Parliamentary Assembly
Assemblée parlementaire
https://pace.coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Doc. 13293
03 septembre 2013

La sécurité nationale et l'accès à l'information

Rapport[1]
Commission des questions juridiques et des droits de l'homme
Rapporteur: M. Arcadio DÍAZ TEJERA, Espagne, Groupe socialiste

Résumé

La commission rappelle l'importance du principe de transparence, notamment l'accès à l'information détenue par les autorités publiques, pour la démocratie et la bonne gouvernance en général, et pour la lutte contre la corruption en particulier. Elle considère les intérêts de sécurité nationale légitimes et clairement définis comme des raisons suffisantes pour retenir certaines informations. En même temps, l'accès à l'information représente une composante essentielle de la sécurité nationale, en favorisant la participation démocratique, l'élaboration de politiques solides et le droit de regard du public sur l'action gouvernementale.

La commission se félicite de l'adoption, en juin 2013, par une large assemblée d'experts d'organisations internationales et de la société civile, d'universitaires et de praticiens de la sécurité nationale, des «Principes globaux de la sécurité nationale et du droit à l'information» visant à fournir des orientations aux législateurs et aux responsables concernés dans le monde entier en vue de parvenir à un juste équilibre entre l'intérêt public en matière de sécurité nationale et en termes d'accès à l'information. Elle adhère aux «Principes globaux» et demande aux autorités compétentes de l'ensemble des Etats membres du Conseil de l'Europe de les prendre en compte en modernisant leur législation et leur pratique concernant l'accès à l'information.

La commission insiste sur un certain nombre de principes particulièrement importants, dont la nécessité d'un contrôle efficace des activités des services secrets, la protection de signalements en bonne foi d'abus par des «donneurs d'alerte» et la reconnaissance d'une «exception d'intérêt général» comme sauvegarde contre des exceptions trop larges de la règle générale de la libre accessibilité de toute information détenue par des autorités publiques. Des informations concernant la responsabilité d'agents de l'Etat ayant commis de graves violations des droits de l'homme, comme des assassinats, des disparitions forcées, des actes de torture ou des enlèvements, ne sont pas des secrets dignes d'être protégés.

1. Renvoi en commission: Doc. 12548, Renvoi 3762 du 15 avril 2011.

Sommaire **Page**

A. Projet de résolution[2]

1. L'Assemblée parlementaire rappelle l'importance du principe de transparence, notamment l'accès à l'information détenue par les autorités publiques, pour la démocratie et la bonne gouvernance en général, et pour la lutte contre la corruption en particulier.

2. Elle note avec satisfaction que le Conseil de l'Europe a été la première organisation intergouvernementale à élaborer un instrument juridique international sur l'accès à l'information, à savoir la Convention du Conseil de l'Europe sur l'accès aux documents publics (STCE n° 205), tout en rappelant son Avis 270 (2008) sur le projet de convention dans lequel l'Assemblée avait encouragé le Comité des Ministres à améliorer le texte en vue d'assurer une transparence encore plus grande. La convention doit encore obtenir quatre ratifications pour entrer en vigueur.

3. L'Assemblée considère les intérêts de sécurité nationale légitimes et clairement définis comme des raisons suffisantes pour retenir l'information détenue par les autorités publiques. En même temps, l'accès à l'information représente une composante essentielle de la sécurité nationale, en favorisant la participation démocratique, l'élaboration de politiques solides et le droit de regard du public sur l'action de l'Etat.

4. Rappelant sa Résolution 1838 (2011) sur les recours abusifs au secret d'Etat et à la sécurité nationale: obstacles au contrôle parlementaire et judiciaire des violations des droits de l'homme et sa Résolution 1675 (2009) sur la situation des droits de l'homme en Europe: la nécessité d'éradiquer l'impunité, l'Assemblée souligne la nécessité de fixer des limites raisonnables à l'invocation de la sécurité nationale comme motif de restriction de l'accès à l'information.

5. En particulier, l'Assemblée confirme sa position, exprimée au paragraphe 4 de sa Résolution 1838 (2011), selon laquelle des informations concernant la responsabilité d'agents de l'Etat ayant commis de graves violations des droits de l'homme, comme des assassinats, des disparitions forcées, des actes de torture ou des enlèvements ne sont pas des secrets dignes d'être protégés. Le «secret d'Etat» ne doit pas être invoqué pour soustraire de telles informations à un contrôle judiciaire ou parlementaire.

6. L'Assemblée se félicite de l'adoption, le 12 juin 2013, par une large assemblée d'experts d'organisations internationales et de la société civile, d'universitaires et de praticiens de la sécurité nationale, des «Principes globaux de la sécurité nationale et du droit à l'information» (ci-après «les Principes globaux»), qui sont basés sur les normes existantes et les bonnes pratiques des Etats et des institutions internationales. Les Principes globaux visent à fournir des orientations aux législateurs et aux responsables concernés dans le monde entier en vue de parvenir à un juste équilibre entre l'intérêt public en matière de sécurité nationale et en termes d'accès à l'information.

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

8. L'Assemblée souhaite insister, en particulier, sur les principes suivants:

8.1. En règle générale, l'ensemble des informations détenues par les autorités publiques doivent être librement accessibles; de plus, les entreprises, notamment les sociétés privées de services militaires ou de sécurité, ont la responsabilité de divulguer l'information sur des situations, activités ou pratiques dont il y a raisonnablement lieu de croire qu'elles ont un effet sur l'exercice des droits de l'homme.

8.2. Les exceptions à la règle de libre accès à l'information qui sont basées sur la sécurité nationale, ou d'autres intérêts publics d'égale importance, tels que la protection des relations internationales, la santé et la sûreté ou l'environnement, ou des intérêts privés, doivent être prévues par la loi, poursuivre un but légitime et être nécessaires dans une société démocratique.

8.3. Les limitations à la règle du libre accès à l'information, y compris la règle de la neutralité d'internet, doivent être interprétées de manière restrictive. La charge de prouver la légitimité de toute restriction incombe à l'autorité publique qui souhaite retenir l'information.

8.4. Les règles sur la procédure de classification et de déclassification de l'information et la désignation des personnes autorisées à exécuter cette tâche doivent être claires et publiquement accessibles. L'information peut être retenue pour des raisons liées à la sécurité nationale uniquement pendant le temps nécessaire pour protéger un intérêt légitime de sécurité nationale.

---

2. Projet de résolution adopté à l'unanimité par la commission le 24 juin 2013.

8.5. En tant que correctif par rapport aux exceptions trop générales, l'accès à l'information doit être accordé même s'il fait en principe l'objet d'une exception légitime, dès lors que l'intérêt général que commande la communication de cette information revêt une importance supérieure à la défense des intérêts qui conduisent l'administration à la tenir secrète. Cet intérêt général prime habituellement lorsque la publication de l'information en question:

8.5.1. apporte d'importants éléments de réflexion à un débat public en cours;

8.5.2. favorise la participation des citoyens au débat politique;

8.5.3. fait état de graves abus, notamment de violations des droits de l'homme, d'autres infractions pénales, d'abus de fonctions publiques et de dissimulation intentionnelle d'actes répréhensibles graves;

8.5.4. renforce l'obligation de rendre des comptes dans la gestion des affaires publiques en général et dans l'utilisation des fonds publics en particulier;

8.5.5. présente un avantage pour la santé publique ou la sécurité publique.

8.6. L'information concernant des violations graves des droits de l'homme ou du droit humanitaire ne doit en aucun cas être retenue pour des raisons de sécurité nationale.

8.7. Toute personne qui signale des abus dans l'intérêt général (donneur d'alerte) doit être protégée de tout type de représailles, dans la mesure où il ou elle a agi de bonne foi et a suivi les procédures applicables.

8.8. Les demandes d'accès à l'information doivent être traitées dans un délai raisonnable. Les décisions de refuser l'accès doivent être dûment motivées, susceptibles de recours devant un organisme indépendant et soumises en dernier ressort à un contrôle juridictionnel. Dès réception d'une demande d'information, une autorité publique doit en principe confirmer ou infirmer qu'elle détient l'information demandée.

8.9. Les instances publiques de surveillance chargées de contrôler les activités des services de sécurité doivent être indépendantes du pouvoir exécutif et disposer de compétences pertinentes, de solides pouvoirs d'investigation et du plein accès aux informations protégées.

9. L'Assemblée encourage tous les Etats membres du Conseil de l'Europe qui ne l'ont pas encore fait à signer et ratifier la Convention du Conseil de l'Europe sur l'accès aux documents publics et à la mettre en œuvre et, en temps utile, à l'améliorer dans l'esprit des Principes globaux.

B. Projet de recommandation[3]

1. L'Assemblée se réfère à sa Résolution ... (2013) sur la sécurité nationale et l'accès à l'information et invite le Comité des Ministres:

1.1. à étudier les moyens de promouvoir l'entrée en vigueur et la mise en œuvre rapide de la Convention du Conseil de l'Europe sur l'accès aux documents publics (STCE n° 205);

1.2. à revoir les politiques du Conseil de l'Europe concernant l'accès à l'information et la classification et déclassification des documents au regard de la résolution de l'Assemblée;

1.3. à encourager les Etats membres du Conseil de l'Europe à prendre en considération les «Principes globaux de la sécurité nationale et du droit à l'information», adoptés le 12 juin 2013 par une assemblée d'experts d'organisations internationales et de la société civile, d'universitaires et de praticiens de la sécurité nationale, en particulier concernant les points mis en avant dans la résolution ci-dessus mentionnée, en modernisant leur législation et leur pratique.

3. Projet de recommandation adopté à l'unanimité par la commission le 24 juin 2013.

C. Exposé des motifs, par M. Díaz Tejera, rapporteur

1. Introduction

1.1. Procédure

1. Le 22 mars 2011, l'Assemblée parlementaire a décidé de renvoyer, pour rapport, la proposition de résolution «Sécurité nationale et accès à l'information» à la commission des questions juridiques et des droits de l'homme[4]. Lors de sa réunion du 6 juin 2011, la commission m'a désigné rapporteur.

2. A l'occasion de l'audition consacrée à la liberté des médias en Europe, organisée par la sous-commission des médias en Suède le 12 septembre 2011, Mme Agnès Callamard, directrice exécutive de l'organisation non gouvernementale (ONG) Article 19, s'est adressée aux parlementaires sur la question de la sécurité nationale et de l'accès à l'information.

3. Lors de sa réunion du 6 septembre 2012, la commission a examiné une note introductive[5] présentant les éléments en jeu et les évolutions en cours en la matière.

4. A la suite de l'invitation de l'Open Society Justice Initiative (OSJI) et du Center for Advanced Security Theory (CAST) de l'université de Copenhague, j'ai assisté à une consultation d'experts consacrée à la sécurité nationale et au droit à l'information à Copenhague du 20 au 22 septembre 2012. Cette réunion portait sur les lois et pratiques des pays européens en matière de juste équilibre entre le droit à l'information du public et la nécessité occasionnelle du secret en vue de protéger les intérêts nationaux légitimes dans le domaine de la sécurité et, d'autre part, à contribuer à l'élaboration des «Principes globaux de la sécurité nationale et du droit à l'information»[6] (ci-après les «Principes globaux») qui ont été finalisés le 12 juin 2013. A Copenhague, j'ai présenté l'acquis du Conseil de l'Europe dans ce domaine, notamment les précédentes résolutions de l'Assemblée basées sur les rapports de M. Dick Marty sur la restitution et la détention secrète[7].

5. Lors de sa réunion du 11 décembre 2012, la commission a tenu un échange de vues avec trois experts:

– Mme Sandra Coliver, juriste, Liberté d'information et d'expression, à l'Open Society Justice Initiative (OSJI), qui assure la coordination du projet «Principes globaux de la sécurité nationale et du droit à l'information», New York, Etats-Unis;

– Mme Susana Sanchez Ferro, Professeur à l'Université de Madrid, Espagne;

– Lord Alexander Carlile of Berriew CBE QC, ancien contrôleur indépendant, Londres, Royaume-Uni.

M. Matthew Pollard, conseiller juridique, Amnesty International (Londres), a aussi participé à la discussion lors de la réunion de la commission.

