Parliamentary Assembly
Assemblée parlementaire
http://assembly.coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Version provisoire

Commission des questions juridiques et des droits de l'homme

Améliorer la protection des donneurs d'alerte

Projet de rapport*

Rapporteur : M. Pieter Omtzigt, Pays-Bas, Groupe du Parti populaire européen

A. Projet de résolution

1. L'Assemblée rappelle sa Résolution 1729 (2010) et sa Recommandation 1916 (2010), qui invitent tous les États membres à améliorer la protection des donneurs d'alerte, à renforcer l'obligation de rendre des comptes et à soutenir la lutte contre la corruption et la mauvaise gestion, dans le secteur public comme dans le secteur privé.

2. Elle rappelle par ailleurs sa Résolution 1954 (2013) et sa Recommandation 2024 (2013), qui adhèrent aux Principes de Tshwane sur la sécurité nationale et le droit à l'information en vue de renforcer le juste équilibre entre le droit des citoyens à savoir et la protection des préoccupations légitimes en matière de sécurité nationale.

3. L'Assemblée souligne l'importance de la jurisprudence de la Cour européenne des droits de l'homme, qui affirme le droit au respect de la vie privée, à la liberté d'expression et à la protection des donneurs d'alerte, y compris dans les domaines de la sécurité nationale et du renseignement.

4. Elle se félicite par ailleurs de la récente adoption, par le Comité des Ministres, de la Recommandation 2014(7), qui appelle les États membres à créer un cadre normatif, judiciaire et institutionnel adéquat pour la protection des donneurs d'alerte.

5. Elle observe que le Conseil de l'Europe a mis en place des lignes directrices destinées aux agents sur le signalement des malversations ; ces lignes directrices, qui établissent des voies de signalement internes, reprennent une partie, mais pas l'intégralité, des principes énoncés par l'Assemblée et le Comité des Ministres.

6. Compte tenu des révélations faites à propos des opérations massives de surveillance et des intrusions dans la vie privée auxquelles la NSA et d'autres services de renseignement ont procédé, qui concernent les communications de nombreuses personnes sans qu'elles soient soupçonnées d'aucun acte répréhensible, l'Assemblée constate à regret que la divulgation d'informations relatives à la sécurité nationale est généralement exclue de la protection accordée aux donneurs d'alerte.

7. Elle considère que les mesures de protection des donneurs d'alerte devraient viser l'ensemble des personnes concernées qui dénoncent les actes répréhensibles susceptibles de violer les droits des autres individus garantis par la Convention européenne des droits de l'homme, y compris les personnes qui travaillent pour le compte des services de sécurité nationale ou de renseignement.

8. Comme le fait de donner l'alerte, d'une part, est essentiel pour assurer le respect des limites légales imposées aux opérations massives de surveillance (voir la Résolution * 2015, paragraphe *) et, d'autre part, a des ramifications internationales dans le domaine de la sécurité nationale ou du renseignement, l'Assemblée estime que les donneurs d'alerte (y compris les agents des services administratifs compétents

* Projet de résolution et projet de recommandation adoptés par la commission le 18 mars 2015.

et des entreprises privées concernées sous contrat avec l'État), dont les révélations sont par ailleurs conformes à la Résolution 1729 (2010), à la Recommandation 2014(7) du Comité des Ministres ou aux Principes de Tshwane avalisés par la Résolution 1954 (2013), devraient se voir octroyer l'asile dans tout État membre du Conseil de l'Europe lorsqu'ils sont persécutés dans leur propre pays.

9. L'Assemblée appelle par conséquent :

9.1. les États membres et observateurs du Conseil de l'Europe et l'Union européenne, le cas échéant, à :

9.1.1. adopter une législation relative à la protection des donneurs d'alerte qui vise également le personnel des services de sécurité nationale ou de renseignement et des entreprises privées qui exercent leurs activités dans ce domaine ;

9.1.2. octroyer l'asile, autant que possible en vertu du droit interne, aux donneurs d'alerte menacés de mesures de rétorsion dans leur pays d'origine, sous réserve que leurs révélations réunissent les conditions nécessaires à leur protection au titre des principes énoncés par l'Assemblée ;

9.1.3. convenir d'un instrument juridique contraignant (convention) consacré à la protection des donneurs d'alerte sur la base de la Recommandation 2014(7) du Comité des Ministres, en tenant compte des événements récents.

9.2. les États-Unis d'Amérique à permettre à M. Snowden de rentrer sans craindre l'engagement de poursuites pénales à son encontre dans des conditions qui ne l'autoriseraient pas à soulever l'exception d'intérêt général.

B. Projet de recommandation

1. L'Assemblée rappelle sa Résolution * (2015) et sa Recommandation 1916 (2010).

2. Elle se félicite de l'adoption par le Comité des Ministres de la Recommandation (2014)7, qui représente une avancée importante dans la bonne direction.

3. Elle invite le Comité des Ministres :

   3.1. à promouvoir l'amélioration supplémentaire de la protection des donneurs d'alerte, en lançant le processus de négociation d'un instrument juridique contraignant sous la forme d'une convention-cadre ouverte aux États tiers et portant sur la révélation des méfaits commis par les personnes employées dans le domaine de la sécurité nationale et du renseignement ;

   3.2. dans l'intervalle, à réfléchir aux voies et moyens de prévoir l'assistance technique du Conseil de l'Europe aux États membres pour la mise en œuvre de la Recommandation (2014)7, et

   3.3. à encourager le Secrétaire Général à améliorer encore les dispositions relatives aux donneurs d'alerte applicables au Conseil de l'Europe, en vue de les mettre pleinement en conformité avec les principes énoncés par l'Assemblée et le Comité des Ministres.

C. Exposé des motifs par M. Pieter Omtzigt, rapporteur

1. Introduction

1. Du versement de pots-de-vin aux autres actes de corruption, de la fraude aux violations des droits de l'homme, les donneurs d'alerte nous ont aidé à lutter contre l'impunité, en révélant les malversations du secteur public comme du secteur privé. Le fait de protéger les personnes qui contribuent au débat public en divulguant des informations permet d'améliorer l'obligation démocratique de rendre des comptes, la gouvernance et la protection des droits de l'homme. L'Assemblée a encouragé par le passé les États à élaborer des cadres juridiques et à mettre en œuvre des moyens adéquats d'obtenir des révélations de la part des donneurs d'alerte et d'y donner suite, à renforcer la protection des individus qui divulguent des informations dans l'intérêt général contre les mesures de rétorsion dont ils peuvent faire l'objet et à favoriser la création d'un environnement dans lequel les citoyens se sentent moins menacés lorsqu'ils font état de malversations[1].

2. Les révélations faites par Edward Snowden ont démontré une fois encore l'importance de l'action des donneurs d'alerte, en mettant en lumière les abus des activités de renseignement, qui sont pour l'instant exclues des mesures de protection des donneurs d'alerte. Les documents divulgués grâce à M. Snowden ont révélé que les États pouvaient intercepter les communications et accéder aux données à caractère personnel, quelle qu'en soit la forme, de toute personne, à tout moment et partout. Ces révélations ont lancé un débat planétaire sur l'utilisation des technologies qui portent atteinte à la vie privée des citoyens, une pratique que bien des gens redoutaient sans être en mesure de la dénoncer, faute de preuves, en raison du secret qui entoure de manière omniprésente les activités des services de renseignement.

3. Le 6 novembre 2013, la commission des questions juridiques et des droits de l'homme m'a nommé rapporteur pour deux sujets intimement liés : « Les opérations massives de surveillance »[2] et le « Protocole additionnel à la Convention européenne des droits de l'homme sur la protection des donneurs d'alerte »[3]. Après un premier tour de table le 6 novembre 2013, la commission a décidé, lors de sa réunion du 27 janvier 2014, sur la base de ma note introductive[4], de remplacer le titre initial du futur rapport, « Protocole additionnel à la Convention européenne des droits de l'homme sur la protection des donneurs d'alerte », par l'intitulé « Améliorer la protection des donneurs d'alerte » et d'inviter M. Edward Snowden et Mme Anna Myers, coordinatrice du Réseau international des donneurs d'alerte (Whistleblowing International Network – WIN) à un échange de vues avec la commission. Malheureusement, pour l'audition sur « Les opérations massives de surveillance » d'avril 2014, il n'a pas été possible d'obtenir les assurances nécessaires qui auraient permis à M. Snowden de se rendre en toute sécurité à Strasbourg et de voyager librement dans un pays de son choix après cette audition. La commission a par conséquent dû se contenter, lors de sa réunion du 24 juin 2014, d'auditionner M. Snowden par liaison vidéo en direct depuis Moscou, où il avait provisoirement trouvé refuge[5]. J'aimerais remercier M. Snowden d'avoir été prêt à s'adresser à la commission et à répondre en direct aux questions qui lui étaient posées, malgré les risques qu'il pouvait courir sur le plan juridique. J'ai présenté le contenu de ces révélations et leurs conséquences de façon assez précise dans le rapport sur « Les opérations massives de surveillance », que la commission a adopté à l'unanimité à l'occasion de sa réunion du 26 janvier 2015[6]. Le 22 janvier 2015, la commission a également procédé à un échange de vues avec Maria Bamieh, procureur britannique détaché auprès d'Eulex au Kosovo, qui avait tiré la sonnette d'alarme sur des faits allégués de corruption commis au sein même d'Eulex, et a entendu une déclaration faite depuis sa prison par le donneur d'alerte de la CIA John Kiriakou, qui était présentée en direct au moyen d'une liaison vidéo par son avocate, Jesselyn Radack, elle-même donneuse d'alerte et ancien agent du Département américain de la Justice.

4. Lorsque les révélations concernent les activités nationales de renseignement, des intérêts différents et parfois contraires entrent en jeu de façon plus prononcée que dans les autres actions des donneurs d'alerte. La liberté d'expression des donneurs d'alerte et la liberté d'information des citoyens se heurtent à l'obligation faite à l'agent de renseignement de protéger les informations secrètes ; la transparence et l'obligation démocratique de rendre des comptes s'opposent à la nécessité de préserver le secret des opérations de renseignement pour assurer leur efficacité. Mais le légitime besoin de secret et de confidentialité ne devrait pas être invoqué de manière abusive pour dissimuler les violations des droits de l'homme commises par les

[1] Voir la Résolution 1729 (2010) et la Recommandation 1916 (2010).
[2] Proposition de résolution, doc. 13288 du 6 août 2013.
[3] Proposition de résolution, doc. 13278 du 5 juillet 2013.
[4] Du 23 janvier 2014, document AS/Jur (2014) 2.
[5] [Vidéo du témoignage d'Edward Snowden du 26 juin 2014 (en anglais)]
[6] Document AS/Jur (2015)1 du 19 janvier 2015.

agents gouvernementaux. Même lorsque, d'une part, la législation limite la surveillance et, d'autre part, des mécanismes de surveillance parlementaire ou judiciaire raisonnablement efficaces sont mis en place pour veiller à ce que les services de renseignement soient amenés à rendre compte de leurs actes devant les citoyens, ce qui n'est pas encore le cas dans la plupart des pays, les donneurs d'alerte, cette « épée de Damoclès » de la divulgation protégée des violations commises, représentent un moyen utile de garantir dans la pratique le respect de ces limites légales.

5. Comme je l'avais indiqué dans mon précédent rapport sur la protection des donneurs d'alerte, adopté par l'Assemblée en janvier 2010, la plupart des États membres du Conseil de l'Europe ne disposaient à l'époque d'aucun cadre législatif efficace pour protéger les donneurs d'alerte de bonne foi qui divulguaient de graves violations des droits de l'homme ou actes de corruption, et encore moins d'une définition légale généralement admise des critères constitutifs de la qualité de « donneur d'alerte ». La notion même de « dénonciation des irrégularités » était inconnue de nombreux pays ; cette notion ne doit pas être confondue avec l'activité de « mouchard », extrêmement péjorative, surtout dans les pays qui ont subi des périodes de pouvoir totalitaire ou autoritaire ; elle ne doit pas davantage être envisagée uniquement dans le cadre du renforcement de « la protection des témoins », qui concerne inévitablement le système judiciaire répressif.

