctions pénales ne doivent s'appliquer qu'à la divulgation de catégories étroites d'informations, clairement définies dans la loi ;

*Remarque : Si le droit national prévoit des catégories d'information dont la divulgation pourrait faire l'objet de sanctions pénales, elles doivent être similaires aux catégories suivantes en termes de spécificité et d'impact sur la sécurité nationale : données technologiques sur les armes nucléaires ; sources, codes et méthodes de renseignement ; codes diplomatiques ; identité d'agents en couverture ; propriété intellectuelle dont l'état est propriétaire et dont la connaissance pourrait nuire à la sécurité nationale.*

(ii) La divulgation doit présenter un risque réel et identifiable de dommage significatif ;

(iii) Toute sanction pénale telle que définie dans la loi et appliquée, doit être proportionnelle au dommage causé ;

(iv) La personne doit être en mesure d'invoquer la défense de l'intérêt public, comme souligné dans le Principe 43.

## Principe 47 : Protection contre les sanctions pour la possession et la diffusion d'informations classifiées par les personnes qui ne sont pas membres du personnel public

(a) Une personne qui n'est pas fonctionnaire ne peut être sanctionnée pour la réception, la possession ou la divulgation au public d'informations classifiées.

(b) Une personne qui n'est pas fonctionnaire ne peut être accusée de conspiration ou d'autre crime pour avoir recherché et obtenu des informations.

*Remarque : Ce Principe a pour intention d'éviter les poursuites pénales pour l'acquisition ou la reproduction des informations. Toutefois, ce Principe n'a pas pour intention d'empêcher la poursuite d'une personne pour d'autres crimes tels que le vol pour effraction ou le chantage, commis lors de la recherche ou de l'obtention des informations.*

*Remarque : Les divulgations par des tiers jouent un rôle important de mesure corrective face à un excès généralisé de classification.*

## Principe 48 : Protection des sources

Toute personne qui n'est pas fonctionnaire ne peut être contrainte à révéler une source confidentielle ou des documents non publiés lors d'une enquête concernant la divulgation non autorisée d'informations à la presse ou au public.

*Remarque : Ce Principe fait uniquement référence aux enquêtes concernant la divulgation non autorisée d'informations et non à celles qui concernent d'autres crimes.*

## Principe 49 : Restrictions préalables

(a) Les restrictions préalables à la publication dans l'intérêt de la protection de la sécurité nationale doivent être interdites.

*Remarque : Les restrictions préalables sont des décisions de justice ou d'autres agences de l'état consistant à interdire la publication de contenus spécifiques se trouvant déjà en la possession d'une personne qui n'est pas fonctionnaire.*

(b) Si des informations ont été rendues publiques par quelque moyen que ce soit, légal ou non, tout effort visant à empêcher toute autre publication de ces informations sous la forme qui est déjà dans le domaine publique est présumé non valide.

*Remarque : « Rendues publiques » signifie que les informations ont été assez largement diffusées pour qu'aucune mesure pratique ne permette de préserver le secret de ces informations.*

# Partie VIII : Principe de conclusion

## Principe 50 : Relation de ces Principes avec les autres normes

Rien dans ces Principes ne doit être interprété comme une restriction ou une limitation d'aucun droit à l'information reconnu par les lois et normes internationales, régionales ou nationales, ni d'aucune disposition de lois nationales ou internationales offrant une meilleure protection à la divulgation d'informations par le personnel public ou d'autres individus.

# Annexe : Organisations partenaires

Les 22 organisations suivantes ont apporté une contribution significative à la rédaction des Principes et sont déterminées à travailler à la diffusion, la publication et à la mise en œuvre de ces Principes.[2] Après le nom de chaque organisation figurent celui de la ville où se trouve son siège et le pays ou la région où elle exerce. Les organisations qui œuvrent activement dans trois régions ou plus sont identifiées comme « internationales ».

- Africa Freedom of Information Centre (Kampala / Africa)
- African Policing Civilian Oversight Forum (APCOF) (Cape Town / Afrique)
- Alianza Regional por la Libre Expresión e Información (Amériques)
- Amnesty International (Londres / international)
- Article 19, Campagne mondiale en faveur de la liberté d'expression (Londres / international)
- Forum asiatique pour les droits humains et le développement (Forum Asia) (Bangkok / Asie)
- Center for National Security Studies (Washington DC / États-Unis)
- Université d'Europe centrale (Budapest / Europe)
- Centre for Applied Legal Studies (CALS), Wits University (Johannesburg/Afrique du Sud)

2. De plus, Aidan Wills et Benjamin Buckland, du Centre de Genève pour le Contrôle démocratique des forces armées (DCAF), sans aucune affiliation avec les organisations partenaires, ont également apporté des contributions significatives à la Partie V sur les Organismes de surveillance et à la Partie VI sur les Divulgations d'intérêt public, ainsi qu'aux Principes dans leur ensemble

- Centre for European Constitutionalization and Security (CECS), Université de Copenhague (Copenhague / Europe)
- Centre for Human Rights, Université de Pretoria (Pretoria / Afrique)
- Centre for Law and Democracy (Halifax / international)
- Centre for Peace and Development Initiatives (Islamabad / Pakistan)
- Centre for Studies on Freedom of Expression and Access to Information (CELE), École de droit de l'Université de Palerme (Buenos Aires / Argentine)
- Commonwealth Human Rights Initiative (New Delhi / Commonwealth)
- Egyptian Initiative for Personal Rights (Le Caire / Égypte)
- Institute for Defence, Security and Peace Studies (Djakarta / Indonésie)
- Institute for Security Studies (Pretoria / Afrique)
- Commission internationale de juristes (Genève / international)
- National Security Archive (Washington DC / international)
- Open Democracy Advice Centre (Cape Town / Sud de l'Afrique)
- Open Society Justice Initiative (New York / international).

« Les Principes représentent une contribution majeure au droit d'accès à l'information et au droit à la vérité en ce qui concerne les violations des droits humains, et je crois qu'ils devraient être adoptées par le Conseil des droits de l'homme. Tous les États devraient prendre en compte ces principes lorsqu'ils interpretent leurs lois sur la sécurité nationale. »

***Frank La Rue**, Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression des Nations Unies*

« Mon bureau se félicite de la publication des Principes de Tshwane qui proposent un équilibre approprié entre la capacité de l'État à protéger la sécurité et la protection des libertés individuelles. »

***Catalina Botero**, Rapporteur spéciale pour la liberté d'expression de l'Organisation des États américains*

« Ces Principes globaux n'auraient pas pu survenir à un moment plus opportun.»

***Pansy Tlakula**, Rapporteur spécial sur la liberté d'expression et l'accès à l'information en Afrique*

« L'Assemblée adhère aux Principes globaux et demande aux autorités compétentes de l'ensemble des États membres du Conseil de l'Europe de les prendre en compte en modernisant leur législation et pratique concernant l'accès à l'information. »

*Résolution de l'Assemblée parlementaire du Conseil de l'Europe, 2 Octobre 2013*