---

4. Doc. 12548, Renvoi 3762 du 15 avril 2011.
5. Document AS/Jur (2012) 27.
6. Principes globaux de la sécurité nationale et du droit à l'information (également dénommés «Principes de Tshwane» ou «Principes globaux»), publiés le 12 juin 2013, élaborés par 17 ONG et cinq centres universitaires (Africa Freedom of Information Centre; African Policing Civilian Oversight Forum; Alianza Regional por la Libre Expresión e Información; Amnesty International; Article 19, la campagne mondiale pour la liberté d'expression; Forum asiatique pour les droits de l'homme et le développement (Forum Asia); Center for National Security Studies; Université d'Europe centrale; Centre for Applied Legal Studies, Wits University; Centre for European Constitutionalisation and Security (CECS), Université de Copenhague; Centre for Human Rights, Université de Pretoria (Tshwane); Centre for Law and Democracy; Centre for Peace and Development Initiatives; Centre for Studies on Freedom of Expression and Access to Information, Faculté de droit de l'Université de Palerme; Commonwealth Human Rights Initiative; Egyptian Initiative for Personal Rights; Institute for Defence, Security and Peace Studies; Institut d'études de sécurité; Commission internationale de juristes; National Security Archive; Open Democracy Advice Centre; et Open Society Justice Initiative); grâce à une consultation conduite par l'Open Society Justice Initiative impliquant les trois rapporteurs spéciaux chargés de la liberté d'expression des Nations Unies, l'Organisation des Etats américains (OEA) et la Commission africaine des droits de l'homme et des peuples, le Représentant de l'Organisation pour la sécurité et la coopération en Europe (OSCE) chargé de la liberté des médias, ainsi que le rapporteur spécial des Nations Unies sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste: www.right2info.org/national-security/Tshwane_Principles (en anglais).
7. Doc. 10957, rapport sur «Allégations de détentions secrètes et de transferts interétatiques illégaux de détenus concernant des Etats membres du Conseil de l'Europe», 12 juin 2006; Doc. 11302, rapport sur «Détentions secrètes et transferts illégaux de détenus impliquant des Etats membres du Conseil de l'Europe: second rapport», 11 juin 2007; et le Doc. 12714, rapport sur «Les recours abusifs au secret d'Etat et à la sécurité nationale: obstacles au contrôle parlementaire et judiciaire des violations des droits de l'homme», 16 septembre 2011.

1.2. Aperçu des principaux éléments en jeu

6. La sécurité nationale a, tout particulièrement depuis le déclenchement en 2001 de la «guerre contre le terrorisme», fréquemment été invoquée pour restreindre les libertés et justifier les abus des agents publics. Le fait que l'administration accorde au parlement, à la justice et aussi aux citoyens un accès infime aux informations secrètes crée un déséquilibre des pouvoirs en faveur de l'exécutif. Ce problème prend sa source dans une question plus vaste: l'absence d'accès aux informations détenues par l'Etat, qui est renforcée par «l'invocation systématique et arbitraire du privilège du secret d'Etat»[8].

7. L'accès à l'information revêt une importance capitale dans une société démocratique. Il est l'instrument de la jouissance des autres droits de l'homme; il offre une garantie contre les abus de pouvoir, en renforçant la transparence et l'obligation de rendre des comptes de l'administration, tout en permettant la participation effective des citoyens à une société avertie[9].

8. La protection de la sécurité d'une nation et de ses citoyens représente, bien entendu, un élément important de l'intérêt général. Pour pouvoir protéger la nation et mener à bien des opérations militaires et de renseignement, il est souvent indispensable de tenir certains types d'information hors de portée du grand public. Le conflit inévitable entre l'accès autorisé ou interdit aux informations est renforcé par l'absence de cadre juridique clair et de normes internationales, voire par leur manque de mise en œuvre effective. Le caractère excessivement étendu et flou des exceptions faites au principe de l'accès à l'information au nom de la sécurité nationale permet de dissimuler des activités illégales et restreint l'accès des victimes à la justice[10].

9. Les mécanismes de surveillance parlementaires et judiciaires sont souvent mal armés pour trouver le juste équilibre entre ces intérêts contradictoires. Cela tient au fait que ces mécanismes n'ont pas eux-mêmes accès aux informations secrètes ou classées confidentielles ou, s'agissant des mécanismes parlementaires, au fait que leur composition est d'ordinaire le reflet de la majorité parlementaire qui soutient le gouvernement au pouvoir. La plupart des atteintes aux droits de l'homme commises dans le cadre de la «guerre contre le terrorisme» ont de fait été dévoilées grâce aux informations révélées par des donneurs d'alerte et au travail d'investigation des journalistes et des ONG plutôt que par l'action des mécanismes de surveillance parlementaires ou judiciaires[11].

10. Ces donneurs d'alerte ont ainsi acquis une certaine importance, en dévoilant des informations qui présentaient un intérêt pour le public, notamment sur les atteintes aux droits de l'homme commises sous couvert de sécurité nationale et de secret d'Etat. Malheureusement, certaines de ces personnes sont aujourd'hui en détention provisoire, accusées d'espionnage[12]. Citons, pour de plus amples informations sur ce sujet majeur, l'admirable travail de notre collègue de l'Assemblée, M. Pieter Omtzigt[13]. Les Principes globaux cités auparavant couvrent également quelques orientations importantes sur la protection des donneurs d'alerte[14].

11. L'absence d'information sur d'importantes questions d'intérêt général empêche tout contrôle effectif et favorise une culture du secret et de l'impunité qui, à son tour, menace les valeurs démocratiques sur lesquelles reposent nos sociétés. Il convient par conséquent de veiller à créer un environnement favorable, qui permette à l'exécutif de respecter, de protéger et de garantir la transparence, en évitant ainsi la création d'un terrain propice aux atteintes aux droits de l'homme commises au nom de la sécurité nationale.

2. Le droit international des droits de l'homme applicable en matière d'accès à l'information

12. Diverses résolutions[15] ont reconnu à l'échelon international l'existence d'un droit de l'homme de l'accès à l'information, bien qu'il soit habituellement considéré comme un aspect du droit à la liberté d'expression[16]. Les dispositions relatives à la liberté d'expression de la Déclaration universelle des droits de l'homme et du Pacte international relatif aux droits civils et politiques (ci-après «le PIDCP») garantissent le droit individuel à rechercher et obtenir des informations, qui est une composante du droit d'accès à l'information[17]. L'observation générale N° 34 affirme que l'article 19 du PIDCP «vise un droit d'accès à l'information détenue

---

8. Doc. 12714, *op. cit.*, paragraphe 45.
9. R. Peled et Z. Rabin, *The Constitutional Right to Information*, 42 *Columbia Human Rights Law Review* 357, 2011, p. 357.
10. Principes globaux (note 6 supra), Introduction (Contexte et justification).
11. Rapport Doc. 12714, *op. cit.*, Exposé des motifs, paragraphes 2 et 50.
12. *Ibid.*, paragraphe 50; voir le cas de Bradley Manning, paragraphes 62-63 et 91 ci-après.
13. Voir Résolution 1729 (2010), Recommandation 1916 (2010), et rapport Doc. 12006 sur la «Protection des "donneurs d'alerte"», 14 septembre 2009, rapporteur: M. Pieter Omtzigt.
14. Voir ci-après, paragraphes 83-94.

par les organismes publics»[18]. La Convention européenne des droits de l'homme (STE n° 5, «la Convention») prévoit le droit de recevoir des informations en vertu de la garantie de la liberté d'expression[19], même s'il ressort difficilement de la Convention l'existence d'un droit général d'accès à l'information détenue par l'Etat. L'Organisation des Etats Américains et l'Union africaine ont récemment adopté des lois-types sur l'accès à l'information pour contribuer à l'adoption d'une législation nationale.

2.1. L'évolution à l'échelon national

13. La législation relative à la liberté d'information a connu ces dernières décennies une évolution rapide à l'échelon national et régional, avec la reconnaissance d'un droit d'accès aux informations détenues par l'Etat et aux documents publics[20]. Selon l'Open Society Justice Initiative, en juin 2013, 94 pays dans le monde avaient adopté, sous une forme ou une autre, des dispositions ou une législation sur la liberté d'information[21], tandis que 20 autres Etats étaient en passe de se doter de ce type de texte[22]. Depuis le début des années 1990, le droit à l'information a également été intégré dans un certain nombre de constitutions nationales nouvelles ou révisées[23]. Au moment de la rédaction de ce rapport, plus de 5,2 milliards de personnes dans 95 pays du monde bénéficiaient du droit d'accès à l'information au moins en droit[24]. Sur les 47 Etats membres du Conseil de l'Europe, seuls six, à savoir Andorre, Chypre, Luxembourg, Monaco, Saint-Marin et l'Espagne, ne possèdent pas encore de législation sur l'accès à l'information[25].

14. Mais la qualité de la législation nationale et de sa mise en œuvre varie considérablement d'un pays à l'autre[26]; il est donc souhaitable que les normes internationales soient précisées, notamment les exceptions au principe de l'accès à l'information au nom de la sécurité nationale.

2.2. L'évolution en Europe

2.2.1. La Convention du Conseil de l'Europe sur l'accès aux documents publics

15. Le Conseil de l'Europe a affirmé à diverses occasions l'existence d'un droit d'accès à l'information[27] et a adopté la première convention internationale sur le droit d'accès aux documents publics, la Convention du Conseil de l'Europe sur l'accès aux documents publics (STCE n° 205) en 2008[28].

16. La réalisation la plus importante de la Convention est la reconnaissance du principe selon lequel l'accès aux documents publics est la règle, et son refus l'exception[29]. La Convention donne le droit à «toute personne» d'accéder à des documents publics, quels que soient ses motifs ou intentions. Elle énonce aussi la première définition largement admise de la notion de «documents publics», qui signifie «toutes informations

---

15. Voir par exemple la résolution de l'Assemblée générale des Nations Unies A/RES/59(I), 1946; les résolutions de l'Assemblée générale de l'OEA Accès à l'information: renforcement de la démocratie, AG/RES. 1932 (XXXIII-O/03), 10 juin 2003; AG/RES. 2057 (XXXIV-O/04), 8 juin 2004; AG/RES. 2121 (XXXV-O/05), 26 mai 2005; AG/RES. 2252 (XXXVI-O/06), 6 juin 2006 GA/RES. 2288 (XXXVII-O/07), 5 juin 2007; AG/RES. 2418 (XXXVIII-O/08), 3 juin 2008; AG/RES. 2514 (XXXIX-O/09), 4 juin 2009; Déclaration de Nueva Leon, 13 janvier 2004.
16. T. Mendel, The Right to Information in Latin America: A Comparative Legal Survey, 2009, p 1.
17. Article 19 de la Déclaration universelle des droits de l'homme; article 19(2) du PIDCP.
18. Observation générale n° 34 (juillet 2011), paragraphe 18 (disponible (en anglais) sur: http://www2.ohchr.org/english/bodies/hrc/comments.htm).
19. Article 10 de la Convention.
20. J. Ackerman et I. Sandoval, The Global Explosion of Freedom of Information Laws, 58 Admin. L. Rev. 85 2006, p. 85 et suiv.
21. Open Society Justice Initiative, www.right2info.org/resources/publications/laws-1/countries-with-foi-laws_march-2013.
22. http://right2info.org/laws.
23. Peled et Rabin, *op. cit.*, p. 372 et suivantes.
24. Voir Right 2 Info, «Constitutional Provisions, Laws and Regulations», 24 octobre 2011: www.right2info.org/laws/constitutional-provisions-laws-and-regulations.
25. *Ibid*.
26. Le rapport d'Amanda Jacobsen en donne un excellent aperçu sur la base de recherches empiriques approfondies (Université de Copenhague): www.right2info.org/resources/publications/national-security-expert-papers/jacobsen_nat-sec-and-rti-in-europe.
27. Voir la Recommandation du Comité des Ministres N° (81) 9 du 25 novembre 1981 sur «L'accès à l'information détenue par les autorités publiques»; et la Déclaration sur la liberté d'expression et d'information du Comité des Ministres, adoptée le 29 avril 1982.
28. Adoptée par le Comité des Ministres le 27 novembre 2008 lors de la 1042bis réunion des Délégués des Ministres: CM/Del/Dec(2008)1042bis/1.2d/annexe2E.
29. Préambule de la convention, point 7 et articles 2 et 3.

enregistrées sous quelque forme que ce soit, rédigées ou reçues et détenues par les autorités publiques»[30] – comprenant donc aussi les documents qui ne sont pas produits par les autorités publiques qui les détiennent, et quelle que soit leur forme ou leur format (textes écrits, enregistrements vidéos ou audiovisuels, photographies, courriels, informations stockées dans des bases de données électroniques)[31].

17. Une faiblesse, selon l'approche de ce rapport, est la longue liste de limitations possibles au droit d'accès à l'information dressée à l'article 3, notamment la protection de la sécurité nationale, la défense et les relations extérieures, la sûreté publique, les missions de tutelle, l'inspection et le contrôle par l'administration, jusqu'aux intérêts commerciaux et autres intérêts économiques, et la protection de l'environnement. J'imagine difficilement dans quelle mesure la protection de l'environnement pourrait tirer un avantage du fait que des informations restent hors du domaine public – l'inverse serait normalement vrai. Ces exceptions ne sont pas définies dans la Convention. Mais la phrase introduisant la liste de l'article 3 prévoit que les limitations «sont établies précisément dans la loi, nécessaires dans une société démocratique et proportionnelles au but».