6. Un certain nombre de progrès ont pu être observés depuis 2010, qui doivent très certainement être mis en partie au crédit de la résolution antérieure de l'Assemblée. Selon une étude publiée par Transparency International en 2013 et consacrée aux seuls États membres de l'Union européenne, quatre d'entre eux (Luxembourg, Roumanie, Slovénie et Royaume-Uni) disposaient d'un cadre juridique de protection des donneurs d'alerte jugé « poussé », tandis que, sur les 23 autres États membres de l'UE[7], 16 prévoyaient une protection légale partielle des agents qui font état de malversations, les sept pays restants ne présentant qu'un cadre extrêmement limité, voire aucun cadre juridique[8]. Toutefois, même les cadres juridiques « poussés » n'étaient pas tous applicables aux agents du secteur public et du secteur privé.

7. Le Recueil des bonnes pratiques et principes directeurs du G20 pour la législation relative à la protection des donneurs d'alerte (« G20 Compendium of Best Practices and Guiding Principles for Legislation on the Protection of Whistleblowers »[9]), établi par l'OCDE et avalisé par le G20 lors de son sommet de Cannes en novembre 2011 dans le cadre du plan d'action de lutte contre la corruption du G20, préconise six principes directeurs applicables à la création et au réexamen d'un cadre juridique de la protection des donneurs d'alerte. Les États doivent veiller à ce que la législation :

(1) mette en place un cadre institutionnel clair et efficace pour protéger les agents contre toute mesure disciplinaire ou autre forme de discrimination lorsqu'ils révèlent de bonne foi et pour des motifs raisonnables certains actes soupçonnés de malversations ou de corruption aux autorités compétentes ;

(2) donne une définition précise du champ d'application des révélations protégées et des personnes protégées par la loi ;

(3) assure aux donneurs d'alerte une protection solide et complète ;

(4) définisse clairement la procédure applicable et les moyens prévus pour faciliter le signalement des actes soupçonnés de corruption et encourage l'utilisation de moyens protecteurs et aisément accessibles pour donner l'alerte ;

(5) garantisse la mise en place de mécanismes de protection efficaces, notamment en chargeant une instance spécifique, responsable et habilitée à recueillir des plaintes faisant état de mesures de rétorsion et/ou d'enquêtes insuffisantes et à mener des investigations à ce sujet, ainsi qu'en prévoyant un éventail complet de voies de recours ; et

(6) à ce que la mise en œuvre de la législation relative à la protection des donneurs d'alerte soit appuyée par une sensibilisation, une communication, une formation et une évaluation périodique de l'efficacité du cadre de la protection.

[7] La Croatie, qui a adhéré à l'UE en juillet 2013, ne figure pas encore dans cette étude.
[8] Transparency International, *Whistleblowing in Europe: Legal Protections for Whistleblowers in the EU* (2013) (en anglais).
[9] *G20 Study: Whistleblower Protection Frameworks, Compendium of Best Practices and Guiding Principles for Legislation* (en anglais).

8. Nous examinerons au cours du présent rapport, dans un premier temps, l'acquis du Conseil de l'Europe dans le domaine de la protection des donneurs d'alerte, notamment les travaux précédents de l'Assemblée, la jurisprudence de la Cour européenne des droits de l'homme et la récente recommandation du Comité des Ministres (CM). En présentant cette recommandation du CM, je proposerai quelques mesures supplémentaires que les États devraient envisager de prendre à la lumière des récentes évolutions, en vue d'améliorer la protection des donneurs d'alerte, indépendamment de leur domaine d'activité ou du statut public ou privé de leur employeur. Avant de tirer un certain nombre de conclusions, nous examinerons plus attentivement la situation des donneurs d'alerte qui travaillent dans le secteur de la sécurité nationale, en accordant une attention particulière au cas d'Edward Snowden.

2. L'acquis du Conseil de l'Europe : promouvoir les droits de l'homme et encourager le débat public grâce à la protection des donneurs d'alerte

2.1. Les travaux antérieurs de l'Assemblée parlementaire

9. Le Conseil de l'Europe a constamment et de manière cohérente salué la contribution des donneurs d'alerte au débat public sur les questions relatives aux droits de l'homme lorsqu'ils utilisaient en dernier ressort leurs révélations pour lutter contre l'impunité des actes de corruption et des autres graves violations des droits de l'homme.

10. Mon précédent rapport sur la « Protection des «donneurs d'alerte» » (Résolution 1729 (2010) et Recommandation 1916 (2010)) avait permis la réalisation d'un travail de fond sur cette question. L'Assemblée a admis que le fait de donner l'alerte était un moyen de mettre un terme aux malversations susceptibles d'être préjudiciables à autrui, une occasion de renforcer l'obligation de rendre des comptes et un instrument permettant d'intensifier la lutte contre la corruption et la mauvaise gestion dans le secteur public et le secteur privé. La résolution indiquait expressément que la législation relative aux donneurs d'alerte devait être applicable aux membres des forces armées et des services spéciaux. L'examen des maigres protections accordées à l'époque aux donneurs d'alerte dans les différents États a conduit à conclure qu'elles justifiaient la prise de mesures substantielles par les États, en vue de créer, renforcer et faire respecter la protection des donneurs d'alerte, dans le respect de certains principes directeurs.

11. L'Assemblée recommandait notamment que :

(1) la législation prévoie une protection efficace contre toute forme de mesures de rétorsion à l'égard des donneurs d'alerte de bonne foi, qui utilisent les voies internes existantes pour donner l'alerte ;

(2) lorsque les voies internes pour donner l'alerte n'existent pas, ne fonctionnent pas correctement ou ont raisonnablement peu de chances de fonctionner correctement étant donné la nature du problème dénoncé par le donneur d'alerte, il convient de protéger de la même manière celui qui utilise les voies externes, y compris les médias ;

(3) tout donneur d'alerte devrait être considéré comme un acteur de bonne foi, dès lors qu'il avait des motifs raisonnables de croire que les informations divulguées étaient exactes, même s'il s'avère par la suite que ce n'était pas le cas, et qu'aucun motif illicite ou contraire à l'éthique ne l'a poussé à agir par la suite ;

(4) il importe que les États veillent à l'existence de mécanismes répressifs satisfaisants pour enquêter sur les révélations et rechercher le moyen de remédier aux défaillances constatées ;

(5) le Conseil de l'Europe devrait donner l'exemple, en mettant en place son propre mécanisme d'alerte au sein de l'organisation.

12. L'Assemblée a par la suite adopté plusieurs autres résolutions et recommandations qui considèrent les donneurs d'alerte comme un moyen d'efficace de renforcer, notamment, la transparence de l'administration, le respect des droits de l'homme et la bonne gouvernance.

13. Dans sa Résolution 1838 (2011), « 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 » (rapporteur : Dick Marty, Suisse/ADLE), l'Assemblée a affirmé qu'un contrôle judiciaire et parlementaire adéquat du gouvernement et de ses agents était indispensable au respect de l'État de droit et de la démocratie, surtout par les services secrets. L'Assemblée soulignait que les informations relatives à la responsabilité des agents publics ayant commis de graves violations des droits de l'homme (par exemple des meurtres, des

disparitions forcées, des actes de torture, des enlèvements) ne devaient pas être protégées comme des secrets d'État légitimes. Le rapport examinait de façon assez précise les différentes enquêtes judiciaires et parlementaire menées par les États membres du Conseil de l'Europe, à la suite de la révélation de graves violations des droits de l'homme commises par la CIA, avec la complicité des services de plusieurs États européens, faites dans les rapports antérieurs de l'Assemblée parlementaire sur les prisons secrètes de la CIA et les « restitutions » de prisonniers[10]. L'Assemblée a observé que bon nombre d'États membres étaient dépourvus de surveillance parlementaire ou judiciaire de leurs services de sécurité et de renseignement ou que cette surveillance était foncièrement inadaptée. Elle appelait par conséquent à une protection adéquate des journalistes et de leurs sources[11] et des donneurs d'alerte[12], qui offraient un moyen de surveillance supplémentaire permettant de déceler et de prévenir les violations des droits de l'homme commises par les membres des services secrets.

14. Dans sa Résolution 1954 (2013), « La sécurité nationale et l'accès à l'information » (rapporteur : Arcadio Diaz Tejera, Espagne/SOC), l'Assemblée soulignait la nécessité de contrôler fermement les activités des services secrets, de protéger les révélations de bonne foi des « donneurs d'alerte » sur les méfaits commis et de faire primer « l'intérêt général », afin de garantir que le principe général de la libre accessibilité de toutes les informations détenues par les pouvoirs publics ne souffre pas d'exceptions excessivement étendues au titre de la « sécurité nationale ». Ce rapport traitait des problèmes posés par les informations révélant que des agents publics avaient commis de graves violations des droits de l'homme, telles que des meurtres, des disparitions forcées, des actes de torture ou des enlèvements, sans être tenus de répondre de leurs actes au motif que ceux-ci constituaient des « secrets d'État ». L'Assemblée indiquait qu'elle adhérait aux « Principes globaux sur la sécurité nationale et le droit à l'information » (les « Principes de Tshwane »[13]), qui comportent des éléments utiles sur la protection des donneurs d'alerte dans le cadre de la sécurité nationale, et prévoient notamment la nécessité de défendre vigoureusement l'intérêt général. Les « Principes de Tshwane », avalisés par l'Assemblée en 2013, étaient eux-mêmes inspirés de la première déclaration faite par l'Assemblée dans le rapport de 2011 établi par Dick Marty (Résolution 1838 (2011), voir plus haut), qui affirmait que les informations relatives à la responsabilité des agents publics ayant commis des violations des droits de l'homme ne devaient pas être protégées comme des secrets d'État légitimes.

2.2. La jurisprudence de la Cour européenne des droits de l'homme (la Cour)

15. La Cour a également énoncé les principes applicables à la protection de la liberté d'expression dans les affaires de donneurs d'alerte, y compris lorsque ceux-ci sont fonctionnaires, voire agents d'un service de renseignement national. Les nouvelles requêtes introduites devant la Cour contre les programmes de surveillance massive qui ont été révélés grâce aux fichiers Snowden sont toujours pendantes[14], mais les arrêts antérieurs offrent un excellent point de départ pour déterminer les principes fondamentaux du juste équilibre entre, d'une part, la liberté d'expression et d'information, surtout lorsqu'elle sert à dénoncer des faits répréhensibles, notamment des actes illicites et des violations des droits de l'homme et, d'autre part, l'obligation de maintenir le secret des informations liées à la sécurité nationale.

16. L'article 10 de la Convention européenne des droits de l'homme protège la liberté d'expression, qui comprend « la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques ». Dans son deuxième paragraphe, l'article 10 soumet l'exercice de ces libertés « à certaines formalités, conditions, restrictions ou sanctions prévues par la loi, qui constituent des mesures nécessaires, dans une société démocratique, à la sécurité nationale, à l'intégrité territoriale ou à la sûreté publique, à la défense de l'ordre et à la prévention du crime, à la protection de la santé ou de la morale, à la protection de la réputation ou des droits d'autrui, pour empêcher la divulgation d'informations confidentielles ou pour garantir l'autorité et l'impartialité du pouvoir judiciaire ».

---

[10] Voir « Allégations de détentions secrètes et de transferts interétatiques illégaux de détenus concernant des Etats membres du Conseil de l'Europe », Doc. 10957, Résolution 1507 (2006) et Recommandation 1754 (2006), et « Détentions secrètes et transferts illégaux de détenus impliquant des Etats membres du Conseil de l'Europe : second rapport », Doc. 11302, Résolution 1562 (2007) et Recommandation 1801 (2007), rapporteur dans les deux cas : Dick Marty, Suisse/ADLE).

[11] Recommandation 1950 (2011), « La protection des sources d'information des journalistes ».

[12] Résolution 1729 et Recommandation 1916 (2010), « Protection des «donneurs d'alerte» ».

[13] Disponible sur : http://www.opensocietyfoundations.org/publications/global-principles-national-security-and-right-information-tshwane-principles/fr.

[14] Voir l'affaire pendante *Big Brother Watch et autres c. Royaume-Uni*, requête n° 58170/13, affaire communiquée le 7 janvier 2014, et les autres affaires de la Cour européenne des droits de l'homme dans l'article de MTI-EcoNews/Hongrie du 29 novembre 2013, « *NGO to turn to Strasbourg court over security services' secret surveillance* ».

17. Dans l'affaire *Guja c. Moldova*,[15] la Cour européenne des droits de l'homme a utilisé un critère d'appréciation pour déterminer si l'ingérence de l'État dans la liberté d'expression du requérant (un donneur d'alerte) était conforme à l'article 10.2 de la Convention européenne des droits de l'homme et a finalement conclu à une violation. En l'espèce, le requérant avait adressé deux lettres qui n'étaient pas qualifiées de confidentielles au *Jurnal de Chişinău*, qui avait publié ces communications pour montrer que des responsables publics exerçaient des pressions sur les services répressifs. L'une de ces lettres était une note adressée par le vice-président du Parlement, M. Mişin, au service du procureur général ; la seconde avait été envoyée par le vice-ministre de l'Intérieur, M. A. Uraschi, à un substitut du procureur général, afin de faire pression sur le traitement par le ministère public des poursuites pénales engagées à l'encontre de quatre fonctionnaires de police, dont l'un était notamment accusé de mauvais traitements et de détention illégale. Le requérant et un autre procureur soupçonné d'avoir fourni les lettres au requérant avaient été révoqués, au motif que les lettres divulguées à la presse étaient secrètes et que le requérant n'avait pas consulté ses supérieurs avant de les révéler.

18. La Cour a conclu à la violation de l'article 10. Elle a tout d'abord estimé que « l'article 10 est applicable en l'espèce, même s'il [le requérant] n'est pas l'auteur des informations adressées au journal », puisque « la protection de l'article 10 s'étend à la sphère professionnelle en général et aux fonctionnaires en particulier », comme elle l'avait déclaré par le passé dans des affaires contre l'Allemagne, le Liechtenstein, le Royaume-Uni et l'Espagne[16]. Bien qu'elle reconnaisse l'existence d'un devoir de loyauté, de réserve et de discrétion des fonctionnaires envers leur employeur, la Cour considère que :

> « la dénonciation par [les agents de la fonction publique, qu'ils soient contractuels ou statutaires,] de conduites ou d'actes illicites constatés sur leur lieu de travail doit être protégée dans certaines circonstances. Pareille protection peut s'imposer lorsque l'agent concerné est seul à savoir – ou fait partie d'un petit groupe dont les membres sont seuls à savoir – ce qui se passe sur son lieu de travail et est donc le mieux placé pour agir dans l'intérêt général en avertissant son employeur ou l'opinion publique »[17].

19. La Cour avalise par conséquent l'idée que les révélations publiques devraient intervenir en dernier ressort, une fois que l'agent a consulté

> « son supérieur ou […] une autre autorité ou instance compétente. La divulgation au public ne doit être envisagée qu'en dernier ressort, en cas d'impossibilité manifeste d'agir autrement »[18].

20. En recourant à un critère d'appréciation qui comporte différents facteurs, la Cour est parvenue à la conclusion que l'ingérence de l'administration dans la liberté d'expression du requérant n'était pas proportionnée aux intérêts que l'administration cherchait à défendre. Premièrement, elle a vérifié si le requérant avait d'autres moyens de révéler ces éléments, ce qui n'était pas le cas puisque aucune législation ni réglementation nationale ne prévoyait en République de Moldova le signalement d'irrégularités par des agents. Deuxièmement, la Cour a apprécié la nature de l'intérêt général concerné par les informations divulguées, qu'elle a jugée en faveur du requérant, dans la mesure où la pratique de l'ingérence des responsables politiques dans la justice répressive était un sujet très largement abordé, dont le Président de la République de Moldova lui-même avait fait son cheval de bataille pendant sa campagne électorale, en préconisant le renforcement de l'indépendance de la justice. En concluant en ce sens, la Cour a également observé que

> « [l]'intérêt de l'opinion publique pour une certaine information peut parfois être si grand qu'il peut l'emporter même sur une obligation de confidentialité imposée par la loi »[19].

21. Troisièmement, la Cour a vérifié l'authenticité des informations divulguées, qui était établie. Quatrièmement, elle a apprécié l'éventuel préjudice subi par les pouvoirs publics par suite des révélations et a vérifié s'il était supérieur aux intérêts défendus par ces révélations. Bien qu'elle ait estimé que les lettres adressées au service du procureur général avaient fortement nui à la confiance des citoyens dans l'indépendance de l'institution, la Cour a estimé que l'intérêt général que représentait le fait d'être informé

---

[15] Requête n° 14277/04, arrêt du 12 février 2008.
[16] *Vogt c. Allemagne (*requête n° 17851/91, arrêt du 2 septembre 1995, paragraphe 53), *Wille c. Liechtenstein* (requête n° 28396/95, arrêt du 28 octobre 1999, paragraphe 41), *Babar Ahmed et autres c. Royaume-Uni (*requêtes n° 24027/07, 11949/08, 36742/08, 66911/09 et 67354/09, arrêt du 2 septembre 1998, paragraphe 56, et *Fuentes Bobo c. Espagne (*requête n° 39293/98, arrêt du 29 février 2000, paragraphe 38).
[17] Guja c. Moldova, requête n° 14277/04, arrêt du 12 février 2008, paragraphe 72.
[18] Ibid. paragraphe 73.
[19] Ibid. paragraphe 74.

des pressions excessives et des actes répréhensibles dont le pouvoir judiciaire était la cible était extrêmement important dans une société démocratique, considérant

> « qu'une libre discussion des problèmes d'intérêt public est essentielle en démocratie et qu'il faut se garder de décourager les citoyens de se prononcer sur de tels problèmes »[20].

22. Cinquièmement, la Cour a apprécié les motivations qui avaient poussé le requérant à divulguer ces informations et a observé qu'il avait agi de bonne foi. Enfin, sixièmement, la Cour a comparé la lourdeur de la peine à d'autres facteurs et a conclu que l'application de la peine maximale au requérant dissuaderait sérieusement d'autres agents de signaler une malversation.

23. De même, dans l'affaire *Heinisch c. Allemagne*[21], la Cour a affirmé que

> « l'intérêt général que représente le fait d'être informé sur la qualité des services publics prévaut sur la protection de la réputation d'une organisation ».

24. Mme Heinisch était devenue donneuse d'alerte en divulguant des informations sur les défaillances supposées des soins dispensés par l'établissement de santé publique dans lequel elle était infirmière. Par suite de cet acte, il avait été mis fin à son contrat de travail, ce que la Cour a considéré comme une ingérence dans la liberté d'expression de la requérante, garantie par l'article 10. Le deuxième paragraphe de cette disposition définit les cas dans lesquels l'État peut porter atteinte à l'exercice, par une personne, de sa liberté d'expression : premièrement, ces restrictions ou conditions doivent être « prévues par la loi » ; deuxièmement, elles doivent être « nécessaires, dans une société démocratique », pour les raisons énumérées par l'article. La Cour a conclu dans l'affaire Heinisch que, bien que le fait de mettre fin à une relation de travail sans avertissement soit effectivement « prévu par la loi », les informations divulguées en l'espèce par la requérante « présentaient indéniablement un intérêt public »[22] et semblaient authentiques. La Cour a estimé que la requérante avait suffisamment averti son employeur avant de porter plainte au pénal. La position de la Cour reflète l'adhésion ancienne du Conseil de l'Europe aux valeurs de transparence, liberté d'expression et d'information, obligation faite aux pouvoirs publics de rendre des comptes et lutte contre la corruption.

25. Dans l'affaire *Sosinowska c. Pologne*[23], qui concernait également le secteur de la santé[24], la requérante, spécialiste dans un hôpital, avait été licenciée pour avoir « exprimé des opinions négatives sur les compétences du médecin en chef », portant ainsi atteinte au « principe de solidarité professionnelle ». La Cour a conclu que la requérante avait été « sanctionnée essentiellement pour avoir fait part à d'autres employés du service, aux autorités hospitalières et au consultant régional de ses préoccupations au sujet de la qualité des soins médicaux dispensés aux patients sur l'ordre de son supérieur ». Les propos de la requérante portaient sur des questions « d'intérêt général »[25] ; ils relevaient par conséquent de sa liberté d'expression, garantie par l'article 10, et n'auraient pas dû entraîner des sanctions disciplinaires.

26. Dans l'affaire *Bucur et Toma c. Roumanie*[26], le premier requérant, qui travaillait pour les Services de renseignement roumains, avait révélé au cours d'une conférence de presse que ces services avaient illégalement mis sur écoute un grand nombre de journalistes, de responsables politiques et d'hommes d'affaires. Un membre de l'opposition, qui faisait partie de la commission parlementaire chargée du contrôle des services de renseignement, et que le requérant avait tout d'abord contacté, lui avait conseillé de rendre immédiatement ces informations publiques, parce qu'aucune mesure ne serait prise par la commission, dans laquelle le parti au pouvoir était majoritaire. Le requérant a été jugé coupable de violation de secret officiel. La Cour de Strasbourg a conclu que cette condamnation portait atteinte au droit du requérant à la liberté d'expression (article 10 de la Convention européenne des droits de l'homme), car ces poursuites n'étaient pas « nécessaires dans une société démocratique ». La Cour a souligné qu'au moment de la révélation de

---

[20] Ibid., paragraphe 91.
[21] Requête n° 28274/08, arrêt du 21 juillet 2011.
[22] Ibid., paragraphe 71.
[23] Requête n° 10427/09, arrêt du 18 octobre 2011.
[24] Les donneurs d'alerte jouent un rôle particulièrement important dans le domaine de la santé, où ils défendent les droits des patients face à de puissantes structures. Le Service national de la santé du Royaume-Uni (NHS) a connu d'importantes réformes grâce aux donneurs d'alerte qui avaient attiré l'attention sur de graves défaillances. Une enquête ordonnée par le gouvernement et menée par Sir Robert Francis, conseiller de la reine, a abouti, documents à l'appui, à un compte rendu « choquant » du traitement réservé aux donneurs d'alerte par le Service national de la santé (voir The Guardian, 11 février 2015, « *NHS whistleblowers ignored, bullied and intimidated, inquiry finds* » ; voir également la déclaration de Public Concern At Work du 11 février 2015.
[25] Ibid., paragraphes 79 et 83.
[26] Requête n° 40238/02, arrêt du 8 janvier 2013.

ces informations, les nouvelles dispositions légales qui prévoyaient le cadre juridique applicable aux donneurs d'alerte n'avaient pas encore été adoptées et le requérant n'avait pas d'autre moyen efficace de communiquer ces informations sur les abus des services de renseignement. Elle a également souligné que les révélations du requérant présentaient un intérêt général considérable, car elles concernaient les abus commis par des hauts responsables et touchaient aux fondements démocratiques de l'État. La Cour a également conclu à la violation du droit au respect de la vie privée (article 8 de la Convention européenne des droits de l'homme) des autres requérants (qui avaient été victimes de cette surveillance illégale).

27. Le plus récent des arrêts qui composent cette série renforçant la protection des donneurs d'alerte est celui qui a été rendu dans l'affaire *Matúz c. Hongrie*[27]. La Cour a conclu à l'unanimité que le licenciement d'un donneur d'alerte, journaliste de la télévision publique hongroise, qui avait été confirmé par les juridictions hongroises était constitutif d'une violation de l'article 10. Le requérant avait, en publiant un livre qui critiquait son employeur pour la censure alléguée qu'exerçait un directeur de cette entreprise publique, enfreint la clause de confidentialité de son contrat de travail.

28. La Cour a conclu que le licenciement avait été uniquement provoqué par la publication de l'ouvrage, sans qu'il soit tenu compte des capacités professionnelles du journaliste, et constituait ainsi une ingérence dans l'exercice de sa liberté d'expression. Cette ingérence n'avait pas été « nécessaire dans une société démocratique », car le requérant avait agi dans l'intérêt général, en attirant l'attention de l'opinion publique sur la censure pratiquée au sein de la télévision nationale. La Cour a tenu compte du fait que le requérant avait agi de bonne foi et que l'ouvrage avait été publié uniquement après que le requérant avait tenté en vain de se plaindre à son employeur de la censure alléguée. Elle a également observé que les juridictions nationales s'étaient prononcées contre le requérant uniquement parce que la publication de l'ouvrage n'avait pas respecté ses obligations contractuelles, sans prendre en compte l'argument qu'il avait avancé : il avait exercé sa liberté d'expression dans l'intérêt général.