18. Cette Convention a été critiquée par plusieurs organisations de la société civile[32], par certains Etats européens et par l'Assemblée parlementaire du Conseil de l'Europe pour l'étroitesse de sa portée. L'Avis 270 (2008) de l'Assemblée adressé au Comité des Ministres[33], rédigé par M. Klaas de Vries pour le compte de notre commission, a fait le choix inhabituel de recommander au Comité des Ministres de demander au Comité directeur pour les droits de l'homme (CDDH) de rouvrir les négociations:

– pour élargir la définition des «pouvoirs publics», de manière à englober un plus large éventail d'activités des pouvoirs publics et à accroître ainsi l'étendue des informations mises à disposition;

– pour prévoir un délai de traitement des demandes;

– pour préciser et renforcer la procédure de contrôle applicable en cas de rejet d'une demande d'information.

19. Le Comité des Ministres n'a pas suivi la recommandation de l'Assemblée et le texte a été ouvert à la signature dans la version présentée à celle-ci. L'existence même de cette convention, quand bien même elle se limiterait à l'expression du plus petit dénominateur commun, constitue néanmoins un progrès pour le droit d'accès à l'information en droit international. L'objectif déclaré de la convention est l'établissement de normes communes minimales, qui devraient être acceptables pour le plus grand nombre d'Etats possible, tout en incitant chacun d'eux à s'acheminer vers le niveau de transparence atteint par les Etats les plus avancés. Il convient de noter à ce propos que plusieurs «nouvelles démocraties», dans lesquelles régnaient autrefois, du temps des régimes précédents, l'absence de transparence et l'oppression, sont désormais à l'avant-garde des pays qui disposent de la législation la plus libérale en matière d'accès aux documents publics, alors que certaines «démocraties bien établies» demeurent à la traîne[34].

20. La convention doit obtenir 10 ratifications pour entrer en vigueur. Jusqu'à présent, six pays (Bosnie-Herzégovine, Hongrie, Lituanie, Monténégro, Norvège et Suède) ont ratifiée et huit autres (Belgique, Estonie, Finlande, Géorgie, Monaco, Slovaquie et Slovénie) ont signé la convention mais ne l'ont pas encore ratifiée. Quatre ans après l'ouverture à la signature, la participation est décevante, compte tenu du fait que le texte n'a volontairement pas imposé de dispositions trop ambitieuses.

21. A mon avis, l'Assemblée devrait appeler les Etats membres qui ne l'ont pas encore fait à signer et ratifier la Convention sur l'accès aux documents publics, afin de démontrer leur engagement de principe en faveur de la transparence et de la bonne gouvernance. Dès l'entrée en vigueur de l'instrument, l'organe de suivi, le Groupe de spécialistes sur l'accès aux documents publics[35], commencera ses activités et pourra examiner les questions en suspens au cas par cas. Ce travail majeur sera engagé par les spécialistes nommés sur proposition des pays qui ont montré le plus vif intérêt pour la transparence, en ratifiant rapidement l'instrument. On peut par conséquent escompter que le Groupe de spécialistes fixe un cap progressiste, notamment sur des questions sur lesquelles l'Assemblée, dans son avis mentionné auparavant,

---

30. Article 1.2.*b* de la convention.
31. Voir Rapport explicatif, paragraphe 11.
32. Mendel, *op. cit.*, p. 13.
33. Voir aussi Doc. 11698, rapport sur le «Projet de Convention du Conseil de l'Europe sur l'accès aux documents publics», rapporteur: M. Klaas de Vries.
34. Selon une étude réalisée par l'Open Society Justice Initiative, les demandes d'information faites auprès des services administratifs obtiennent des réponses plus fréquentes et de meilleure qualité en Arménie, Bulgarie et Roumanie qu'en France et en Espagne; voir Transparency and Silence, A survey of access to information laws and practices in 14 countries, Open Society Justice Initiative, New York/Budapest, 2006, p. 12.
35. Article 11 de la convention.

a estimé le texte de la convention trop restrictif. La convention prévoit aussi un dispositif visant à faire des propositions d'amendement au texte[36], qui permettra des améliorations au regard de l'expérience pratique du Groupe de spécialistes.

22. Tout bien considéré, la façon la plus réaliste pour l'Assemblée de contribuer à un réel progrès sur ce sujet est donc, selon moi, de promouvoir vivement la ratification de la convention du Conseil de l'Europe, afin qu'elle entre en vigueur. En tant que parlementaires nationaux, nous pouvons faire pression sur nos gouvernements quant à la signature et la ratification de cet instrument et leur demander de rendre compte de la façon dont ils la mettent en œuvre. Nous devrions agir ainsi, au lieu d'encourager le Comité des Ministres à entamer les négociations visant à améliorer la convention avant même son entrée en vigueur.

2.2.2. L'évolution dans l'Union européenne

23. A l'échelon de l'Union européenne, l'article 42 de la Charte des droits fondamentaux garantit aux citoyens «un droit d'accès aux documents des institutions, organes et organismes de l'Union, quel que soit leur support»[37]. Un droit similaire est déjà reconnu à l'article 255 du Traité établissant l'Union européenne (TUE), mis en œuvre par le Règlement (CE) n° 1049/2001[38]. Depuis 2008, la Commission européenne et un groupe d'Etats membres ont tenté de réduire le champ d'application du règlement[39], tandis que le Parlement européen[40] et un autre groupe d'Etats membres opposent, avec le soutien des ONG compétentes, une résistance aux restrictions proposées et vont jusqu'à faire du lobbying en faveur d'une extension supplémentaire de l'accès à l'information aux documents détenus par l'Union européenne[41]. La présidence danoise de l'Union européenne a tenté de parvenir à une solution de compromis sur un ensemble limité de réformes[42]. La présidence chypriote de l'Union européenne s'est engagée en juillet 2012 à relever le même défi[43], mais aucune solution n'a toutefois été trouvée au terme de la présidence irlandaise en juin 2013.

24. Access Info Europe a fait une demande intéressante en décembre 2008 concernant un document relatif à la réforme (toujours) en cours des règles de transparence de l'Union européenne. Le Conseil de l'Union européenne a fourni à Access Info Europe le document comprenant des propositions de réforme des Etats membres, mais en ayant supprimé les noms des pays, de sorte qu'il était impossible de savoir quel pays avait fait quelle proposition. Access Info Europe a contesté la décision du Conseil et le 22 mars 2011, le Tribunal (de l'Union européenne) a statué en faveur de la transparence. Le Conseil, rejoint par la République tchèque, la France, la Grèce, l'Espagne et le Royaume-Uni, a fait appel de la décision, alors que le Parlement européen s'est joint à Access Info Europe pour demander la pleine transparence de la procédure législative. L'avocat général espagnol, Cruz Villalón, a récemment constaté dans ses conclusions à la Cour de justice de l'Union européenne, à Luxembourg, que la procédure législative du Conseil doit être aussi transparente que les procédures similaires au niveau national, affirmant que «"Légiférer" est, par définition, une activité normative qui, dans une société démocratique, ne peut se développer qu'en suivant une procédure à caractère public[44]». En tant que membre d'un organe législatif, je ne peux qu'être d'accord.

25. Un autre exemple très concret a récemment illustré la nécessité de renforcer la transparence des institutions européennes. Deux demandes d'un journaliste de Bloomberg News en vue de la communication par la Banque centrale européenne de deux documents internes[45] ont été refusées par son Président,

---

36. Article 12 conjointement avec l'article 19 de la convention.
37. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:303:0001:0016:FR:PDF.
38. Voir le rapport de la Commission concernant l'application au cours de l'année 2010 du Règlement (CE) n° 1049/2001 relatif à l'accès public aux documents du Parlement européen, du Conseil et de la Commission: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0492:FIN:FR:PDF.
39. Voir la proposition de règlement du Parlement européen et du Conseil relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission, présentée par la Commission: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0229:FIN:FR:PDF.
40. Voir le rapport du Parlement européen sur la proposition de règlement du Parlement européen et du Conseil relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission (refonte): www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2011-0426+0+DOC+XML+V0//FR.
41. Voir «EU Transparency – Campaign on the reform of EU access to documents regulation»: www.access-info.org/en/european-union/226-reforming-regulation-1049; voir également la compilation de documents pertinents réalisée par Statewatch, disponible (en anglais) sur: www.statewatch.org/foi/observatory-access-reg-2008-2009.htm.
42. Voir Access Info Europe, *Last window of hope for EU transparency talks still open: Danish Presidency to broker agreement*, 16 juin 2012 (www.access-info.org).
43. Voir Access Info Europe, Cypriot Presidency prepares for agreement on access to EU documents, 9 juillet 2012.
44. Voir les conclusions complètes sur: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62011CC0280:fr:HTML.

M. Mario Draghi. En résumé, ces documents portent sur des allégations selon lesquelles, au début des années 2000, la Grèce s'est arrangée pour dissimuler ses niveaux d'endettement grâce au recours de swaps de devises avec la banque américaine d'investissement Goldman Sachs. Elle aurait agi de la sorte afin de se conformer aux critères sur les niveaux de la dette publique desquels dépendait l'adhésion de la Grèce à la zone euro[46]. Quand Bloomberg a poursuivi la BCE pour avoir accès à ces documents, la BCE a fait valoir avec succès devant le Tribunal (de l'Union européenne) que ces documents ne devaient pas être divulgués au motif que «la divulgation de ces documents aurait porté atteinte à la protection de l'intérêt public en ce qui concerne la politique économique de l'Union et de la Grèce[47]».

26. Il semble que la BCE craignait que la divulgation porte atteinte à la confiance publique quant à la capacité de la Grèce à honorer ses obligations au titre de la dette et menace donc la confiance en la monnaie unique[48]. Personnellement, je considère que la confiance publique dans les politiques économiques de l'Union, notamment les mesures prises par la BCE, tireront parti, au lieu d'en souffrir, d'une plus grande transparence. Des hypothèses au sujet de l'incidence sur les marchés financiers de la communication de ces documents ne sont pas, à mon avis, un obstacle légitime à la divulgation. Je comprends donc la déception de Bloomberg vis-à-vis de la décision, qui concerne clairement les ONG préoccupées par la liberté de la presse[49]. L'engagement juridiquement contraignant pris par les institutions européennes à l'égard de l'accès à l'information dans l'article 42 de la Charte risque, semble-t-il, d'être écrasé par une nouvelle «culture du secret» à Bruxelles et à Francfort. Un pourvoi intenté par Bloomberg devant la Cour de justice de l'Union européenne est toujours en suspens[50].

27. Il convient de noter que M. Draghi, l'actuel président de la BCE, était vice-président de Goldman Sachs au moment où les swaps mentionnés auparavant auraient été réalisés. Tandis que M. Draghi a nié toute implication[51], la simple apparence ou l'éventualité d'un conflit d'intérêt devrait peser fortement en faveur de la divulgation des documents permettant potentiellement de régler l'affaire une fois pour toutes.

28. Alors que le refus de divulguer ces documents n'était pas basé sur une exemption de sécurité nationale, il est rappelé que tous les autres motifs d'intérêt public visant à restreindre l'accès doivent aussi respecter les normes des Principes globaux[52]. L'affaire démontre la nécessité de réformer le Règlement 1049/2001 au regard des normes modernes afin d'éviter une culture du secret qui se développe au niveau européen.

29. A mon avis, il est fondamental que les institutions européennes donnent le meilleur exemple possible en matière de transparence et d'accès aux informations. La confiance du public envers les responsables politiques pâtit de l'excès de confidentialité. Ceci est d'autant plus marqué dans le cas de la politique européenne, que les citoyens perçoivent inévitablement comme étant plus distante, plus complexe et plus technocratique que leurs propres préoccupations locales.

2.3. La jurisprudence de la Cour européenne des droits de l'homme en matière d'accès à l'information

30. Pendant des années, la Cour européenne des droits de l'homme a considéré, dans son interprétation de l'article 10 de la Convention européenne des droits de l'homme (liberté d'expression), que celui-ci ne conférait aucun droit d'accès individuel à l'information détenue par l'Etat[53]. Ces derniers temps, elle a modifié prudemment, au cas par cas, son interprétation. En 2006, la Cour a examiné une affaire dans laquelle une

---

45. Le premier document était intitulé «L'incidence des échanges hors marché sur le déficit et la dette publics. Le cas de la Grèce» et le deuxième traitait de Titlos Plc, structure qui a permis à la Banque nationale de Grèce SA (ETE), le principal prêteur du pays, d'emprunter à la BCE en créant des garanties.
46. «Greek Debt Crisis: How Goldman Sachs Helped Greece to Mask its True Debt», Beat Balzli, Spiegel Online, 8 février 2010.
47. Affaire T-590/10, *Thesing et Bloomberg Finance c. BCE*, arrêt du Tribunal du 29 novembre 2012; «ECB Wins Ruling to Deny Access to Secret Greek Swap Files», Stephanie Bodoni, Elisa Martinuzzi et Gabi Thesing, Bloomberg, 29 novembre 2012.
48. «ECB Tells Court Releasing Greek Swap Files Would Inflame Markets», Elisa Martinuzzi et Gabi Thesing, Bloomberg, 14 juin 2012.
49. «MLDI applies for permission to intervene in case against European Central Bank», Media Legal Defence Initiative, 31 mai 2013; Transparency of the European Central Bank on the Financial Crisis: Access Info Europe applies to join key case at European Court of Justice, Access Info, 6 mai 2013.
50. Pourvoi formé le 18 janvier 2013 par Gabi Thesing, Bloomberg Finance LP, contre l'arrêt du Tribunal (septième chambre) rendu le 29 novembre 2012 dans l'affaire T-590/10: *Gabi Thesing, Bloomberg Finance LP c. Banque centrale européenne*, JO C 101/9, 6 avril 2013.
51. «Draghi Says He Knew Nothing About Goldman-Greece Deal», Jana Randow et Jeff Black, Bloomberg, 14 juin 2011.
52. Principes globaux, Introduction, page 1.