2.3. La Recommandation (2014)7 du Comité des Ministres

29. En réponse au rapport consacré en 2010 par l'Assemblée à la protection des donneurs d'alerte, le Comité des Ministres (CM) a adopté la Recommandation CM/Rec(2014)7[28] aux États membres. La recommandation du CM reflète très largement la position exprimée par l'Assemblée dans sa Résolution 1729 (2010) et sa Recommandation 1916 (2010). Le Comité des Ministres a notamment reconnu que les États devaient adopter une législation complète applicable aux donneurs d'alerte, afin d'encourager et de protéger les mises en garde faites en toute bonne foi contre les diverses violations du droit, et notamment les violations des droits de l'homme. Il a conseillé à juste titre aux États d'adopter une « approche globale et cohérente pour faciliter les signalements et les révélations d'informations d'intérêt général »[29]. L'existence de dispositions éparpillées dans les différents domaines du droit risque en effet d'empêcher les éventuels donneurs d'alerte de bien comprendre les dispositions légales applicables à des situations précises.

2.3.1. Le champ d'application personnel et matériel

30. En recommandant aux États d'adopter une législation qui donne une définition claire du champ d'application des révélations et des personnes placées sous la protection de la loi, la recommandation du CM définit de manière plus complète que la résolution de l'Assemblée le champ d'application personnel de la protection des donneurs d'alerte. Elle s'applique aux personnes dans le cadre de leur « relation de travail », ainsi qu'aux personnes qui ont eu connaissance d'une menace ou d'un préjudice pour l'intérêt général « durant le processus de recrutement ou à un autre stade de la négociation précontractuelle » (paragraphes 3-4).

31. Le CM a néanmoins prévu une exception trop large pour les activités de renseignement. Le paragraphe 5 de la recommandation autorise l'application « d'un régime particulier ou de règles particulières, prévoyant notamment des droits et obligations modifés » aux informations « relatives à la sécurité nationale, à la défense, au renseignement, à l'ordre public ou aux relations internationales de l'Etat ». Mais la recommandation ne donne aucune définition de la « sécurité nationale ». Au vu des révélations faites par Edward Snowden, un cadre plus particulier devrait être élaboré pour les révélations liées à la sécurité nationale. L'existence de garanties est indispensable pour éviter que les services de renseignement ne dissimulent de graves violations des droits de l'homme en classant abusivement toutes les informations en la matière dans la catégorie des questions de « sécurité nationale ».

---

[27] Requête n° 73571/10, arrêt du 21 octobre 2014.
[28] Disponible sur : http://www.coe.int/t/dghl/standardsetting/cdcj/CDCJ%20Recommendations/CMRec(2014)7F.pdf.
[29] Annexe à la Recommandation (2014)7, paragraphe 7.

32. Au vu des « Principes de Tshwane » auxquels l'Assemblée a souscrit dans sa Résolution 1954 (2013)[30], il importe que les États définissent clairement dans leur législation les catégories étroites d'informations qui peuvent faire l'objet d'une rétention pour des raisons de sécurité nationale (principe 3(c)). Le principe 37 énumère les catégories d'actes répréhensibles qui présentent un grand intérêt pour les citoyens et que les agents publics devraient être autorisés à divulguer sans craindre de représailles. Ces actes dont la révélation est considérée comme une « divulgation protégée » sont les crimes, les violations des droits de l'homme et du droit humanitaire international, la corruption, les menaces pour la santé et la sécurité publiques, les dangers pour l'environnement, l'abus de fonction publique, l'erreur judiciaire, la mauvaise gestion ou le gaspillage des ressources, les mesures de rétorsion prises suite à la divulgation de l'une des catégories précitées d'actes répréhensibles et la dissimulation délibérée d'une situation relevant de l'une des catégories susmentionnées.

33. Le principe 10 énumère plusieurs catégories d'informations qui présentent un intérêt général particulièrement élevé et devraient par conséquent être déjà publiées en amont et ne jamais faire l'objet d'une rétention. Parmi elles figurent les informations relatives à de graves violations des droits de l'homme et du droit humanitaire international, les violations systématiques et répandues des droits à la liberté individuelle et à la sécurité, ainsi que les autres mauvais traitements. Il convient de noter que le principe 10 E (1) précise que « [l]e cadre légal général concernant toutes les formes de surveillance ainsi que les procédures à suivre pour autoriser la surveillance, sélectionner les cibles de surveillance et utiliser, partager, conserver et détruire les données interceptées, doivent être accessibles au public ».

34. Les « Principes de Tshwane » (principe 43) exigent surtout que les agents publics bénéficient d'une exception de « défense de l'intérêt public », même lorsqu'ils font l'objet de poursuites pénales ou civiles pour avoir fait des révélations qui n'étaient pas protégées par ces principes, dès lors que l'intérêt général présenté par la divulgation de l'information en question prévaut sur l'intérêt général qu'il y aurait à ne pas la divulguer.

35. Il convient par conséquent que les États ne prévoient pas de dispositions ou d'exceptions générales fondées uniquement sur le secteur d'activités dont fait partie le donneur d'alerte. Les agents des services de renseignement ou des entreprises privées chargées de ce type de mission peuvent être amenés, au même titre que les autres agents publics ou employés du secteur privé, à avoir connaissance d'actes répréhensibles graves dans le cadre de leurs relations de travail. Le caractère sensible des informations et le préjudice que pourrait causer leur révélation doivent être pris en compte pour déterminer si l'intérêt général de cette divulgation prévaut sur le risque de préjudice, mais le caractère confidentiel des informations ne saurait interdire d'emblée une divulgation protégée. Dans le cas contraire, les administrations pourraient se soustraire à toute forme de contrôle des citoyens, en classant abusivement ces informations.

2.3.2. Voies de signalement et de révélation d'informations et suites données à ces signalements et révélations

36. Le Comité des Ministres a intégré les principales propositions faites par l'Assemblée à propos des moyens adéquats qui permettent aux donneurs d'alerte de signaler et de révéler des informations relatives à des actes illégaux, dans le secteur public comme dans le secteur privé. Le CM énumère les différents moyens auxquels les donneurs d'alerte peuvent recourir, notamment le signalement interne au sein d'une organisation ou d'une entreprise, le signalement aux organes réglementaires publics, aux services répressifs et aux organes de contrôle compétents et la révélation publique d'informations. Le CM recommande également que les donneurs d'alerte soient « informé[s], par la personne à qui le signalement a été fait, de l'action entreprise pour y donner suite ». Il est clair que le but premier des donneurs d'alerte est de mettre un terme aux actes répréhensibles qu'ils révèlent. Les voies internes de signalement ne sont d'aucune utilité si aucune enquête en bonne et due forme n'est menée et si aucune mesure appropriée n'est prise pour remédier aux méfaits allégués. Il y a par conséquent lieu de se féliciter de cette disposition particulière.

37. Mais l'amélioration de ces dispositions reste possible. Premièrement, les personnes ou les instances qui traitent ces signalements doivent être véritablement indépendantes et habilitées à agir au vu des informations communiquées par les donneurs d'alerte. Comme l'indique le principe de Tshwane n° 39, les organismes de surveillance doivent être « indépendants, sur les plans institutionnel et opérationnel, du secteur de la sécurité et des autres autorités desquelles peuvent provenir des divulgations, ce qui inclut le pouvoir exécutif ». Il serait inutile de prévoir des voies internes de signalement si leur rôle se limitait à dissuader les éventuels donneurs d'alerte de se manifester. En pareil cas, les services placés sous l'autorité

[30] Voir plus haut le paragraphe 14.

de l'organe accusé d'actes répréhensibles utiliseraient cette procédure interne pour identifier et persécuter les donneurs d'alerte avant même qu'ils puissent effectivement signaler ces actes.

38. Deuxièmement, ces instances doivent avoir réellement la possibilité de donner suite aux signalements des donneurs d'alerte et de prendre des mesures pour y remédier. Il convient donc que les États envisagent d'intégrer le principe de Tshwane n° 39(B)(3), en vertu duquel « la loi doit garantir aux organismes indépendants de surveillance l'accès à toutes les informations utiles et leur confier les pouvoirs d'enquête nécessaires pour appuyer cet accès. Ces pouvoirs doivent inclure le pouvoir d'assignation et le pouvoir de demander un témoignage sous serment ou déclaration sur l'honneur ». Ce principe traduit de manière pertinente le but visé par les paragraphes 19 et 20 de la recommandation du Comité des Ministres : mener rapidement une enquête sur les informations signalées par les donneurs d'alerte et informer ces derniers des progrès de l'enquête.

2.3.3. Confidentialité

39. Le paragraphe 18 de la recommandation du Comité des Ministres concrétise de manière satisfaisante la proposition faite par l'Assemblée, qui souligne la nécessité de protéger l'identité du donneur d'alerte, sauf s'il consent à ce qu'elle soit dévoilée ou si sa divulgation s'avère indispensable pour écarter une menace imminente ou grave pour l'intérêt général.

2.3.4. Protection contre les mesures de rétorsion

40. Le fait de protéger les donneurs d'alerte contre les représailles qu'il pourrait subir non seulement encourage davantage de personnes à faire état d'informations relatives à de graves violations des droits de l'homme et autre malversations, mais protège également leur droit à un recours effectif, garanti par l'article 13 de la Convention européenne des droits de l'homme. Cet article prévoit en effet que

> « [t]oute personne dont les droits et libertés reconnus dans la présente Convention ont été violés, a droit à l'octroi d'un recours effectif devant une instance nationale, alors même que la violation aurait été commise par des personnes agissant dans l'exercice de leurs fonctions officielles ».

41. Les Principes de Tshwane (principe 41) recommandent également de protéger ceux qui divulguent des informations faisant état de malversations contre les mesures de rétorsion qu'ils pourraient subir. Cette protection s'applique aux poursuites engagées aussi bien au pénal qu'au civil pour la divulgation d'informations classifiées ou d'autres informations confidentielles.

42. Dans l'ensemble, le Comité des Ministres a suivi les recommandations faites par l'Assemblée pour protéger les donneurs d'alerte contre les mesures de rétorsion. La recommandation du CM énumère différentes formes de représailles, telles que « le licenciement, la suspension, la rétrogradation, la perte de possibilités de promotion, les mutations à titre de sanction, ainsi que les diminutions de salaire ou retenues sur salaire, le harcèlement ou toute autre forme de sanction ou de traitement discriminatoire », ce qui est suffisamment large pour englober tous les types possibles de mesures de rétorsion.

43. Je souscris également aux recommandations faites par le Comité des Ministres dans les paragraphes 11 et 22. Le paragraphe 11 précise que

> « [u]n employeur ne devrait pas pouvoir se prévaloir des obligations légales ou contractuelles d'une personne pour empêcher cette personne de faire un signalement ou une révélation d'informations d'intérêt général, ou pour la sanctionner pour cette action ».

44. Le paragraphe 22 part du principe que le donneur d'alerte ne devrait pas perdre le bénéfice de sa protection

> « au seul motif qu'[il] a commis une erreur d'appréciation des faits ou que la menace perçue pour l'intérêt général ne s'est pas matérialisée, à condition qu'elle ait eu des motifs raisonnables de croire en sa véracité ».

45. Cette position est conforme aux Principes de Tshwane, qui garantissent une protection contre les mesures de rétorsion au donneur d'alerte qui, d'une part, a « des motifs raisonnables de croire que les informations divulguées tendent à mettre en évidence des méfaits » qui entrent dans l'une des catégories concernées par la divulgation protégée et définies par le principe 37 et, d'autre part, utilise la voie de signalement (interne ou externe) adéquate.

46. Le Comité des Ministres n'a pas recommandé aux États d'amener les auteurs de mesures de rétorsion à risquer eux-mêmes une contre-attaque, en les exposant à une éventuelle action reconventionnelle de la part des donneurs d'alerte victimes de leurs méthodes. Cette menace serait selon moi un moyen d'efficace de dissuader les éventuels auteurs de représailles de passer à l'action.

47. Conformément au principe de Tshwane n° 41 D., le Comité des Ministres a recommandé que la charge de la preuve que le préjudice subi par le donneur d'alerte n'était pas motivé par un désir de représailles incombe à l'employeur ; mais il n'a pas précisé quel niveau de preuve était exigé pour ce faire. Le paragraphe 6.3. de la Résolution 1729 (2010) de l'Assemblée est plus précis, car il préconise que l'employeur soit tenu de démontrer « au-delà de tout doute raisonnable » que toute mesure prise à l'encontre d'un donneur d'alerte a été motivée par des raisons autres que l'acte de signalement effectué aux médias par ce dernier, autrement dit qu'elle n'a eu aucun lien avec ses révélations.