ONG de protection de l'environnement s'était vue refuser l'accès à des documents qui concernaient une centrale nucléaire. Elle a en l'espèce estimé que le refus de l'Etat de communiquer ces informations portait atteinte au droit de la requérante, découlant de l'article 10, à les obtenir[54]. Cette approche a été confirmée à nouveau dans deux affaires de 2009 contre la Hongrie. La Cour a conclu que le refus opposé aux demandes d'information – dans le premier cas, de la part de l'Union hongroise pour les libertés civiles concernant des documents relatifs aux procédures devant la Cour constitutionnelle et dans le second, de la part d'un historien concernant des données historiques détenues par le service de sécurité de l'Etat hongrois – violait l'article 10[55]. Dans le premier cas, la Cour a pourtant renvoyé à sa jurisprudence antérieure plus restrictive résumée dans l'arrêt *Leander*, mais pour ensuite affirmer:

> *«Cela étant, [la Cour] a récemment élargi son interprétation de la notion de "liberté de recevoir des informations" (Sdružení Jihočeské Matky/République tchèque (déc.), n° 19101/03, 10 juillet 2006), s'approchant de la reconnaissance d'un droit d'accès à l'information[56].»*

31. En 2012, la Cour a confirmé cette avancée dans un arrêt de la Grande Chambre contre la Suède, où elle a conclu que le refus d'un administrateur de l'Université de donner aux demandeurs – des chercheurs indépendants – accès à des données provenant de la recherche médicale rassemblées par l'Université «porterait atteinte aux droits [des demandeurs] […] de recevoir des informations par le biais de la consultation des documents publics en question[57]».

32. Il convient de noter que la Cour a été la première instance judiciaire à invoquer le principe selon lequel dès lors qu'une information a été rendue publique, les restrictions relatives à sa publication ultérieure ne sont plus justifiables, même pour des raisons de sécurité nationale: en 1991, la Cour a statué que l'injonction permanente sur une biographie d'un ancien membre des services de sécurité du Royaume-Uni ne pouvait être maintenue étant donné que le document avait déjà été publié aux Etats-Unis, estimant qu'en raison de la diffusion antérieure, la publication ne pouvait plus produire de préjudice identifiable[58]. Ce principe a été confirmé à l'ère d'internet où l'information devient publique rapidement et de manière irréversible. Il se reflète aussi dans les Principes globaux[59].

33. Dans son arrêt de la Grande Chambre sur l'affaire *El-Masri c. L'ex-République yougoslave de Macédoine*[60], concernant une victime allemande du programme de remises et de détentions secrètes de la CIA[61], la Cour a fait un grand pas vers la reconnaissance d'un «droit à la vérité» des victimes des violations de droits de l'homme[62]. Renvoyant au rapport de l'Assemblée, la Cour a aussi vivement critiqué le secret dont les autorités ont entouré les violations commises à l'encontre de M. El-Masri:

> *«La notion de "secret d'Etat" a souvent été brandie pour faire obstacle à la recherche de la vérité (paragraphes 46 et 103 ci-dessus), et elle a également été invoquée par le gouvernement américain dans le cadre de l'affaire portée par le requérant devant les tribunaux américains (paragraphe 63 ci-dessus). Le rapport Marty a en outre conclu que "[l]a même démarche a[vait] induit les autorités de «l'ex-République yougoslave de Macédoine» à cacher la vérité" (paragraphe 46 ci-dessus)[63].»*

---

53. *Leander c. Suède*, Requête n° 9248/81, arrêt du 26 mars 1987, paragraphe 74; *Gaskin c. Royaume-Uni*, Requête n ° 10454/83, arrêt du 7 juillet 1989, paragraphe 52; *Guerra c. Italie*, Requête n° 14967/89, arrêt du 19 février 1998, paragraphe 53; *McGinley et Egan c. Royaume-Uni*, Requêtes n^{os} 21825/93 et 23414/94, arrêt du 9 juin 1998; *Roche c. Royaume-Uni*, Requête n° 32555/96, arrêt du 19 octobre 2005, paragraphe 172 (mais la Cour a estimé que le refus de communiquer l'information était contraire à une obligation positive née de l'article 8).

54. *Sdruženi Jihočeské Matky c. République tchèque*, Requête n° 19101/03, décision sur la recevabilité du 10 juillet 2006. En l'espèce, la Cour a estimé que le refus était suffisamment justifié et s'appliquait aux restrictions prévues à l'article 10.2; la Cour a par conséquent conclu à l'irrecevabilité de la requête.

55. *Társaság A Szabadságjogokért (Union hongroise pour les libertés civiles) c. Hongrie*, Requête n° 37374/05, arrêt du 14 avril 2009 et *Kenedi/Hongrie*, Requête n° 31475/05, arrêt du 26 mai 2009.

56. *Társaság A Szabadságjogokért (Union hongroise des libertés civiles) c. Hongrie*, *ibid*., paragraphe 35.

57. *Gillberg c. Suède*, Requête n° 41723/06, arrêt du 3 avril 2012 (Grande Chambre).

58. *The Observer et The Guardian c. Royaume-Uni*, Requête n° 13585/88; *Sunday Times c. Royaume-Uni (n° 2)*, Requête n° 13166/87 – arrêts du 26 novembre 1991.

59. Principes globaux, Principe 49.*b*.

60. Requête n° 39630/09, arrêt du 13 décembre 2012.

61. Voir rapports de M. Dick Marty, *op. cit.*, Doc. 10957, paragraphe 3.1, et Doc. 11302 rev., chapitre VI.i.

62. La Cour examine cet aspect en vertu de l'aspect procédural de l'article 3 au lieu de l'article 10, voir paragraphe 192: «l'enquête inadéquate conduite en l'espèce a privé le requérant de la possibilité d'être informé de ce qui s'était passé, et notamment d'avoir un compte rendu précis des souffrances que l'intéressé disait avoir endurées et du rôle joué par ceux qu'il en tenait pour responsables», et paragraphe 264: «La Cour estime que la question soulevée sur le terrain de cette disposition recoupe au fond les griefs tirés par le requérant de l'article 3, et a déjà été traitée dans le cadre de l'examen de ceux-ci (paragraphe 192 ci-dessus).»

63. *El-Masri c. L'ex-République yougoslave de Macédoine*, paragraphe 191.

34. A mon avis, il convient de féliciter et d'encourager la Cour, qui continue sur la voie de l'élaboration, au cas par cas, d'un droit à l'information. Un tel droit est une condition préalable importante à l'exercice effectif de nombreux autres droits qui sont expressément reconnus par la Convention, tel que le droit à la vie et à ne pas subir de torture (articles 2 et 3), à la liberté et à la sûreté (article 5), au respect de la vie privée (article 8), à la liberté d'expression (article 10), et même à des élections libres (article 3, Premier Protocole).

3. Restrictions imposées au droit d'accès à l'information

35. Le droit d'accès à l'information, qui est un des aspects du droit à la liberté d'expression, n'est pas absolu en vertu de la Convention européenne des droits de l'homme et peut faire l'objet des restrictions prévues à l'article 10.2. Parmi les motifs de limitation figure la protection du souci légitime de la sécurité nationale, ainsi que le souligne le titre de ce rapport. Mais toute restriction doit être prévue par la loi, poursuivre un but légitime et être nécessaire dans une société démocratique[64]. Cette exception à la règle doit être interprétée de façon restrictive.

36. Compte tenu du fait que la sécurité nationale est l'un des motifs publics les plus importants pour restreindre l'information, lorsque les autorités publiques font valoir d'autres raisons pour restreindre l'accès dans l'intérêt général – notamment les relations internationales, l'ordre public, la santé publique et la sécurité publique, l'application de la loi et les intérêts économiques de l'Etat –, elles doivent respecter les mêmes normes pour imposer des restrictions à l'accès à l'information que celles appliqués aux considérations de sécurité nationale[65].

37. Afin d'éviter autant que possible toute ambiguïté et toute disparité dans l'application de ces exceptions à la règle de libre accès à l'information détenue par les organismes publics, j'estime qu'un aspect fondamental de mon mandat de rapporteur est de contribuer à la définition et à la diffusion de certains principes directeurs à cet égard. Le projet d'élaborer les Principes globaux susmentionnés s'est révélé extrêmement utile. En ma qualité de rapporteur à l'Assemblée, j'ai pris activement part à l'élaboration de ces principes, lors de la conférence européenne de consultation à Copenhague en septembre 2012. Je constate avec satisfaction que mes principaux arguments, ainsi que ceux d'autres acteurs européens, ont été pris en considération dans la formulation du texte définitif des Principes globaux rédigés à Pretoria (Tshwane) en avril 2013[66].

3.1. Le point de départ: il convient de présumer du caractère accessible de toute information détenue par l'Etat

38. Compte tenu des principes de démocratie et d'Etat de droit, il convient de présumer du caractère public et accessible de toute information détenue par l'Etat[67].

39. Les Principes globaux rappellent qu'en plus de l'Etat et d'autres autorités publiques, les entreprises du secteur de la sécurité nationale, notamment les sociétés privées de services militaires ou de sécurité, ont la responsabilité de divulguer l'information sur des situations, activités ou pratiques dont il y a raisonnablement lieu de croire qu'elles ont un effet sur l'exercice des droits de l'homme[68].

40. Les autorités souhaitant restreindre l'accès à des documents doivent justifier leur choix en démontrant sa conformité avec l'article 10.2 de la Convention européenne des droits de l'homme. Les Principes globaux confirment que, dans tous les cas, la «charge de la preuve» visant à démontrer la légitimité de toute restriction à l'accès à l'information incombe à l'autorité publique qui cherche à retenir l'information[69].

---

64. Article 10.2 de la Convention.
65. Principes globaux, Principe 2.*b*.
66. Voir paragraphe 4 ci-dessus. J'avais demandé au secrétariat de notre commission d'accepter l'invitation de l'OSJI à participer à la réunion de finalisation visant à rassembler les résultats des consultations pour l'élaboration des «Principes globaux», connus aussi sous le nom de «Principes de Tshwane». Ces consultations ont eu lieu à Pretoria (Tshwane), en Afrique du Sud, du 4 au 6 avril 2013.
67. ARTICLE 19, Droit du public à l'information: Principes relatifs à la législation sur la liberté de l'information, 1999 (ci-après «Principes de la liberté de l'information»), Principe 1.
68. Principes globaux, Principe 1.*b*.
69. *Ibid*., Principe 4.

41. Outre cette présomption générale, certaines catégories d'information entraînent une plus forte présomption en faveur de la divulgation. Parmi ces catégories d'information, qui peuvent ne pas être divulguées pour des raisons de sécurité nationale uniquement dans des circonstances tout à fait exceptionnelles, figurent les suivantes[70]:

– des violations du droit international des droits de l'homme et du droit international humanitaire; s'agissant des violations flagrantes des droits de l'homme ou des violations graves du droit humanitaire international et des violations systématiques ou généralisées des droits à la liberté et à la sûreté de la personne, ces informations ne peuvent en aucun cas être retenues pour des raisons de sécurité nationale;

– les garanties relatives au droit à la liberté et à la sûreté de la personne, à la prévention de la torture et des traitements inhumains et dégradants (interdits par l'article 3 de la Convention) et le droit à la vie (consacré à l'article 2), en particulier les lois et règlements portant sur les motifs, les procédures de détention et le traitement des détenus, notamment les méthodes d'interrogatoire;

– les structures et pouvoirs publics, notamment les lois et règlements applicables à ces autorités et leurs instances de surveillance et mécanismes de contrôle internes;

– les décisions de recourir à la force militaire ou d'acquérir des armes de destruction massive, notamment l'information sur l'ampleur et la portée générales de l'intervention et l'explication des motifs;

– l'information sur la surveillance: le cadre juridique relatif aux procédures à suivre pour l'autorisation, l'utilisation, le partage, le stockage et la destruction des données interceptées;

– l'information budgétaire et financière, notamment une information budgétaire suffisante pour permettre au public de comprendre les finances et les règlements du secteur de la sécurité;

– l'obligation de rendre des comptes concernant les violations constitutionnelles et statutaires et autres abus de pouvoir;

– la santé publique, la sûreté publique et l'environnement, notamment (ainsi que spécifié au Principe général 10.H):

> *«1. En cas de menace réelle ou imminente contre la santé publique, la sûreté publique ou l'environnement, toute information qui pourrait permettre au public de comprendre ou prendre des mesures pour éviter ou atténuer les préjudices résultant de cette menace, qu'elle soit due à des causes naturelles ou provoquée par des activités humaines, notamment par des actions de l'Etat ou des actions d'entreprises privées;*
>
> *2. D'autres informations, mises à jour régulièrement, sur l'exploitation des ressources naturelles, la pollution et les inventaires des émissions, les effets sur l'environnement des vastes travaux publics proposés ou existants, ou des extractions de ressources, et les plans d'évaluation et de gestion des risques pour les installations particulièrement dangereuses.» (traduction non officielle).»*

42. Les informations dont le caractère secret est jugé légitime devraient, elles aussi, conserver ce statut uniquement tant qu'il s'avère «nécessaire dans une société démocratique», ainsi que mentionné dans l'article 10.2. Comme une information peut, avec le temps, perdre de son intérêt, mais aussi de son caractère dangereux en cas de publication, il convient de tenir compte de ce facteur et d'éviter toute période de classification inutilement et/ou excessivement longue.