48. La recommandation du Comité des Ministres aurait dû, selon moi, préciser davantage les circonstances dans lesquelles les donneurs d'alerte peuvent recourir à des voies externes pour signaler des actes répréhensibles, ainsi que le degré de protection dont ils jouissent dans ce cas. Le CM préconise de prendre des mesures pour mettre en œuvre les voies de signalement internes et pour protéger les donneurs d'alerte, mais il ne précise pas quand et à quelles conditions un donneur d'alerte peut renoncer à utiliser les voies internes et recourir aux voies externes, en révélant des informations par exemple aux médias. La recommandation mentionne dans son paragraphe 24 que

> « [l]e fait que le lanceur d'alerte ait révélé des informations au public sans avoir eu recours au système de signalement interne mis en place par l'employeur peut être pris en considération lorsqu'il s'agit de décider des voies de recours ou du niveau de protection à accorder au lanceur d'alerte ».

49. Mais que se passe-t-il lorsqu'il n'était pas raisonnable d'attendre du donneur d'alerte qu'il utilise les voies internes, car elles ne fonctionnaient pas ou ne pouvaient raisonnablement pas être considérées comme une option viable pour le donneur d'alerte pour d'autres raisons, par exemple parce que les donneurs d'alerte qui avaient recouru auparavant à ces moyens avaient subi des mesures de rétorsion ou n'étaient pas parvenus à faire correctement prendre en compte leurs préoccupations ?

50. Dans son paragraphe 23, la recommandation du CM préconise ce qui suit :

> "[u]n lanceur d'alerte devrait pouvoir invoquer, dans le cadre d'une procédure civile, pénale ou administrative, le fait que le signalement ou la révélation d'informations ait été fait conformément au cadre national ».

51. Cela suppose que le pays concerné dispose réellement d'un cadre national applicable aux donneurs d'alerte. De plus, comme nous l'avons indiqué plus haut, la recommandation ne précise pas à quel moment les États devraient juger opportun qu'un donneur d'alerte utilise des voies externes de signalement. De fait, elle indique uniquement dans son paragraphe 17 que,

> « [e]n règle générale, le signalement interne et le signalement aux organes réglementaires publics, aux autorités de répression et aux organes de contrôle compétents devraient être encouragés,

sans mentionner les voies externes de signalement. Il est cependant prévisible que le cadre interne de signalement ne fonctionne pas dans certains cas, parce que l'organe chargé de recevoir ces signalements n'est pas indépendant ou compte des personnes qui risquent de se trouver en situation de conflit d'intérêts.

52. Les Principes de Tshwane donnent des orientations à suivre pour renforcer le cadre juridique de la protection (qui reste exceptionnelle) des révélations publiques. Il importe que la législation définisse clairement les conditions dans lesquelles cette protection est accordée.

53. Le principe 40 énonce que la législation devrait protéger les révélations faites aux citoyens sous certaines conditions. Il faut, d'une part, qu'elles satisfassent à au moins l'un des quatre critères prévus (les révélations faites en interne n'ont eu aucun succès ; les révélations faites en interne risquent d'entraîner la dissimulation des faits répréhensibles ; il n'existe aucun mécanisme interne de signalement ; seuls des révélations faites immédiatement à l'extérieur permettent d'écarter un danger de mort ou un risque pour la santé ou la sécurité des personnes). D'autre part, ces révélations doivent remplir deux conditions cumulatives : le donneur d'alerte doit, premièrement, divulguer uniquement la quantité d'informations raisonnablement nécessaire pour mettre en lumière les actes répréhensibles et, deuxièmement, avoir raisonnablement considéré que l'intérêt général qui commandait la révélation de ces informations était supérieur au préjudice qu'elle pouvait causer à ce même intérêt général.

54. Comme bon nombre d'États membres du Conseil de l'Europe ne disposent pas encore d'un solide cadre juridique de protection des donneurs d'alerte et comme l'indépendance réelle des mécanismes internes de signalement des commissions de surveillance qui ont été ou seront mis en œuvre reste à démontrer, une définition claire des conditions exceptionnelles dans lesquelles les donneurs d'alerte peuvent recourir à une divulgation publique des informations semble essentielle au renforcement des mesures de protection des donneurs d'alerte.

55. Enfin, j'aimerais rappeler l'observation faite par Mme Myers, l'experte auditionnée par la commission en juin dernier[31]. Au lieu de se demander si tel ou tel donneur d'alerte est un traître ou un saint, il vaudrait mieux vérifier si les destinataires des informations communiquées les ont appréciées à leur juste valeur et ont procédé à une enquête à leur sujet et si les responsables d'un préjudice éventuellement causé ont été amenés à répondre de leurs actes. Pour ce faire, il est primordial que les États veillent à l'existence d'organes de surveillance véritablement indépendants, mènent des enquêtes au sujet des révélations protégées et donnent les suites qui conviennent aux éléments signalés par les donneurs d'alerte, en assurant leur protection.

2.3.5. Conseil, sensibilisation et évaluation

56. Il y a lieu de se féliciter des deux points ajoutés par le Comité des Ministres dans sa recommandation par rapport aux propositions formulées par l'Assemblée dans sa Résolution 1729 (2010). Premièrement, le paragraphe 28 de la recommandation du CM préconise « […] de donner aux personnes qui prévoient de faire un signalement ou une révélation d'informations d'intérêt général un accès gratuit à des informations et à des conseils confidentiels ».

57. Par ailleurs, je souscris pleinement à la recommandation que les autorités nationales procèdent à l'évaluation périodique de l'efficacité de leur cadre national respectif applicable à la protection des donneurs d'alerte (paragraphe 29 de la recommandation du CM). Ces évaluations peuvent à l'évidence s'avérer bénéfiques pour les États et devraient prendre en compte les lignes directrices et bonnes pratiques disponibles, comme le Recueil des bonnes pratiques et principes directeurs du G20 pour la législation relative à la protection des donneurs d'alerte et les Principes de Tshwane.

58. Enfin, je partage également l'idée avancée par le Comité des Ministres au paragraphe 27 de sa recommandation : le cadre national de la protection des donneurs d'alerte « devrait faire l'objet d'une large promotion afin de développer les attitudes positives parmi l'opinion publique et les milieux professionnels, et de faciliter la révélation d'informations lorsque l'intérêt général est en jeu ». Comme l'indique le paragraphe 8 de la Résolution 1729 de l'Assemblée, les ONG peuvent jouer un précieux rôle complémentaire en favorisant la création d'un environnement propice aux révélations ou signalements publics d'informations.

3. Les révélations d'Edward Snowden : réévaluer les mesures de protection des donneurs d'alerte actuellement applicables aux acteurs du renseignement

59. À la lumière des faits nouveaux, et notamment des révélations faites par Edward Snowden, qui ont dévoilé l'étendue considérable des programmes de surveillance massive et de l'atteinte portée aux mesures de sécurité d'internet, il est indispensable de réévaluer les mesures de protection des donneurs d'alerte en vigueur, en vue de proposer les améliorations éventuellement nécessaires. La divulgation d'informations liées à la sécurité nationale est en général exclue des mesures de protection actuelle des donneurs d'alerte, même lorsque ces révélations peuvent s'avérer indispensables pour faire connaître et déceler les pratiques abusives des services secrets et amener leurs auteurs à répondre de ces actes.

60. Les fichiers communiqués par les journalistes avec l'aide de M. Snowden ont indéniablement contribué à la défense de l'intérêt général en dévoilant la nature et l'étendue des opérations massives de surveillance menées à travers le monde et les menaces que certaines pratiques font peser sur la sécurité d'internet. Dans le rapport qui portait sur « Les opérations massives de surveillance »[32], j'ai résumé les principales révélations qui donnaient une description des technologies complexes dont la NSA et les autres services de renseignement disposent et auxquelles ils recourent dans des proportions stupéfiantes pour

[31] Voir la Communication d'Anna Myers (en anglais), juriste et coordinatrice d'experts du Réseau international des donneurs d'alerte (Whistleblowing International Network) faite à l'occasion de l'audition « Améliorer la protection des donneurs d'alerte » de la commission des questions juridiques et des droits de l'homme de l'Assemblée parlementaire, 24 juin 2014.

[32] Doc. AS/Jur (1)2015 du 19 janvier 2015, adopté à l'unanimité par la commission des questions juridiques et des droits de l'homme le 26 janvier 2015 et inscrit à l'ordre du jour de la partie de session d'avril 2015 de l'Assemblée.

intercepter, analyser et conserver les communications des citoyens des cinq continents, sans que ceux-ci n'en soupçonnent l'existence ni ne soient soupçonnés d'aucun acte répréhensible.

61. Sans l'intervention de M. Snowden, nous ignorerions encore les différents programmes utilisés quotidiennement par les services de renseignement et qui portent atteinte à notre vie privée. Les révélations de M. Snowden nous ont permis de découvrir que la NSA pouvait enregistrer les communications téléphoniques d'un pays tout entier[33], accéder aux données à caractère personnel conservées par des sociétés internet de premier plan, avec ou sans leur consentement[34], mettre sur écoute le téléphone de la chancelière allemande, Mme Merkel, et de 121 autres chefs d'État et de gouvernement, voire espionner les Nations Unies, l'Union européenne et d'autres organisations internationales[35]. Certains de ces programmes ont été appliqués en collaboration avec des États alliés, tandis que d'autres les prenaient pour cible.

62. Bien que la confidentialité soit indispensable au bon fonctionnement des activités légales des services de renseignement, elle ne saurait être invoquée pour dissimuler des abus de pouvoir et assurer l'impunité des auteurs d'actes illégaux, qui portent atteinte au droit au respect de la vie privée et aux autres droits de l'homme en échappant au contrôle des mécanismes parlementaires et judiciaires de surveillance en place, dont le fonctionnement est notoirement entravé par la difficulté à accéder aux informations classées secrètes par ceux-là même qui s'opposent à leur divulgation. Les donneurs d'alerte qui travaillent pour le compte des services concernés offrent un moyen de déceler et de sanctionner les transgressions, ils représentent « l'épée de Damoclès » de la divulgation protégée des abus et assurent en pratique le respect des limites imposées à la surveillance par la loi. Il est révélateur de constater que ce point a été vigoureusement souligné lors de notre première audition d'avril 2014 par M. Hansjörg Geiger, ancien chef du BND allemand.

63. Pourtant, en vertu de la législation actuellement en vigueur aux États-Unis, M. Snowden tomberait sous le coup de chefs d'accusation extrêmement graves pour espionnage, sans pouvoir invoquer une exception d'intérêt général. À l'époque où les États-Unis renforçaient leur législation relative à la protection des donneurs d'alerte au profit des agents fédéraux et des employés du secteur privé (par exemple du secteur de la finance), au point que rares étaient ceux qui en étaient exclus dans le secteur privé, si tant est qu'il en eût, les agents des activités de renseignement se trouvaient en revanche dans une situation schizophrène. De 2008 à 2012, les entreprises privées chargées d'activités de renseignement pour le compte du Département de la Défense (DEA et NSA, pour lesquelles travaillaient des employés comme M. Snowden) bénéficiaient des droits de protection accordés aux donneurs d'alerte, comme le fait d'être jugé par un jury en vertu de la loi relative à la Défense nationale (National Defence Authorisation Act), mais ceux-ci ont été supprimés en 2013. Cette protection concernait cependant les mesures de rétorsion ou le traitement injuste subi de la part de l'employeur, mais ne s'appliquait pas aux poursuites pénales. De fait, le nombre de poursuites engagées à l'encontre des donneurs d'alerte a considérablement augmenté sous l'administration Obama, qui a mis en accusation un plus grand nombre d'auteurs de fuites – c'est-à-dire de personnes qui avaient révélé des informations à l'opinion publique américaine et qui correspondaient difficilement aux « espions » visés par la loi relative à l'espionnage adoptée au moment de l'entrée en guerre des États-Unis durant la première guerre mondiale – que toutes les administrations précédentes réunies[36].

64. Les diverses dispositions relatives à la protection des donneurs d'alerte mentionnées par l'Assemblée dans sa Résolution 1729 (2009) semblent n'être d'aucune utilité pour M. Snowden. La loi américaine relative à la protection des donneurs d'alerte de 1998 (Whistleblower Protection Act of 1998 – WPA) exclut expressément les agents de renseignement, tandis que la loi relative à la protection des donneurs d'alerte des activités de renseignement (Intelligence Community Whistleblower Protection Act – ICWPA), texte de loi distinct adopté au même moment, vise les agents de l'Agence centrale de renseignement, de l'Agence nationale de sécurité et des autres services de renseignement américains, ainsi que le personnel des entreprises privées travaillant pour le compte de ces agences et services, mais ne prévoit aucune véritable protection et n'incrimine pas les mesures de rétorsion. Elle légalise plutôt les révélations et autorise les donneurs d'alerte de la sécurité nationale à communiquer des informations classifiées à une entité

[33] Voir The Intercept du 19 mai 2014, *« Data Pirates of the Caribbean: the NSA Is Recording Every Phone Call in the Bahamas »*.
[34] Voir The Guardian du 6 septembre 2013, « *Revealed: how US and UK spy agencies defeat internet privacy and security »*.
[35] Voir The Guardian du 30 juin, 2014, *« New NSA leaks show how US is bugging its European allies »*.
[36] Voir The New York Times du 23 septembre 2013, *« Former F.B.I. Agent to Plead Guilty in Press Leak »*. Donald Sachtleben (FBI) a été la septième personne poursuivie pour fuites au cours de l'administration Obama, alors que seuls trois cas de ce type avaient donné lieu à des poursuites sous l'ensemble des présidences précédentes ; la dernière affaire en date concerne un agent, Jeffrey A. Sterling (CIA), jugé coupable d'espionnage pour avoir communiqué des documents au New York Times (voir : « *C.I.A. Officer Is Found Guilty in Leak Tied to Times Reporter* », The New York Times du 26 janvier 2015 (disponible sur : http://www.nytimes.com/2015/01/27/us/politics/cia-officer-in-leak-case-jeffrey-sterling-is-convicted-of-espionage.html?_r=1).

compétente (l'Inspection générale ou le Congrès des États-Unis, par l'intermédiaire du Département de la Justice), mais pas aux citoyens, et s'applique uniquement aux « préoccupations urgentes »[37]. L'instruction présidentielle générale 19 (PPD-19) du 10 octobre 2012 cherche à combler les lacunes du droit en protégeant les agents des activités de renseignement qui signalent des cas de « gaspillage, fraude, abus », mais uniquement les « agent[s] contractuel[s] qui travaillent pour le compte d'un élément des activités de renseignement ». Le texte est seulement applicable aux agents contractuels des entreprises privées et vise à les protéger contre les mesures de représailles prises sur le plan de l'habilitation en matière de sécurité et ne semble pas viser les agents qui signalent des violations des droits de l'homme. Cette instruction a force de loi, mais peut être annulée à tout moment par l'actuel Président ou ses successeurs.

65. Le 7 juillet 2014, le Président Obama a promulgué la « loi d'autorisation des activités de renseignement pour l'exercice 2014 » (Intelligence Authorization Act for Fiscal Year 2014), qui comporte une partie consacrée à la « Protection des donneurs d'alerte des activités de renseignement ». Cette disposition précise que les agents des services de renseignement qui divulguent à des entités désignées (par exemple leur supérieur hiérarchique, un inspecteur général ou les commissions du renseignement de la Chambre des représentants ou du Sénat) des informations sur d'éventuels actes répréhensibles commis au sein de leurs services seront protégés contre toute mesure de rétorsion. Pour la première fois, les agents des services de renseignement peuvent invoquer la protection de la loi en leur qualité de donneurs d'alerte s'ils subissent des représailles pour avoir coopéré dans le cadre d'une enquête ou avoir témoigné sous serment.

66. Bien que cette protection soit désormais codifiée sous forme de loi, elle n'existait pas à l'époque des révélations d'Edward Snowden et n'est toujours pas applicable aux entreprises privées sous contrat avec l'État, comme l'ancien employeur de M. Snowden. En outre, certains avocats s'inquiètent de ce que, dans la pratique, la loi pourrait ne pas atteindre les buts qu'elle poursuit, car ces voies internes de signalement pourraient servir en réalité à identifier et à sanctionner les éventuels donneurs d'alerte, au lieu de donner suite à leurs préoccupations. *Deutsche Welle* a indiqué que la nouvelle loi permettait aux donneurs d'alerte de saisir une commission administrative d'une demande de recours s'ils s'estimaient victimes de mesures de rétorsion à cause de leurs révélations ; mais ils n'ont aucun droit à être entendus en bonne et due forme par une instance indépendante et les membres de la commission sont tous choisis par le directeur du Service de renseignement national[38]. Qui plus est, les agents des services de renseignement ne bénéficient d'aucune protection en leur qualité de donneurs d'alerte s'ils ont signé un accord de confidentialité et leurs avocats n'ont pas accès aux éléments de preuve si ceux-ci sont classifiés.

67. Pourtant, les donneurs d'alerte restent pour les citoyens un moyen indispensable de connaître en dernier ressort les défaillances de l'obligation de rendre des comptes à l'échelon local, régional, national, voire international. Les fichiers Snowden ont révélé le manque criant de transparence et d'obligation démocratique de rendre des comptes au cours des différentes étapes de la procédure d'adoption et de mise en œuvre de la législation (lorsqu'elle existe) qui autorise les services de l'État à mener des opérations massives de surveillance. Le Haut-Commissaire des Nations Unies aux droits de l'homme, Mme Navi Pillay, a remercié M. Snowden d'avoir lancé un débat planétaire sur les pouvoirs de surveillance des États, en déclarant que « les personnes qui révèlent des violations des droits de l'homme devraient être protégées, car nous avons besoin d'elles »[39]. « Il nous a rendu un immense service en révélant ces informations » qui « vont exactement dans le sens de ce besoin de transparence et de consultation que nous préconisons ».

68. Le rapport de juin 2014 du Haut-Commissariat des Nations Unies aux droits de l'homme, « Le droit à la vie privée à l'ère du numérique », adopte une position analogue à celle du Conseil de l'Europe sur la nécessité d'encourager les donneurs d'alerte à signaler les violations des droits de l'homme, les actes de corruption et les fraudes. Il considère les programmes de surveillance massive qui recueillent des informations sur les courriers électroniques, les appels téléphoniques et les connexions internet de millions de citoyens ordinaires dans de nombreux États comme autant d'atteintes possibles au respect de la vie privée. Le rapport appelle l'ensemble des pouvoirs, ainsi que les institutions civiles totalement indépendantes, à prendre part au contrôle des programmes de surveillance, afin de veiller à ce que les droits garantis aux citoyens en ligne soient les mêmes que les droits hors ligne. Dans les États où les mécanismes de contrôle des programmes de surveillance sont limités, inexistants ou insuffisamment transparents, les divulgations protégées effectuées par les donneurs d'alerte jouent un rôle inestimable dans le contrôle des pouvoirs des services de sécurité et garantissent que les graves atteintes aux droits de

[37] Par exemple « un problème grave ou flagrant, un abus, une violation de la législation ou de la réglementation, une défaillance du financement de l'administration ou des opérations des activités de renseignement qui concernent des informations classifiées, mais ne s'applique pas aux divergences d'opinions qui ont trait aux questions de politique publique », « loi relative à la protection des donneurs d'alerte des activités de renseignement », article (g)(1)(A).
[38] Voir Deutsche Welle du 10 juillet 2014, *« Whistleblower law expands protection to US intelligence agents »*.
[39] The Guardian du 16 juillet 2014, *« Edward Snowden should not face trial, says UN human rights commission »*

l'homme commises par les agents de l'État ne seront pas abusivement dissimulées derrière le prétexte du « secret d'État ».

69. Le cas de John Kiriakou, qui est à ce jour le seul agent de la CIA à avoir été placé en détention à cause des méthodes de torture utilisées dans le cadre de la « guerre contre le terrorisme », qui ont été décrites en détail dans un rapport publié récemment par le Sénat américain[40], est édifiant : M. Kiriakou a été placé en détention pour avoir donné l'alerte sur les « méthodes d'interrogatoire », telles que la torture par l'eau (waterboarding), qu'il ne supportait plus. Le message qu'il a adressé depuis sa prison et que son avocate, Mme Jesselyn Radack, elle-même donneuse d'alerte au Département américain de la Justice, a lu par liaison vidéo en direct lors de la réunion de la commission du 29 janvier 2015[41] est profondément émouvant.

70. À la suite des révélations d'Edward Snowden et d'autres donneurs d'alerte, certains États ont apporté des modifications à la législation, en vue de dissuader le fait de donner l'alerte, au lieu de l'encourager. En Australie, par exemple, la nouvelle législation en matière de sécurité adoptée en septembre 2014[42] équivaut à une répression énergique des donneurs d'alerte, qui pourrait également concerner les journalistes. Les dispositions en question étendent en effet les pouvoirs de l'Organisation australienne de renseignement pour la sécurité (Asio) et prévoient une nouvelle infraction passible de cinq ans d'emprisonnement pour « toute personne » divulguant des informations relatives à des « opérations spéciales de renseignement ». Ces faits sont passibles de 10 ans d'emprisonnement si les informations divulguées « mettent en danger la santé ou la sécurité d'une personne ou nuisent au bon déroulement d'une opération spéciale de renseignement ».

71. Ces mesures sont contraires à la position prise par l'Assemblée en faveur de la transparence, qui a été réaffirmée dans la Résolution 1954 (2013), « La sécurité nationale et l'accès à l'information ». Dans l'esprit des Principes de Tshwane avalisés par l'Assemblée dans sa Résolution, j'encourage tous les États à réfléchir à la mise en place d'une exception « de défense de l'intérêt public ». Selon le principe de Tshwane n° 43, le personnel public qui fait l'objet de poursuites pénales, civiles ou administratives pour avoir révélé des informations qui ne sont pas considérées comme des divulgations protégées devrait avoir la possibilité de soulever une exception de défense de l'intérêt public sous certaines conditions. Pour vérifier le bien-fondé de cette exception, le ministère public et les tribunaux doivent examiner :

(1) si l'étendue de la divulgation était raisonnablement nécessaire pour révéler ces informations d'intérêt général ;

(2) la portée et la probabilité du préjudice causé à l'intérêt général par la divulgation ;

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

(4) si la personne a tenté de procéder à une divulgation protégée par le biais de procédures internes et/ou auprès d'un organisme indépendant de surveillance et/ou au public, en conformité avec les procédures qui régissent la protection des donneurs d'alerte ; et

(5) l'existence de circonstances impérieuses qui justifiaient la divulgation.

72. Soulignons que le « personnel public » désigne non seulement les agents publics, mais également les employés des sociétés privées sous contrat avec l'État ou de leurs sous-contractants[43].

[40] Voir par exemple le site Web du Projet Sécurité nationale de l'ACLU sur http://www.thetorturereport.org/

[41] « *A law meant for spies is being used against whistleblowers* »] ; l'épreuve subie par M. Kiriakou, Mme Radack et M. Drake (ancien haut fonctionnaire de la NSA, voir paragraphe 86) a fait l'objet d'un documentaire télévisé (« *SILENCED – the war on whistleblowers* »)

[42] Voir The Guardian, 26 septembre 2014, « *Security laws pass Senate amid fears over 'draconian' limits to press freedom* ». « La législation relative à la sécurité nationale autorise le placement en détention des donneurs d'alerte et confère à l'Asio des pouvoirs extrêmement étendus pour recueillir les données en ligne ».

[43] Ou plus précisément « les personnes employées par des organismes non gouvernementaux qui sont la propriété ou sous le contrôle du gouvernement, ou bien qui servent en tant qu'agents du gouvernement, ainsi que les employés des entités privées ou autres qui assurent des fonctions ou des services publics, ou opèrent avec des fonds ou des bénéfices publics conséquents, mais uniquement dans le cadre de l'exercice de ces fonctions, de la prestation des services ou de l'utilisation des fonds ou bénéfices publics » (Principes de Tshwane, Définitions).

4. Les voies internes prévues par le Conseil de l'Europe pour donner l'alerte : un exemple à suivre ?

73. À la suite de la Recommandation 1916 (2010) de l'Assemblée, le Secrétaire Général du Conseil de l'Europe a promulgué l'Arrêté n° 1327 du 10 janvier 2011 relatif à la vigilance et à la prévention en matière de fraude et de corruption. Ce texte fait obligation aux membres du Secrétariat Général « de signaler au /à la Directeur/rice général/e de l'administration ou au/à la Directeur/trice de l'audit interne et de l'évaluation toute conduite dont ils ont des raisons plausibles de croire qu'elle constitue un fait de fraude ou de corruption »[44]. Il y a lieu de se féliciter de la création de cette voie interne de signalement, qui constitue une avancée en direction du renforcement de la transparence et de la gouvernance au sein même du Conseil de l'Europe.