43. La notion d'information «publique» ou «détenue par l'Etat» doit être définie de façon large, de manière à englober les informations détenues par l'administration dans son ensemble, notamment celle des pouvoirs exécutif, législatif ou judiciaire, ainsi que par les instances de surveillance, les agences de renseignement, les forces armées, la police et d'autres agences de sécurité, et par tout organisme assumant une mission de service public et financé par les contribuables. Il importe que, même lorsque le service concerné est susceptible de faire exception à la règle de par la nature de ses activités, il ne soit pas totalement exonéré, d'emblée, de l'obligation de communiquer les informations dont il dispose[71].

70. *Ibid*., Principe 10 (dans lequel figurent d'autres détails et exemples).
71. Principes relatifs à la liberté d'information, Principe 4; Principes globaux, Principes 5 et 9.

44. En outre, «les exceptions doivent s'appliquer uniquement lorsqu'il y a un risque de préjudice important pour un intérêt protégé et dès lors que ce préjudice l'emporte sur l'intérêt général global que présente l'accès à l'information[72]». (traduction non officielle) Cette conception transparaît à juste titre dans diverses séries de principes énoncés par des dispositions non contraignantes applicables à l'accès à l'information, comme les Principes globaux[73].

45. Enfin, le principe de divulgation de l'information concernant les violations des droits de l'homme s'applique que les violations aient été commises par l'Etat qui détient l'information ou par un autre Etat[74]. Cela implique que les Etats membres du Conseil de l'Europe divulguent les informations qu'ils détiennent sur les violations des droits de l'homme commises par d'autres pays, par exemple dans la lutte contre le terrorisme.

3.2. La primauté de l'intérêt général

46. La «primauté de l'intérêt général»[75] affirme l'existence d'un droit d'accès à une information qui fait en principe l'objet d'une exception légitime, dès lors que l'intérêt général qui commande la communication de cette information revêt une importance supérieure à la défense des intérêts qui conduisent l'administration à la tenir secrète. Cette «primauté» offre une garantie précieuse, car il est impossible de donner une définition suffisamment étroite des exceptions pour prendre en compte l'ensemble des informations légitimement secrètes[76]. La définition de «l'intérêt général» doit être suffisamment large pour en permettre l'interprétation souple[77]. Cet intérêt général prime habituellement lorsque l'information en question:

– apporte d'importants éléments de réflexion à un débat public en cours;

– favorise la participation des citoyens au débat politique;

– fait état de graves abus, notamment de violations des droits de l'homme commises par des agents publics;

– renforce l'obligation de rendre des comptes dans la gestion des affaires publiques en général et dans l'utilisation des fonds publics en particulier;

– présente un avantage pour la santé publique ou la sécurité publique[78].

3.3. Une administration indépendante pour statuer sur les demandes d'information formulées en vertu de la liberté d'information

47. Le caractère quelque peu flou (inévitable, malgré nos efforts) de la notion d'intérêt général laisse aux autorités publiques une marge d'appréciation considérable pour communiquer ou non une information, dans la pratique. Pour cette raison, et afin d'éviter un effet dissuasif général sur la divulgation, les agents des autorités publiques qui sont chargés de répondre aux demandes d'information «ne doivent pas être sanctionnés pour la communication d'une information qu'ils estimaient raisonnablement et de bonne foi pouvoir divulguer conformément à la loi»[79] (traduction non officielle).

48. Le rejet d'une demande d'accès à l'information doit être motivé et garantir le droit du requérant à son réexamen diligent à un faible coût par une autorité indépendante sur le plan institutionnel, financier et opérationnel du pouvoir exécutif et de toutes les autorités du secteur de la sécurité[80]. En cas de non

---

72. Voir la déclaration conjointe de 2004 du Rapporteur spécial des Nations unies sur le droit à la liberté d'opinion et d'expression, Ambeyi Ligabo, du Représentant de l'Organisation pour la sécurité et la coopération en Europe sur la liberté des médias, Miklos Haraszti, et du Rapporteur spécial pour la liberté d'expression de l'Organisation des Etats Américains, Eduardo Bertoni: www.cidh.org/Relatoria/showarticle.asp?artID=319&lID=1 (en anglais uniquement). Il convient de noter que la Commission africaine des droits de l'homme et des peuples n'a pas nommé de rapporteur sur la liberté d'expression avant 2005. En 2008, son mandat a été élargi afin d'inclure expressément le droit à l'information.

73. Principes globaux, Principe 3.*b*.ii; ARTICLE 19, Principes de Johannesburg sur la sécurité nationale, la liberté d'expression et l'accès à l'information, 1995 (ci-après «Principes de Johannesburg»), Principes 15 et 16; Principes de la liberté de l'information, Principe 4.

74. Principes globaux, Principe 10.A.5.

75. Voir à ce sujet *The public interest test in FOI legislation*, par Prof. Maeve McDonagh, faculté de droit, Université de Cork, Irlande, 2012, www.right2info.org/resources/publications/eu-mcdonagh-maeve-the-public-interest-test-in-foi-legislation/view.

76. T. Mendel, The Johannesburg Principles: Overview and Implementation, 2003, p. 16.

77. R. Baxter, Public Access to Business Information Held by Government, 1997 Journal of Business Law, p. 4.

78. M. Carter et A. Bouris, Freedom of Information: Balancing the Public Interest, 2006, p. 8.

79. Principes globaux, Principe 44.

communication de l'information, l'autorité à l'origine du refus doit attester qu'elle détient ou non l'information demandée et motiver son refus par écrit[81]. Elle doit fournir des informations suffisantes sur l'identité de l'agent à l'origine de la décision et les moyens de faire appel de celle-ci[82].

49. L'autorité de contrôle indépendante «doit disposer des compétences et des ressources nécessaires pour garantir un réexamen efficace, notamment avoir pleinement accès à toutes les informations pertinentes, même si elles sont classées confidentielles[83]». (traduction non officielle) Ses décisions doivent en principe aussi pouvoir faire l'objet d'un recours devant une autorité judiciaire[84].

3.4. La sécurité nationale en tant qu'exception à l'accès à l'information

3.4.1. Mise en balance des intérêts en jeu

50. La protection de la sécurité nationale est indispensable à la pérennité de tout Etat et à la sécurité de sa population. Il va sans dire que bien des aspects de l'activité des services chargés de la sécurité de l'Etat doivent demeurer hors du domaine public pour que leur action soit efficace. Les informations relatives aux méthodes de travail (tactique), à l'identité des collaborateurs et informateurs, ainsi qu'à d'autres éléments sensibles doivent rester secrètes. On peut difficilement affirmer qu'il existe un intérêt général légitime supérieur à de telles considérations sécuritaires.

51. Mais dans bien des pays, une «culture du secret» s'est développée au fil du temps, enveloppant du secret tout aspect des structures et des activités des agences chargées de la sécurité. Certains services spéciaux sont en effet devenus «un Etat dans l'Etat», et échappent à toute obligation de rendre des comptes. Ce recours abusif au secret a servi à dissimuler de graves violations des droits de l'homme, compromettant le respect de l'Etat de droit[85].

52. L'introduction des Principes globaux donne un bon aperçu des intérêts en jeu:

> *«Un examen attentif de l'histoire récente laisse à penser que les intérêts légitimes en matière de sécurité nationale sont, dans la pratique, mieux protégés lorsque le public est amplement informé des activités que mène le gouvernement, notamment de celles qui visent à protéger la sécurité nationale[86].» (traduction non officielle)*
>
> *«Il est d'autant plus difficile de trouver un équilibre que, dans de nombreux pays, les tribunaux font preuve d'une indépendance minimale et de la plus grande déférence envers les revendications des pouvoirs publics lorsqu'il s'agit de la sécurité nationale. Cette considération est renforcée dans bon nombre de pays par des dispositions législatives en matière de sécurité qui soulèvent des exceptions au droit à l'information ainsi qu'aux règles ordinaires en matière d'administration de preuve et aux droits de l'accusé, dès lors que les autorités prouvent ou simplement invoquent un danger pour la sécurité nationale. Une invocation exagérée des préoccupations relatives à la sécurité nationale de la part de l'Etat peut gravement affaiblir les principales garanties institutionnelles contre les abus de ce dernier: indépendance de la justice, primauté du droit, contrôle du pouvoir législatif, liberté des médias et transparence de l'administration[87].» (traduction non officielle)*

53. A mon sens, ces «garanties institutionnelles» sont effectivement des éléments de la «sécurité nationale» appréhendée en termes de sécurité de nos Etats démocratiques en tant que tels.

---

80. *Ibid*., Définitions, p. 5 et Principe 26.
81. *Ibid*., Principes 19 et 20.*a*.
82. *Ibid*., Principe 20.*b*.
83. *Ibid*., Principe 26.*b*.
84. *Ibid*., Principe 26.*c*; sur la surveillance judiciaire du secteur de la sécurité, voir également la section 4 ci-après, points 83 à 86.
85. Voir le Doc. 10957 «Allégations de détentions secrètes et de transferts interétatiques illégaux de détenus concernant des Etats membres du Conseil de l'Europe»; le Doc. 11302 rev «Détentions secrètes et transferts illégaux de détenus impliquant des Etats membres du Conseil de l'Europe: second rapport»; et le Doc. 12712 «Les droits de l'homme et la lutte contre le terrorisme».
86. Principes globaux, Contexte et justification, p. 2.
87. *Ibid*.

3.4.2. La notion de sécurité nationale

54. Compte tenu de ce qui précède, une restriction basée sur un intérêt de sécurité nationale ne devrait être considérée comme légitime que dans certaines circonstances limitées. Les Principes de Johannesburg sur la sécurité nationale, la liberté d'expression et l'accès à l'information[88] de 1995 sont très stricts, compte tenu du fait qu'une menace contre la sécurité nationale correspond à une menace contre l'existence du pays et qu'il est «nécessaire de protéger l'indépendance politique ou l'intégrité territoriale du pays du recours ou de la menace de recours à la force[89].»

55. Les Principes globaux s'abstiennent d'essayer de fournir une définition positive de la «sécurité nationale». Parvenir à une telle définition, si elle doit être universelle, serait tout aussi difficile que de tenter de définir la notion de «terrorisme», avec laquelle les Nations Unies se débattent depuis des décennies.

56. Au contraire, le Principe 2 prévoit une recommandation sur les procédures, à savoir qu'il convient de faire figurer une définition précise de la «sécurité nationale» dans le droit national, d'une manière conforme aux besoins d'une société démocratique[90]. Dans le même ordre d'idées sur les procédures, le Principe 3, empruntant les termes de la Convention européenne des droits de l'homme et de la jurisprudence de la Cour de Strasbourg, précise:

> *«Aucune restriction du droit à l'information fondée sur des motifs de sécurité nationale ne peut être imposée, à moins que les pouvoirs publics ne soient en mesure de prouver que: (1) la restriction est (a) prévue par la loi et (b) nécessaire dans une société démocratique, (c) afin de protéger un intérêt légitime de sécurité nationale, et (2) la loi prévoit des garanties suffisantes contre les abus, notamment un contrôle rapide, complet, accessible et efficace de la validité de la restriction par une autorité de surveillance indépendante et un contrôle juridictionnel complet.» (traduction non officielle)*

57. Ces conditions sont énoncées clairement et, selon moi, de manière convaincante:

a. *Prévue par la loi*. La loi doit être accessible, sans ambiguïtés, écrite de manière précise et restrictive de façon à permettre aux individus de comprendre quelle information peut être retenue, quelle information doit être divulguée, et quelles actions concernant l'information font l'objet de sanction[91].

b. *Nécessaire dans une société démocratique*.

i. La divulgation de l'information doit présenter un risque réel et identifiable de porter un préjudice significatif à un intérêt légitime de sécurité nationale.

ii. Le préjudice que risque de causer la divulgation doit être supérieur à l'intérêt général présenté par la divulgation.

iii. La restriction doit respecter le principe de proportionnalité et constituer le moyen le moins restrictif disponible de se protéger contre le préjudice.

iv. La restriction ne doit pas compromettre la nature même du droit à l'information.

c. *Protection d'un intérêt légitime de sécurité nationale.* Les catégories restrictives des informations qui peuvent être classées confidentielles sur des motifs de sécurité nationale doivent être définies clairement par la loi.

---

88. Note 73 supra.

89. Principes globaux, Principe 2.*a*; S. Coliver, Commentary to: The Johannesburg Principles on National Security, Freedom of Expression and Access to Information, *Human Rights Quarterly* 20 (1998) 12-80, p. 20.

90. *Ibid*., Principe 2.*c*.; de même, M. Martin Scheinin, Rapporteur spécial des Nations Unies sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans le cadre de la lutte antiterroriste, dans son rapport: Compilation de bonnes pratiques en matière de cadres et de mesures juridiques et institutionnels, notamment de contrôle, visant à garantir le respect des droits de l'homme par les services de renseignement dans la lutte antiterroriste, A/HRC/14/46, 2010, à la Pratique n° 1, observe que: «Si les Etats ont des vues divergentes quant à la définition de la sécurité nationale, il est bon, en pratique, que la sécurité nationale et ses valeurs constitutives soient clairement définies par des lois adoptées par le parlement.»; la déclaration conjointe de 2004 des rapporteurs des Nations Unies sur la liberté d'expression et des médias affirme que «les législations sur le secret doivent définir précisément la notion de sécurité nationale et indiquer clairement les critères invoqués pour déclarer une information secrète, afin d'éviter l'utilisation abusive de l'étiquette "secret" pour empêcher la divulgation d'informations d'intérêt public». (traduction non officielle)

91. Voir aussi note 49 supra.

58. Quant au fond, les Principes globaux débutent par la définition «négative» suivante:

> *«Un intérêt de sécurité nationale n'est pas légitime si son véritable but ou son principal effet est de protéger un intérêt ne concernant pas la sécurité nationale, par exemple de protéger un gouvernement ou des agents publics d'une situation embarrassante ou de la divulgation de graves abus; de dissimuler des informations sur les violations de droits de l'homme, toute autre violation du droit, ou le fonctionnement des institutions publiques; de renforcer ou alimenter un intérêt politique, un parti ou une idéologie particulière; ou de réprimer des manifestations légales*[92]*.» (traduction non officielle)*

59. Je note avec satisfaction que les Principes globaux reflètent la position de l'Assemblée parlementaire selon laquelle les informations relatives aux violations des droits de l'homme ne peuvent être considérées comme des secrets d'Etat légitimes[93], position que j'ai défendue lors de la consultation de Copenhague en septembre 2012.

60. Les Principes globaux illustrent les situations où l'accès à l'information peut être limité, mais où l'intérêt général revêt une importance supérieure et l'accès à l'information reste protégé, par les exemples suivants[94]:

– les plans et opérations militaires en cours et les moyens dont disposent les forcés armées, aussi longtemps que ces informations présentent une utilité opérationnelle (les Principes limitent ainsi l'obligation de communiquer l'information aux cas où elle ne révèle plus rien permettant à l'ennemi de comprendre l'état de préparation, la capacité ou les plans de l'Etat en question);

– les informations sur la production, les capacités ou l'utilisation des systèmes d'armement et autres systèmes militaires, notamment les systèmes de communications;

– les informations sur les mesures spécifiques visant à protéger le territoire de l'Etat, les infrastructures essentielles, ou les institutions nationales essentielles contre les menaces ou le recours à la force ou le sabotage, dont l'efficacité dépend du secret;

– les informations concernant les questions de sécurité nationale relevant ou provenant des opérations, sources et méthodes des services de renseignement;

– les informations concernant des questions de sécurité nationale qui ont été fournies par un Etat étranger ou une instance intergouvernementale avec une attente explicite de confidentialité et d'autres communications diplomatiques dans la mesure où elles concernent des questions de sécurité nationale.

61. J'avais, en ce qui me concerne, proposé certaines modifications au stade de l'élaboration, par exemple d'ajouter les informations relatives à la prévention des actes terroristes et des crimes de même ordre ainsi que des informations en matière de lutte contre le terrorisme au sein de la catégorie des informations dont l'accès peut être limité. En conséquence, une note explicative au Principe 9 indique que:

> *«Dans la mesure où des informations particulières concernant le terrorisme et des mesures de lutte contre le terrorisme sont couvertes par l'une des catégories ci-dessus, le droit du public à l'accès à ces informations peut faire l'objet de restrictions pour des raisons de sécurité nationale conformément à cette disposition et à d'autres dispositions prévues par les Principes.» (traduction non officielle)*

62. S'agissant des communications diplomatiques, j'avais préconisé la limitation de la protection du secret aux communications diplomatiques qui concernaient directement les questions de sécurité nationale. Cela se reflète désormais au Principe général 9. Bon nombre de rapports «confidentiels» d'ambassades vont à peine au-delà de la compilation d'articles de presse et je vois mal en quoi leur publication pourrait être un tant soit peu préjudiciable. Même la publication par «Wikileaks» d'un nombre considérable de télégrammes d'ambassades américaines ne semble pas avoir eu de graves répercussions diplomatiques ou avoir été durablement préjudiciable. Au contraire: nombre de télégrammes parmi ceux qui semblent le plus embarrasser le gouvernement américain montrent en réalité que les diplomates américains ne sont pas nés de la dernière pluie et font heureusement preuve de réalisme et de franchise dans leurs rapports. Cette fuite à grande échelle a permis de tirer un enseignement: la publication d'informations relativement sensibles n'est jamais aussi préjudiciable qu'on pouvait le croire autrefois. Je considère donc la sévérité extrême avec laquelle les autorités américaines traitent M. Bradley Manning, le jeune soldat qui serait la «source» de ces fuites, comme des plus inappropriée[95].

---

92. Principes globaux, Définitions, p. 6. C'est également l'approche suivie par les Principes de Johannesburg, Principe 2.
93. Voir Résolution 1838 (2011), paragraphe 4.
94. Principes globaux, Principe 9.
95. Voir, par exemple, www.reuters.com/article/2013/02/28/us-usa-wikileaks-manning-idUSBRE91R0T720130228.

63. Un dernier motif peut amener à ne pas respecter le droit d'accès à l'information: un «état d'urgence», proclamé en vertu du droit national et international et menaçant l'existence d'un Etat[96]. Ce motif doit être utilisé avec la même prudence que le recours à l'«état d'urgence» en général. Toute dérogation au droit à l'information doit être cohérente avec les autres obligations prévues par le droit international. Les notes du Principe 8 indiquent à juste titre que certains aspects du droit de chercher, recevoir et répandre des informations et des idées sont étroitement liés à l'exercice de certains droits non susceptibles de dérogation (tels que le droit à la vie ou l'interdiction de la torture) et doivent par conséquent aussi être respectés en situation d'urgence.

3.5. Méthodes de classification de l'information

64. Si les informations peuvent être classifiées en fonction de critères restrictifs et juridiques, les Etats utilisent diverses méthodes en la matière, notamment la classification systématique ou automatique de l'ensemble des documents en fonction de critères préétablis et au cas par cas[97]. Du point de vue de la liberté de l'information, les critères juridiques de classification doivent être définis de façon suffisamment claire et étroite et la méthode appliquée doit s'accompagner de garanties procédurales adéquates. Il convient, par exemple, que la loi précise qui est autorisé à classifier les informations et fasse en sorte que ces individus puissent être retrouvés ou identifiables à partir du document classifié afin de faciliter l'obligation de rendre des comptes[98].

65. Il importe que tout document faisant l'objet d'une classification en porte la mention, que la justification de ce choix soit consignée, que le niveau et la durée de classification soient indiqués et que le préjudice que pourrait causer sa divulgation soit précisé[99]. Les agents publics devraient pouvoir contester la classification au niveau interne s'ils estiment qu'elle est inadaptée ou qu'elle n'est plus justifiée[100]. De plus, le fait qu'une information soit classifiée ne doit pas exclure sa divulgation à la suite d'une demande[101].

66. Des délais doivent être imposés pour la classification, conformément au principe selon lequel l'information ne peut être retenue que tant que cela s'avère «nécessaire dans une société démocratique», en vertu de l'article 10.2 de la Convention. Pour garantir le respect de ce principe, une révision régulière de la classification des informations doit avoir lieu au moins tous les cinq ans, avec une règle absolue: aucune information ne doit être classifiée indéfiniment. Au moment de la classification, le personnel concerné doit préciser la date, les conditions ou l'événement à partir duquel la classification devient caduque, pour l'efficacité du processus de contrôle[102].

67. La politique de déclassification du Conseil de l'Europe, adoptée par le Comité des Ministres en 2001[103], donne un exemple positif en la matière: tandis qu'un grand nombre de documents sont publics dès le départ, les documents classés «diffusion restreinte» deviennent automatiquement publics un an après leur production, et les rares documents classés «confidentiel» ou «secret» le deviennent respectivement au bout de dix ans et trente ans, sauf décision spéciale de faire exception à cette règle. L'Assemblée parlementaire, et en particulier la commission des questions juridiques et des droits de l'homme, applique aussi une politique plutôt libérale en la matière. Si la plupart des documents sont initialement classés «diffusion restreinte», les projets de rapport entrent dans le domaine public dès leur adoption par la commission, et celle-ci déclassifie librement d'autres documents dès lors que le rapporteur en fait la demande.

68. Le grand public devrait avoir accès aux procédures et aux normes du système de classification en vigueur dans son pays[104], ainsi qu'à un index d'informations classifiées[105].

---

96. Principes globaux, Principe 8.
97. T. Mendel, *Defining the Scope of National Security: Issues Paper for the Open Society Justice Initiative National Security Principles Project*, mai 2011, p. 6 et suiv.
98. Principes globaux, Principe 13.
99. *Ibid*., Principe 11.
100. Ibid., Principe 14.
101. Ibid., Principe 18.
102. Ibid., Principe 16; voir aussi: Open Society Justice Initiative, Declassification Procedures in Council of Europe Member States (2012).
103. Résolution Res(2001)6.
104. Principes globaux, Principe 12.
105. Ibid., Principe 15.

69. L'article 7 de la Convention européenne des droits de l'homme (pas de peine sans loi) prévoit semble-t-il clairement que, lorsque la violation d'un secret d'Etat est passible de sanction pénale, les citoyens aient accès à la liste des documents protégés à ce titre et mentionnés dans les dispositions pénales pertinentes, et que l'utilisation des informations qui figurent déjà dans le domaine public ne soit pas constitutive d'une violation de secret d'Etat. Le rapport de notre ancien collègue Christos Pourgourides, «Equité des procédures judiciaires dans les affaires d'espionnage ou de divulgation de secrets d'Etat»[106], montre que cette situation ne va pas de soi partout: en Fédération de Russie, plusieurs scientifiques ont été condamnés à de longues peines d'emprisonnement pour avoir «divulgué» des informations qui relevaient déjà incontestablement du domaine public avant que les scientifiques en question ne les utilisent dans le cadre de leurs activités universitaires de recherche et de publication.

70. Parallèlement, les autorités des Etats-Unis ont invoqué le secret d'Etat pour éviter que des plaintes civiles présentées par des victimes de «remise» comme Khalid el-Masri ne soient entendues par une juridiction. Alors que les pouvoirs publics ont affirmé que le procès imposerait d'examiner des secrets d'Etat relatifs à la lutte contre le terrorisme, le rapporteur de l'Assemblée, Dick Marty, a mis en évidence dans un mémoire d'*amicus curiae* qu'il a soumis à la Cour suprême des Etats Unis que l'ensemble des informations nécessaires à la défense de l'affaire de M. el-Masri relevaient déjà du domaine public – plus précisément, dans les propres rapports de l'Assemblée sur les remises et les détentions secrètes[107], qui ont largement couvert l'affaire de M. el-Masri.

71. Les affaires susmentionnées en Russie et aux Etats-Unis auraient violé les Principes globaux. S'agissant des affaires des universitaires russes, les Principes prévoient que les personnes qui n'ont pas accès aux informations classifiées ne doivent pas faire l'objet de poursuites pour la violation des législations sur le secret de l'Etat[108] et que toute loi ou autre règlement juridique en la matière doit être rendu public[109]. Ces dispositions visent principalement à protéger les journalistes, mais couvrent aussi, par exemple, les chercheurs universitaires ou d'ONG. Parallèlement, ainsi que l'énoncent clairement les Principes, il n'est pas question de garantir l'impunité aux journalistes et aux autres chercheurs qui commettent d'autres infractions pénales afin d'obtenir des informations secrètes auxquels ils n'ont pas accès. Inutile d'illustrer ce propos par l'exemple extrême d'un journaliste ou chercheur qui torture ou fait chanter une «source» pour qu'elle lui fournisse une information secrète: une effraction commise afin d'obtenir l'accès à l'information souhaitée demeure une infraction répréhensible.