74. L'Arrêté n° 1327 vise tous les agents du Conseil de l'Europe, quel que soit leur rang, mais également les fonctionnaires hors cadre et les personnes qui interviennent dans les activités de l'Organisation de diverses manières (y compris les juges de la Cour européenne des droits de l'homme, le Commissaire aux droits de l'homme, les stagiaires, les experts, les consultants et les employés de sociétés extérieures sous contrat avec le Conseil)[45]. La comparaison de ce texte et des lignes directrices de la Commission européenne relatives à la transmission d'informations en cas de dysfonctionnements graves (« whistleblowing ») (SEC(2012) 679) montre toutefois que des améliorations peuvent encore être apportées à la réglementation interne du Conseil de l'Europe.

75. Premièrement, les lignes directrices du Conseil de l'Europe ne précisent pas si, et à quelles conditions, la protection contre les mesures de rétorsion est également applicable aux cas dans lesquels les donneurs d'alerte recourent à des voies externes de signalement pour faire état de soupçons raisonnables de fraude ou de corruption. Les dispositions de la Commission européenne prévoient que les agents signalent, en premier lieu, les graves irrégularités dont ils ont connaissance à leur supérieur immédiat, au directeur général ou au chef de service. En deuxième lieu, si le donneur d'alerte craint de faire l'objet de représailles, il est autorisé à signaler directement au Secrétaire général de la Commission ou à l'Office européen de lutte antifraude (OLAF) les faits en question. Troisièmement, en dernier ressort, les agents peuvent utiliser une voie de signalement externe. Lorsque le signalement interne est remis à l'OLAF ou au Secrétaire général, ce dernier doit indiquer au donneur d'alerte le temps nécessaire pour prendre les mesures qui s'imposent dans un délai de 60 jours. Si aucune mesure n'est prise dans ce délai ou si le donneur d'alerte peut démontrer que le temps indiqué est déraisonnable au vu de l'ensemble des circonstances de l'affaire, il est habilité à faire usage de sa possibilité de donner l'alerte par une voie externe, comme le prévoit le règlement du personnel de la Commission. Par ailleurs, si « ni la Commission, ni l'OLAF n'a pris de mesures adéquates dans un délai raisonnable, l'agent qui signale l'acte répréhensible a le droit de porter ses préoccupations à l'attention du Président, soit du Conseil, soit du Parlement, soit encore de la Cour des Comptes européenne, ou à l'attention du Médiateur » ; la protection accordée au donneur d'alerte reste applicable en pareil cas.

76. Le Conseil de l'Europe devrait, selon moi, envisager de préciser, d'une part, le délai dans lequel une réponse doit être donnée au donneur d'alerte et, d'autre part, les conditions dans lesquelles un donneur d'alerte peut recourir à une voie externe pour signaler des irrégularités. L'importance que peuvent avoir ces voies externes est souligné par le fait que le/la Directeur/rice général/e de l'administration, qui est l'une des personnes susceptibles d'être saisies dans le cadre du mécanisme de signalement interne prévu, risque de se trouver dans une situation de conflit d'intérêts si le signalement concerne des abus financiers ou administratifs.

77. Par ailleurs, l'article 4(3) demande que le signalement d'irrégularités soit « si possible, étayé par des informations et des documents fiables », ce qui pourrait soumettre le donneur d'alerte à une obligation excessive. La Commission se montre plus accommodante, puisqu'« il ne sera pas attendu des agents qu'ils démontrent l'existence de l'acte répréhensible et ils ne perdront pas la protection qui leur est accordée uniquement parce que leur honnête préoccupation s'est finalement avérée dépourvue de fondement »[46]. Cette position se rapproche des Principes de Tshwane, qui énoncent dans leur principe 38 que « [l]'auteur d'une divulgation protégée ne doit pas être contraint de fournir des données probantes ou de porter la responsabilité de la preuve en relation avec la divulgation ».

[44] Arrêté n° 1327, article 4.
[45] Arrêté n° 1327 (10 janvier 2011), article 2.
[46] Communication à la Commission européenne SEC(2012) 679, 6 décembre 2012 – Communication du vice-président Šefčovič à la Commission sur les lignes directrices relatives à la transmission d'informations en cas de dysfonctionnements graves ("Whistleblowing"), paragraphe 3.

78. Enfin, les lignes directrices du Conseil de l'Europe autorisent les membres du Secrétariat Général, lorsqu'ils ont un doute sur le fait qu'un acte soit ou non constitutif de fraude ou de corruption, de demander conseil auprès du/de la Directeur/rice général/e de l'administration ou du/de la Directeur/trice de l'audit interne et de l'évaluation[47]. Selon la Commission européenne, en revanche, l'expérience montre qu'il vaut mieux que ces conseils préalables soient dispensés par un point de contact sans lien avec une fonction d'enquête[48]. Comme les directeurs prennent part au processus d'enquête ultérieur, le Conseil de l'Europe devrait également envisager de confier les fonctions de conseil à une autre instance indépendante.

79. Cela dit, le témoignage donné devant la commission des questions juridiques et des droits de l'homme le 29 janvier 2015 par Maria Bamieh, ancienne procureur britannique détachée auprès d'Eulex au Kosovo[49], montre que les meilleures lignes directrices ne suffisent pas à empêcher que l'alerte donnée par une personne ne se transforme pour elle en rude épreuve, tant que la culture institutionnelle dominante n'appréciera pas à sa juste valeur la contribution des donneurs d'alerte. Comme l'enquête sur l'affaire de Mme Bamieh, prévue par les lignes directrices de la Commission, est toujours en cours[50], je préfère ne pas entrer davantage dans les détails à ce stade.

5. Vers une convention visant à renforcer la protection des donneurs d'alerte en Europe et au-delà

80. Comme l'indiquait la recommandation antérieure de l'Assemblée sur la protection des donneurs d'alerte, et au vu des faits nouveaux récemment survenus, j'aimerais encourager les États à s'engager dans la voie de l'élaboration d'un instrument juridique contraignant, afin d'améliorer encore la protection des donneurs d'alerte. Bien que l'intitulé initial de la proposition sur laquelle se fonde le présent rapport penche en faveur d'un protocole additionnel à la Convention européenne des droits de l'homme sur la protection des donneurs d'alerte[51], j'opterais pour une convention distincte, négociée sous les auspices du Conseil de l'Europe, qui n'exigerait pas, contrairement à un protocole additionnel à la Convention européenne des droits de l'homme, la ratification de l'ensemble des États parties. Cette convention-cadre, qui serait complétée et mise en œuvre par la législation nationale, pourrait tenir compte de la diversité des ordres juridiques des États membres du Conseil de l'Europe. Elle devrait être conçue pour accorder aux éventuels donneurs d'alerte une protection légale équivalente, quel que soit le pays dans lequel ils vivent et font leurs révélations. La convention pourrait prolonger et amplifier l'acquis reflété par la recommandation du CM. Son principal avantage serait son caractère juridiquement contraignant, mais cette convention pourrait également être ouverte aux États non européens pour lesquels elle présenterait un intérêt et contribuer ainsi à promouvoir la bonne gouvernance et à restaurer la confiance des citoyens de manière globale.

81. Au cours du processus de rédaction, des enseignements pourraient être tirés des événements récents, notamment lorsque l'alerte est donnée dans le domaine de la sécurité nationale. En outre, les États pourraient envisager d'accorder un droit d'asile aux donneurs d'alerte, surtout lorsqu'ils divulguent des informations sensibles au sujet d'un État qui concernent également d'autres États, et éventuellement lorsqu'ils résident dans un autre État encore. Notre experte, Mme Anna Myers, a expliqué au cours de son audition par la commission en juin 2014 dans quelle mesure la protection transfrontière des donneurs d'alerte est indispensable dans le monde interdépendant actuel. La situation de M. Snowden est un cas d'espèce, car il est particulièrement difficile de garantir que les préoccupations dont il a fait état, qui présentent un intérêt pour de nombreux pays, font l'objet d'une enquête en bonne et due forme, surtout s'il devait être extradé vers les États-Unis, où il aurait à faire face à de graves chefs d'accusation sans pouvoir soulever l'exception d'intérêt général.

82. Indépendamment de la durée inévitable du processus de négociation d'une convention sur la protection des donneurs d'alerte, j'aimerais inviter instamment les États à octroyer l'asile à tout donneur d'alerte de bonne foi, qui satisfait aux critères de la protection des donneurs d'alerte applicables dans l'État saisi d'une demande d'asile et qui est menacé de mesures de rétorsion dans son propre pays. Il s'agit ici évidemment de savoir si Edward Snowden remplirait les conditions nécessaires pour bénéficier de la protection accordée au donneur d'alerte en vertu des normes préconisées ci-dessus.

---

[47] Arrêté n° 1327 (10 janvier 2011), article 4(4).
[48] Communication à la Commission européenne SEC(2012) 679, 6 décembre 2012 – Communication du vice-président Šefčovič à la Commission sur les lignes directrices relatives à la transmission d'informations en cas de dysfonctionnements graves ("Whistleblowing"), paragraphe 5.
[49] Voir le communiqué de presse du 30 janvier 2015, « *A law meant for spies is being used against whistleblowers* ».
[50] Conformément à la décision prise par la commission le 29 janvier 2015, j'ai demandé à la Haute représentante de l'Union européenne pour les affaires étrangères, qui supervise Eulex, un certain nombre d'explications d'ordre institutionnel, mais je n'ai pas encore reçu de réponse, ce qui peut se comprendre.
[51] Voir plus haut, paragraphe 3.

6. Un cas d'espèce : Edward Snowden

83. J'aimerais à présent examiner si les révélations d'Edward Snowden réunissent les conditions nécessaires à la protection accordée aux donneurs d'alerte, conformément aux principes énoncés ci-dessus.

84. La première question qui se pose est celle de l'authenticité des informations divulguées et du fait qu'elles concernent des « méfaits ». Les gouvernements n'ont ni nié, ni confirmé l'existence de bon nombre des techniques de surveillance décrites dans les fichiers divulgués par M. Snowden. Mais il n'a jamais été démontré que ces informations étaient fausses ou trompeuses au point que leur authenticité et leur véracité soient sérieusement mises en doute. Par ailleurs, les activités de surveillance de la NSA révélées par M. Snowden pourraient fort bien être constitutives de violations des droits de l'homme ou d'abus d'autorité publique[52]. Dans mon rapport sur « Les opérations massives de surveillance », j'ai expliqué de manière assez détaillée pourquoi ces programmes portaient notamment atteinte au droit au respect de la vie privée[53]. Même s'il s'avère que tous les programmes de surveillance de la NSA avaient un fondement légal, y compris ceux qui concernaient des citoyens américains qui n'étaient pourtant soupçonnés d'aucun acte répréhensible, M. Snowden avait au moins « des motifs raisonnables de croire que les informations divulguées tendent à mettre en évidence des méfaits […] »[54]. M. Snowden n'est pas le seul à penser que les programmes de surveillance massive de la NSA peuvent être contraires à la Constitution des États-Unis : un juge fédéral au moins est parvenu à la même conclusion[55]. Plus récemment, en janvier 2015, le Tribunal des pouvoirs d'investigation du Royaume-Uni a conclu, dans l'affaire dont il était saisi par Liberty and Privacy International, que les accords secrets d'échange des données de renseignement passés entre le Royaume-Uni et les États-Unis, c'est-à-dire les programmes Prism et Upstream (divulgués avec l'aide d'Edward Snowden), n'avaient pas été conformes à la législation relative aux droits de l'homme (notamment aux articles 8 et 10 de la Convention européenne des droits de l'homme) pendant sept ans, parce que les dispositions internes et les garanties censées assurer le respect de la vie privée des citoyens avaient été tenues secrètes[56].

85. En deuxième lieu, il s'agit d'examiner si les révélations faites réunissent les conditions nécessaires à leur protection, malgré le fait que M. Snowden ait choisi de révéler publiquement ces informations, au lieu de s'en tenir aux voies internes de signalement. Il a communiqué les fichiers électroniques confidentiels qu'il avait copiés, parce qu'il y avait eu accès en sa qualité d'agent contractuel de la NSA, avec un petit nombre de journalistes choisis en fonction de leur réputation de personnes fiables et responsables. Selon les principes énoncés par l'Assemblée[57], les révélations faites par un donneur d'alerte aux citoyens peuvent être protégées uniquement si elles ont eu lieu en dernier ressort et qu'il a cherché à faire état de ses préoccupations par les voies internes.