72. Je partage avec les rédacteurs des Principes l'idée que «les divulgations à des tiers constituent un correctif important pour une classification généralisée.» (traduction non officielle) Je souscris aussi à la position des Rapporteurs spéciaux des Nations Unies et de la Commission interaméricaine des droits de l'homme qui, dans leur déclaration conjointe sur Wikileaks en 2010, ont affirmé que:

> *"[l]l incombe exclusivement aux autorités publiques et à leurs agents de protéger la confidentialité des informations légitimement classifiées sous leur contrôle. La responsabilité d'autres individus, notamment les journalistes, les travailleurs des médias et les représentants de la société civile, qui reçoivent et diffusent des informations classifiées parce qu'ils estiment que l'intérêt général le justifie, ne doit pas être engagée sauf s'ils se sont rendus coupables de fraude ou toute autre infraction pour obtenir l'information[110].» (traduction non officielle)*

73. Dans la même veine, il est tout à fait logique que des personnes n'ayant pas accès aux informations classifiées ne puissent être contraintes à révéler les sources de ces informations[111].

3.6. Les obligations logistiques des autorités publiques en matière d'accès à l'information

74. Si l'exemption illégitime de la sécurité nationale est l'une des plus sérieuses menaces pesant sur le droit d'accès à l'information publique, il n'en demeure pas moins que les autorités publiques ont également d'importantes tâches subsidiaires, qui doivent être remplies afin de garantir la réalisation effective du droit à l'information dans la pratique.

---

106. Doc. 11031 «Equité des procédures judiciaires dans les affaires d'espionnage ou de divulgation de secrets d'Etat», 25 septembre 2006.
107. Supra note 7.
108. Principes globaux, Principe 47.
109. *Ibid*., Principe 3.*a*.
110. Déclaration conjointe sur Wikileaks du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'expression, Frank LaRue, et de la Rapporteure spéciale de la Commission interaméricaine sur les droits de l'homme pour la liberté d'expression, Catalina Botero Marino, 21 décembre 2010 (en anglais uniquement).
111. Principes globaux, Principe 48.

75. Lorsque des demandes d'accès à des informations sont formulées, les autorités publiques doivent consacrer suffisamment de moyens et de temps pour trouver les informations manquantes, quelle que soit la raison de leur disparition[112]. En outre, les procédures menées pour trouver l'information devraient faire l'objet d'un contrôle juridictionnel, de même que les raisons de la disparition. Si l'information ne peut être trouvée, les autorités policières ou administratives doivent enquêter sur la disparition et publier les résultats de l'enquête.

76. Il est recommandé que les délais de réponse aux demandes d'information soient fixés par la loi et n'excèdent pas 20, voire tout au plus 30 jours ouvrables[113]. La loi peut prévoir différents délais en fonction de la complexité et des volumes de l'information. Lorsqu'il est urgent d'obtenir l'information afin de «protéger la vie et la liberté d'une personne», il convient d'appliquer des délais expéditifs.

77. Le fait qu'une partie d'un document demandé est légitimement retenue ou classifiée ne constitue pas un obstacle à l'accès à l'information si certaines parties peuvent en être divulguées. En pareil cas, «les autorités publiques sont tenues de prélever et diffuser l'information non exempte[114]». (traduction non officielle) De plus, une information retenue même légitimement doit être identifiée avec autant de spécificité que possible[115]. L'information divulguée doit être, si possible, mise à disposition dans le format demandé[116].

78. Toutes ces obligations s'appliquent aux informations fournies à des instances de surveillance, ainsi qu'à des membres du public. Si elles ne sont pas remplies, l'effet pratique est le même que si une exemption illégitime de sécurité nationale s'applique. Les excuses logistiques déraisonnables sont par conséquent inacceptables tout comme les refus non fondés de communiquer l'information pour des motifs de sécurité nationale.

3.7. Accès à l'information et respect de la vie privée

79. Le libre accès aux informations détenues par les organismes publics ainsi que préconisé dans ce rapport peut entrer en conflit avec le droit au respect de la vie privée des personnes directement concernées par ces informations. Le droit au respect de la vie privée est également garanti par la Convention européenne des droits de l'homme (article 8). Parallèlement, le droit à l'accès à l'information vient souvent renforcer le droit au respect de la vie privée pour accentuer l'obligation de rendre des comptes faite à l'administration, notamment les violations de ce droit[117]. Le droit d'accès d'une personne aux informations qui la concernent détenues par les autorités publiques sert en pratique à protéger le respect de sa vie privée: cela lui permet de contrôler l'utilisation de ses données à caractère personnel et de rectifier toute information inexacte. Les litiges proviennent généralement d'une mauvaise compréhension des informations accessibles ou protégées, voire du fait que les agents publics invoquent le respect de la vie privée pour dissimuler les malversations ou autres abus des pouvoirs publics[118]. Bien que cette question revête indéniablement une importance capitale pour la définition de la portée du droit à l'information, je compte la traiter uniquement dans la mesure où elle concerne les rapports entre accès à l'information et sécurité nationale. Les divers aspects de l'accès à l'information et du droit au respect de la vie privée ont en effet déjà fait l'objet d'autres travaux de l'Assemblée parlementaire[119].

80. Le droit international des droits de l'homme ne confère aucune primauté à l'un des deux droits – droit d'accès à l'information et droit au respect de la vie privée – sur l'autre. Le juste équilibre doit être trouvé au cas par cas[120]. Il convient tout d'abord qu'une définition claire et compatible des informations à caractère personnel protégées soit donnée par la législation et appliquée par les mécanismes de surveillance pertinents. Des critères d'appréciation objectifs des intérêts contraires doivent ensuite prendre en compte les intérêts privés et publics. Enfin, n'oublions pas qu'un organisme gouvernemental ne peut, de par sa nature collégiale, invoquer son droit au respect de la vie privée. Seul l'agent public concerné par des informations *à caractère personnel* qui portent sur sa vie privée peut invoquer ce droit, qui sera alors mis en balance avec les intérêts des personnes qui consultent et utilisent ces informations. Lorsque les données à caractère personnel concernent des malversations pénalement répréhensibles et d'autres atteintes aux droits de

112. *Ibid*., Principe 21.
113. *Ibid*., Principe 25.
114. *Ibid*., Principe 22.
115. *Ibid*., Principe 23.
116. *Ibid*., Principe 24.
117. D. Banisar, The Right to Information and Privacy: Balancing Rights and Managing Conflicts, 2011, p. 3, 9.
118. *Ibid*., p. 9.
119. Voir, par exemple, Doc. 12695, rapport sur la protection de la vie privée et des données à caractère personnel sur l'internet et les médias en ligne, 29 juillet 2011; rapport Doc. 8130 et Résolution 1165 (1998) sur le droit au respect de la vie privée, 3 juin 1998.
120. D. Banisar, *op. cit*., p. 16.

l'homme, l'intérêt général que présentent la transparence et l'obligation de rendre des comptes des organismes publics peut fort bien primer sur le droit d'un agent public au respect de sa vie privée. Cela dit, le respect de la présomption d'innocence (article 6.2 de la Convention européenne des droits de l'homme) impose de traiter avec le plus grand soin les informations qui allèguent de la commission d'actes pénalement répréhensibles, afin que la publication des informations qui ont donné lieu à une mise en accusation et leur examen en dehors du tribunal ne portent pas atteinte au droit du prévenu à un procès équitable.

81. De surcroît, les victimes de violations des droits de l'homme peuvent parfaitement avoir un intérêt privé légitime à éviter la divulgation publique de leurs noms, afin d'éviter tout préjudice supplémentaire. Ce point est expliqué de manière très pertinente dans une note au Principe 10.A.6.*b*:

> *«Les noms et d'autres données personnelles des victimes, de leurs proches et des témoins peuvent ne pas être divulguées au public dans la mesure nécessaire pour éviter de leur porter un préjudice supplémentaire, si la personne concernée le demande librement et de manière explicite, ou lorsque cela est manifestement compatible avec ce que la personne souhaite ou les besoins particuliers de groupes vulnérables. S'agissant des victimes de violence sexuelle, il convient d'exiger leur consentement explicite. L'identité des victimes mineures (âgées de moins de 18 ans) ne peut être divulguée au public. Ce principe doit toutefois être interprété compte tenu du fait que différents gouvernements ont, à divers moments, dissimulé des violations des droits de l'homme à l'opinion publique en invoquant le droit à la vie privée, notamment ceux des individus mêmes dont les droits sont ou ont été gravement violés, sans égard pour ce que souhaitent véritablement les individus concernés.» (traduction non officielle)*

4. Mécanismes de surveillance, de contrôle et de recours

82. La procédure de contrôle du bien-fondé du rejet d'une demande d'information et les mécanismes de recours doivent garantir l'accessibilité des informations non confidentielles et la protection des informations légitimement confidentielles.

83. Les instances de surveillance, qu'elles soient judiciaires ou parlementaires, et les organes indépendants de contrôle et de recours sont essentiels au maintien d'un système de poids et contrepoids dans le domaine de la sécurité. Ces instances doivent être prévues par la loi et prendre en compte tous les aspects du secteur de la sécurité, dont le respect de la législation, y compris des dispositions relatives aux droits de l'homme, le caractère effectif et l'efficacité des opérations de renseignement, ainsi que les pratiques en vigueur dans les domaines administratif et financier[121]. En outre, lorsque des éléments de preuve suffisants laissent penser qu'une infraction a été commise, il convient de mener une enquête en bonne et due forme et, le cas échéant, d'engager des poursuites pénales. Les considérations de sécurité nationale ne doivent en effet pas conduire à l'impunité de fait des agents publics qui prennent part aux opérations visant au maintien de la sécurité.

84. La difficulté en la matière tient, à l'heure actuelle, au manque d'informations fournies à ces instances[122] ainsi qu'au manque d'expertise et de compréhension de la situation qui leur est imputé[123]. Il est donc essentiel que les institutions de surveillance aient un accès illimité à toutes les informations indispensables à l'exercice de leur mandat[124]. Elles doivent bénéficier de la coopération pleine et entière des services de sécurité concernés, avoir la capacité de mener des enquêtes et de procéder à des contrôles de leur propre initiative, ainsi qu'être investies des pouvoirs nécessaires et des ressources humaines et financières indispensables à l'accomplissement effectif de leur mission[125].

---

121. M. Scheinin, *op. cit.*, Pratique 6.
122. Par exemple, *R. (Khan) v. Secretary of State for Foreign and Commonwealth Affairs* [2012] EWHC 3728 (Admin), un tribunal administratif britannique n'a pas été en mesure d'examiner, y compris dans le cadre d'une procédure de confidentialité, la légalité de renseignements britanniques communiqués aux Etats-Unis en vue de faciliter les frappes de drone au Moyen-Orient parce que le Gouvernement britannique a suivi sa politique consistant à ne pas confirmer ou infirmer l'existence de tels renseignements, ni le fait de savoir s'ils ont été transmis aux Etats-Unis. Le tribunal n'a donc pas pu examiner la question dont il était saisi (celui-ci ayant admis que le gouvernement avait le droit de refuser de lui communiquer cette information).
123. Union interparlementaire (UIP) et Centre pour le contrôle démocratique des forces armées (DCAF), Parliamentary Oversight of the Security Sector, 2003, p. 20.
124. M. Scheinin, *op. cit.*, Pratique 7; Principes globaux, Principe 32.
125. M. Scheinin, *ibid.*; Principes globaux, Principe 33; Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, A New Review Mechanism for the RCMP's National Security Activities, 2006, p. 18.

85. Une autre difficulté tient au fait que les institutions de surveillance sont des organismes nationaux dont la compétence est limitée aux actions du secteur des renseignements de leur propre pays. En même temps, la coopération internationale entre services de renseignement va s'intensifiant, les menaces à la sécurité dépassant aussi les frontières nationales. Les renseignements sont le plus souvent échangés sous réserve qu'ils ne soient pas communiqués par le service récepteur et à la condition que celui-ci ne dévoile pas sa source. Le fruit d'une telle coopération ne fait donc l'objet d'aucun contrôle. Une solution consisterait à renforcer la coopération internationale entre organes nationaux de contrôle pour harmoniser le développement de la coopération au plan opérationnel[126]. Cela ne devrait normalement pas poser de problème pour les institutions de pays soumis aux même normes en matière de transparence et de protection des droits de l'homme. Dans la pratique, cela suppose encore beaucoup de progrès dans les cultures organisationnelles des secteurs du renseignement de la plupart, sinon de tous les Etats membres du Conseil de l'Europe.

86. Il convient de noter que ces instances accomplissent par nature une mission de service public et qu'elles relèvent par conséquent, en principe, du champ d'application du droit d'accès à l'information[127].

87. Pour parvenir au meilleur équilibre possible entre transparence et intérêts de la sécurité nationale, un rapport antérieur de l'Assemblée proposait de créer une instance composée de juges, assistés d'experts en fonctionnement des services secrets. Cette structure devra bénéficier d'un accès illimité à tout type d'informations détenues par le pouvoir exécutif, afin d'être en mesure de définir les informations qui doivent rester confidentielles et celles qu'il convient de rendre publiques. Il importe que la procédure en vigueur devant cette instance soit confidentielle, mais contradictoire, afin qu'elle puisse rendre des décisions objectives en toute connaissance de cause[128].

5. Protection des donneurs d'alerte

88. Pour que le grand public bénéficie des signalements par les donneurs d'alerte, "comme outils permettant d'augmenter la responsabilisation et de renforcer la lutte contre la corruption et la mauvais gestion", ainsi qu'énoncé par l'Assemblée dans sa Recommandation 1916 (2010) sur la protection des «donneurs d'alerte», les agents de l'Etat devraient être protégés contre les représailles lorsqu'ils divulguent des informations faisant état d'actes répréhensibles, quelle que soit la gravité de ces actes et leurs conséquences éventuelles pour la sécurité nationale[129]. Plus précisément, ils devraient être exonérés de responsabilité civile ou pénale et protégés contre la perte de leur emploi et/ou contre les dommages physiques ou psychologiques[130]. De plus, ils ne devraient pas être tenus de fournir des éléments de preuve écrits pour que leur demandes donnent lieu à une enquête ou pour éviter les représailles et ils ne devraient pas non plus assumer la charge de la preuve pour ce qui est de la véracité de l'information divulguée, sous réserve qu'ils agissent de bonne foi[131].

89. Les Principes globaux comportent une liste détaillée de catégories d'informations que les donneurs d'alerte devraient être à même de divulguer sans être en butte à des représailles, notamment des informations:[132]

– sur des infractions pénales;

– sur des violations des droits de l'homme;

– sur des violations du droit humanitaire international;

– sur la corruption;

---

126. Voir le troisième rapport de M. Dick Marty (Doc. 12714, *op. cit.*), paragraphes 52-57.
127. Principes globaux, Principe 34.
128. Voir Doc. 12714 de l'Assemblée, *op. cit.*; voir également à cet égard la controverse survenue au Royaume-Uni au sujet de la "procédure de confidentialité"; par exemple la contribution de Rosalind English, "Secret justice: do we have a compromise?", UK Human Rights Blog, 4 avril 2012, ainsi que les échanges avec David Anderson QC, qui contrôle de manière indépendante la législation britannique en matière de lutte contre le terrorisme. Ces questions se sont récemment posées avec une acuité particulière lorsque la Cour suprême du Royaume-Uni a décidé «à contrecœur» d'examiner partiellement un recours en l'absence d'une partie pour des motifs de sécurité nationale (www.supremecourt.gov.uk/news/bank-mellat-v-hm-treasury.html); Adam Wagner, «Historical first as Supreme Court boots Iranian bank out of secret hearing», UK Human Rights Blog, 21 mars 2013.
129. Principes globaux, Partie IV.
130. *Ibid*., Principe 41.
131. *Ibid*., Principe 38.
132. *Ibid*., Principe 37.

– sur les menaces pour la santé et la sécurité publiques;

– sur les menaces pour l'environnement;

– sur les abus d'autorité;

– sur les erreurs judiciaires;

– sur la mauvaise gestion ou le gaspillage des ressources;

– sur les représailles pour signalement d'un des actes répréhensibles énumérés ci-dessus;

– sur la dissimulation intentionnelle de toute situation relevant de l'une des catégories ci-dessus.

90. Même si l'information divulguée ne relève pas d'une de ces catégories, les donneurs d'alerte devraient pouvoir s'appuyer, le cas échéant, sur «l'intérêt public général» (voir section 3.2, paragraphe 46 ci-dessus) ou sur «la protection de l'intérêt public»[133], ainsi que reconnu par les Principes globaux. Seules des mesures civiles devraient être prises à l'égard des intéressés. L'engagement de poursuites pénales à l'encontre des donneurs d'alerte ne devrait intervenir que dans les circonstances les plus exceptionnelles, être prévu par la loi et proportionné aux dommages causés aux intérêts de la sécurité nationale[134].

91. La sévérité des poursuites pénales engagées contre la source de "Wikileaks", M. Bradley Manning, apparaît comme une violation claire des principes susmentionnés. La diffusion de l'enregistrement vidéo de l'homme tué à Bagdad par l'équipage d'un hélicoptère américain qui prenait pour cible des civils, notamment des journalistes, en commentant ces scènes avec cynisme, a trait à n'en pas douter à des infractions pénales, des violations des droits de l'homme et des violations du droit humanitaire international. Le fait de contribuer à rendre public ces faits pour déclencher le débat et favoriser la responsabilité découlant des actes concernés devrait être salué, pas réprimé. Toute sanction pénale pour ces fuites alléguées devrait être proportionnée au véritable préjudice causé et tenir compte des idéaux de M. Manning, qui avait vingt ans à peine au moment des faits supposés.

92. Pour optimiser les services rendus au grand public par les donneurs d'alerte, les lois relatives à la protection des intéressés devraient prévoir des procédures internes et désigner, au sein des autorités publiques, des agents chargés de recevoir des divulgations protégées[135]. De plus, en l'absence de mécanismes internes, ou lorsque ceux-ci sont défaillants, les donneurs d'alerte devraient être à même de

---

133. Principes globaux, Principe 43: «Défense de l'intérêt public pour les agents de l'Etat

a. Lorsque les agents de l'Etat peuvent faire l'objet d'une procédure pénale ou civile, ou lorsque qu'ils sont passibles de sanctions administratives pour avoir divulgué des informations qui ne sont pas protégées au titre des présents principes, la loi devrait prévoir une exception d'intérêt public si celui-ci est mieux servi par la divulgation que par la non divulgation

b. En se posant la question de savoir si l'intérêt public est mieux servi par la divulgation que par la non-divulgation, le juge ou l'enquêteur doit déterminer:

a. i. si l'étendue de la divulgation était raisonnablement nécessaire pour révéler l'information d'intérêt public;

b. ii. la portée et le risque de préjudice pour l'intérêt public qu'entraîne la divulgation;

c. iii. si la personne avait des raisons sérieuses de croire que la divulgation répondait à l'intérêt public;

d. iv. si la personne ayant divulgué l'information au public a auparavant suivi une procédure interne et/ou s'est adressée à un organe de contrôle indépendant et, ce faisant, si elle a respecté les procédures définies aux Principes 38 à 40; et

e. v. si des circonstances exceptionnelles justifient la divulgation.»

134. *Ibid*., Principe 45; voir également deux arrêts de la Cour européenne des droits de l'homme reconnaissant le bien fondé de la protection des donneurs d'alerte:

– *Bucur et Toma c. Roumanie* (2013), Requête n° 40238/02

M. Bucur travaillait pour le service des écoutes téléphoniques d'une unité du SRI (Service de renseignement roumain) ayant son siège à Bucarest. Invoquant l'article 10 (liberté d'expression), il a contesté avec succès la sanction pénale qu'il s'était vu appliquer pour avoir divulgué des informations classées "top secret". Il avait rendu publiques des cassettes audio, lors d'une conférence de presse, qui contenaient les enregistrements d'appels téléphoniques passés par plusieurs journalistes et hommes politiques ainsi que des éléments à charge qu'il avait consignés dans le registre des conversations.

– *Guja c. Moldovie* (2008), Requête n° 14277/04

Le renvoi par le gouvernement d'un procureur qui avait transmis de manière illicite des informations (sur des pressions politiques indues sur l'appareil judiciaire) à un journal constituait une ingérence illégale dans le droit à la liberté d'expression de l'intéressé (droit de partager l'information) parce que ce renvoi n'était pas nécessaire dans une société démocratique.

135. *Ibid*., Principe 39.A.

faire des signalements protégés à des organes de contrôle indépendants protégeant l'identité des donneurs d'alerte, de façon à les préserver contre les formes les plus subtiles de représailles[136]. Les divulgations publiques, avec tous les risques qu'elles emportent, ne devraient intervenir qu'en dernier recours.

93. Pour assurer la protection universelle des agents publics, ceux-ci ne devraient pas pouvoir lever eux-mêmes ou renoncer à une protection en tant que donneurs d'alerte. Tout accord ou contrat en ce sens doit être considéré comme étant nul dès le départ[137]. Les donneurs d'alerte devraient être en mesure de faire état de représailles ou de menaces à des organes de contrôle indépendants, habilités à prendre des mesures correctives ou réparatrices[138].

94. Ces conditions garantissent la protection des donneurs d'alerte et répondent aux objectifs plus généraux de prévention des abus de pouvoir et de responsabilisation des gouvernements, notamment du secteur du renseignement. Ces conditions devraient être fixées dans des lignes directrices applicables à toutes les autorités publiques afin de promouvoir la sécurité juridique et de rassurer d'éventuels donneurs d'alerte[139].

6. Conclusions

95. L'étendue croissante des opérations spéciales menées au nom de la sécurité nationale et des dispositions pertinentes adoptées pour les mêmes raisons, surtout depuis le 11 septembre, a été préjudiciable à la législation relative à la liberté de l'information, qui vise à renforcer la transparence de l'administration et son obligation de rendre des comptes. Le manque d'informations qui en découle a, à son tour, empêché les parlements, les juridictions et les simples citoyens de prendre part concrètement à la prise des décisions pertinentes et d'obliger le pouvoir exécutif à rendre compte de ses actes.

96. Le Préambule des Principes globaux souligne à juste titre que:

> *«En permettant au public de contrôler l'action des pouvoirs publics, l'accès à l'information est non seulement une garantie contre les abus de la part d'agents de l'Etat, mais elle permet également au public de jouer un rôle dans la définition des politiques de l'Etat et constitue, par conséquent, une composante essentielle d'une véritable sécurité nationale, de la participation démocratique et de l'élaboration de politiques rationnelles. Pour protéger le plein exercice des droits de l'homme, il peut être nécessaire, dans des circonstances particulières, de garder l'information confidentielle pour protéger les intérêts légitimes en matière de sécurité nationale.»*

97. Il est indispensable de mettre en place des garanties adéquates aux différents niveaux de procédure, afin de prévenir tout abus. Des lignes directrices claires doivent être définies pour garantir que les motifs de sécurité nationale soient uniquement invoqués dans des situations appropriées et fassent l'objet d'un contrôle adéquat. Les Principes globaux offrent à cet égard un ensemble de lignes directrices bien conçues. Ils mettent en relief les questions qui présentent un intérêt public légitime particulier et qui ne devraient pas être classifiées secrètes. Ainsi, les informations relatives à de graves violations des droits de l'homme commises par des agents publics ne devraient jamais être classifiées secrètes. Le fait qu'un gouvernement en place risque d'être embarrassé ne constitue pas une menace pour la sécurité nationale. Les organismes qui s'occupent de questions de sécurité nationale devraient être régulièrement contrôlés, y compris par des organes de contrôle parlementaires ou judiciaires dévoués, s'appuyant sur un mandat solide et dotés des moyens nécessaires. Dernier point mais non le moindre, les donneurs d'alerte devraient bénéficier d'une protection adéquate.

98. Le rôle joué par l'Assemblée parlementaire dans la promotion effective des droits de l'homme dans les Etats membres du Conseil de l'Europe suppose qu'elle prenne une part active à l'élaboration et à la promotion de normes communes en matière de droit d'accès à l'information tout en respectant les préoccupations nationales légitimes en matière de sécurité nationale, comme j'ai essayé de le faire dans ce rapport, établi en coopération avec le projet de Principes globaux mis en œuvre avec l'aide de l'Open Society Justice Initiative. Nous devons à présent inviter instamment les parlements nationaux à mettre en place des instances de

136. *Ibid*., Principe 39.B.
137. *Ibid*., Principe 41.E; voir à ce propos, même si elle ne porte pas sur l'exemption au titre de la sécurité nationale, la controverse au sujet des «clauses de confidentialité» signées par le personnel du Service national de santé (www.bbc.co.uk/news/health-21780425).
138. *Ibid*., Principe 41.C.
139. *Ibid*., Principe 42.

surveillance effectives, afin de garantir le respect de ces normes. Il importe que les institutions européennes (notamment le Conseil de l'Europe et l'Union européenne) offrent un exemple constructif en la matière et accordent l'accès le plus large possible aux informations qu'elles détiennent.

99. Dans le projet de résolution, j'ai résumé les principaux points sur lesquels nous devrions tous pouvoir tomber d'accord. Je propose aussi un projet de recommandation au Comité des Ministres, afin d'associer les gouvernements des Etats membres à nos efforts tendant à donner vie à la Convention du Conseil de l'Europe sur l'accès aux documents publics.