86. Au cours de son audition par la commission en juin 2014, M. Snowden a expliqué qu'il avait fait part de ses préoccupations au sujet des programmes de surveillance massive de la NSA à ses collègues et supérieurs, à la fois oralement et par courrier électronique. Il a indiqué que les collègues auxquels il avait expliqué certains nouveaux programmes de surveillance avaient été choqués par ces précisions, mais n'y avaient pas donné suite. La réponse qui lui avait été donnée était que le système n'était pas prévu pour résoudre les problèmes, mais pour les enterrer. Par ailleurs, M. Snowden avait constaté après un examen attentif des faits que les donneurs d'alerte qui s'étaient déjà manifestés au sein de la NSA et avaient persisté à utiliser les voies internes de signalement n'avaient bénéficié d'aucune protection. Ils avaient au contraire subi diverses formes de représailles. M. Thomas Drake, qui avait communiqué à un journal des fichiers non classifiés après avoir signalé en vain par les voies internes le gaspillage d'1,2 milliards USD consacrés à un programme inefficace, avait finalement été poursuivi au pénal. M. William Binney avait également utilisé les voies officielles, ce qui lui avait uniquement valu de voir l'inspecteur général auquel il s'était adressé communiquer son nom au Département de la Justice, qui avait engagé des poursuites pénales à son encontre au titre de la loi relative à l'espionnage. Ces donneurs d'alerte de la NSA n'étaient pas parvenus

[52] Voir les Principes de Tshwane (note 13), principe 37 (b), (g).
[53] Voir Doc. *** (2015) (rapport sur les opérations massives de surveillance), paragraphes 79 à 94.
[54] Voir les Principes de Tshwane (note 13), principe 38 (a) (i).
[55] Le juge fédéral Richard Leon a qualifié en décembre 2013 la collecte des métadonnées faite par la NSA de « technologie quasi-orwellienne » sans doute contraire au Quatrième Amendement (voir Volz, « *The NSA's mass surveillance programme is about to go on trial* », 4 novembre 2014, disponible sur : http://www.nationaljournal.com/tech/the-nsa-s-mass-surveillance-program-is-about-to-go-on-trial-20141103 ; et Doc. *** (2015) (rapport sur les opérations massives de surveillance), paragraphe 70.
[56] Décision disponible sur le site Web du Tribunal des pouvoirs d'investigation ; voir The Guardian du 6 février 2015, « *Trust us' mantra undermined by GCHQ tribunal judgment* ». Cette décision conclut à la non-conformité des accords d'échange d'informations des services de renseignement entre le Royaume-Uni et les États-Unis avec la législation relative aux droits de l'homme.
[57] Voir, par exemple, les Principes de Tshwane (note 13), principes 38 à 40.

par ailleurs à déclencher un vaste débat sur la question. Comme ils n'avaient pas veillé à conserver des éléments de preuves documentaires à l'appui de leurs affirmations, ils avaient été traités de menteurs. Ces exemples avaient convaincu M. Snowden que, pour espérer voir ses démarches aboutir, il ne disposait d'aucune voie viable de signalement des faits en question au sein de l'agence.

87. La NSA a contesté ces assertions, en affirmant que M. Snowden n'avait pas fait part de ses préoccupations à ses supérieurs. Or, l'agence a refusé de divulguer les communications envoyées par M. Snowden depuis son compte à la NSA, à l'exception d'un seul courrier électronique, dans lequel M. Snowden demandait des éclaircissements au sujet de la législation régissant les activités de la NSA, sans mentionner la collecte des données en vrac ni les préoccupations que lui inspiraient les atteintes au respect de la vie privée. Un journaliste a fait, au titre de la loi relative à la liberté de l'information (Freedom of Information Act – FOIA), une demande de communication des courriers électroniques envoyés par M. Snowden depuis son compte à la NSA au cours des cinq premiers mois de 2013. Mais la NSA lui a répondu qu'elle ne pouvait pas communiquer les courriers électroniques envoyés par M. Snowden, car cette démarche porterait atteinte « à sa vie privée », dont le respect est garanti par la sixième exception prévue par la loi relative à la liberté de l'information, qui permet de refuser la communication d'informations constitutives d'une « atteinte clairement injustifiée à la vie privée »[58]. La NSA a également justifié son refus de communiquer ces messages par le fait qu'ils étaient recueillis par les services répressifs et que leur publication nuirait à la bonne marche de la procédure, qu'ils risquaient de révéler l'identité de sources confidentielles et qu'ils divulgueraient les techniques et les méthodes employées par les services répressifs. M. Snowden a rétorqué que la publication par la NSA d'un unique courrier électronique représentait « à l'évidence une communication d'informations adaptée aux besoins de la NSA et incomplète », qui ne reflétait en rien les multiples préoccupations dont il avait fait part à la NSA à de nombreuses reprises, par écrit et oralement.

88. La NSA a adopté une attitude tout aussi floue face à l'augmentation exponentielle des demandes qui lui ont été adressées au titre de la loi relative à la liberté d'information à la suite des révélations faites par M. Snowden. Depuis le 6 juin 2013, l'agence a reçu plus de 5200 demandes de publication d'informations classifiées ; au cours de la même période, l'année précédente, seules 800 demandes de ce type lui avaient été adressées. Selon The Guardian[59], la NSA a refusé de faire droit aux demandes des particuliers qui voulaient savoir si l'agence conservait leurs métadonnées, en leur faisant une réponse de Normand, tout en soulignant la légalité des programmes de surveillance. Ce manque persistant de transparence qui entoure les programmes de surveillance rend le rôle des donneurs d'alerte crucial, car ils représentent la seule source d'information qui permette de vérifier que les services de renseignement agissent dans le cadre de la loi. En résumé, il semblerait que M. Snowden n'ait eu d'autre voie de signalement interne que ses tentatives de faire part de ses préoccupations à ses collègues et supérieurs immédiats.

89. Par ailleurs, pour que les informations divulguées publiquement par M. Snowden puissent bénéficier d'une protection, il faut qu'il ait uniquement révélé la quantité d'informations raisonnablement nécessaire pour mettre en lumière les actes répréhensibles en question et qu'il ait raisonnablement considéré que l'intérêt général que présentaient les informations révélées prévalait sur le préjudice que ces révélations pouvaient causer à l'intérêt général[60].

90. S'agissant du premier point, le fait que M. Snowden ait dû agir en étant extrêmement pressé par le temps complique l'appréciation de la situation. Après avoir accédé aux données sensibles en question, il risquait d'être démasqué par la NSA et, par voie de conséquence, de ne plus être en mesure de prouver ses affirmations. Il était obligé de quitter les États-Unis. En partant, il ne savait pas encore quel pays finirait par lui accorder sa protection. Mais il était conscient du fait que les données qu'il avait copiées en vrac ne pouvaient être publiées intégralement, et encore moins tomber entre les mains des services d'une puissance étrangère, sans nuire à la sécurité nationale. Lors de ses deux auditions par la commission en avril et juin 2014, Edward Snowden s'est présenté comme un patriote américain, désireux de défendre la Constitution des États-Unis et le respect de la vie privée des citoyens, y compris à l'extérieur du territoire américain. Il n'avait en aucun cas l'intention de compromettre les intérêts légitimes de la sécurité nationale ni de venir en aide aux ennemis de la liberté. Afin d'atténuer au maximum ce risque, il avait pris des dispositions avec des journalistes responsables et dignes de confiance, qui travaillaient pour des « institutions journalistiques respectées », comme The Guardian et The New York Times. Il les avait chargés de conserver les données qu'il avait copiées en vrac, à condition qu'ils apprécient indépendamment, au besoin en consultant les autorités, les données qui pouvaient être publiées sans mettre en danger les intérêts légitimes de la sécurité

[58] Voir US News du 14 juillet, 2014, *« NSA: Releasing Snowden Emails Would Violate His Privacy »*.
[59] Jason Leopold, « *Top NSA officials struggled over surge in FOIA requests, emails reveal* », The Guardian du 29 mai 2014.
[60] Voir les Principes de Tshwane (note 13), principe 40 (b) et (c).

nationale et celles qui ne devaient pas l'être[61]. Il semblerait que le choix opéré par les journalistes auxquels M. Snowden avait confié ces données ait été assez responsable : à ce jour, la NSA n'a pas été en mesure de mettre en avant un quelconque préjudice réel causé à la sécurité nationale par la publication des données communiquées par M. Snowden aux journalistes auxquels il avait délégué, par nécessité, le choix des documents que l'intérêt général commandait de publier.

91. La deuxième condition, c'est-à-dire le fait que M. Snowden ait raisonnablement pensé que l'intérêt général que présentait la divulgation des informations prévalait sur le préjudice que ces révélations pouvaient causer à l'intérêt général, semble également réunie. Les programmes et techniques qui permettent à la NSA et aux autres services de renseignement de procéder à la collecte en vrac et à l'analyse des données à caractère personnel dans le monde entier n'auraient jamais été connus de l'opinion publique sans la publication des fichiers à laquelle a contribué M. Snowden. Cette publication présentait clairement un intérêt pour les citoyens américains et pour ceux de nombreux autres pays visés par les programmes de surveillance massive et d'intrusion, qui ont ainsi été révélés. Le grand intérêt des médias pour ces révélations, ainsi que les nombreuses enquêtes parlementaires et autres enquêtes publiques menées à l'échelon national[62] ou dans le cadre des Nations Unies[63], du Parlement européen[64] et, enfin et surtout, par notre propre Assemblée, montrent l'étendue de l'intérêt du public pour les préoccupations soulevées par M. Snowden. Le débat qui a suivi a déjà entraîné un certain nombre de modifications de la législation et je ne peux qu'espérer que les futures recommandations que formulera l'Assemblée à partir du rapport élaboré en parallèle sur « Les opérations massives de surveillance », adopté par la commission en janvier 2015, aboutiront à la prise d'autres mesures nationales et internationales, en vue de mettre en place et de faire respecter un cadre juridique adéquat et des mesures de protection techniques, qui permettront de concilier les préoccupations légitimes en matière de sécurité nationale et le droit de l'homme fondamental du respect de la vie privée.

92. Enfin, le préjudice causé par les révélations de M. Snowden à l'intérêt général que présente la protection des activités légales des services de renseignement et de sécurité ne semble pas supérieur à l'énorme contribution de ces révélations au débat sur la nécessité de protéger le respect de la vie privée et d'amener les services de renseignement à répondre de leurs actes. Les autorités américaines ont commencé par affirmer que les révélations de M. Snowden avaient mis en danger la vie d'agents secrets, mais elles n'ont jamais fourni aucune information précise qui permette de vérifier cette affirmation. En tout état de cause, l'administration américaine avait elle-même l'habitude de divulguer des informations sur des agents secrets pour en tirer politiquement profit[65]. Au cours de son audition par la commission en juin 2014, M. Snowden a répondu de la manière suivante aux allégations selon lesquelles ces révélations avaient atténué la capacité des services de renseignement à lutter efficacement contre le terrorisme et la criminalité organisée :

93. Premièrement, l'efficacité des programmes de surveillance massive examinés aujourd'hui n'a jamais été démontrée. C'est ce qu'a conclu, par exemple, la Commission de surveillance du respect de la vie privée et des libertés civiles (Privacy and Civil Liberties Oversight Board – PCLOB)[66]. La PCLOB a critiqué les programmes d'enregistrement des communications téléphoniques mis en place par la NSA, qui n'avaient présenté qu'un intérêt « minime » pour la lutte contre le terrorisme et n'avaient donné « aucun exemple de situation dans laquelle le programme a directement contribué à découvrir un complot terroriste inconnu auparavant ou à déjouer un attentat terroriste »[67]. Bien que la PCLOB, dans son rapport remis au Président Obama en janvier 2014, ait finit par conclure à la légalité de la plupart des programmes de surveillance, elle a émis des doutes sur la proportionnalité de cette surveillance, compte tenu de ses maigres résultats. Ces doutes se sont accrus à la suite de la publication, en juin 2014, d'informations selon lesquelles neuf communications interceptées sur 10 dans le cadre de ces programmes ne poursuivaient pas un but légitime

[61] Voir Luke Harding, *The Snowden Files*, Éditions du Guardian, 2014, passim.
[62] Voir Doc. *** (2015) (rapport sur les opérations massives de surveillance), paragraphes 70 à 77.
[63] Voir « Le droit à la vie privée à l'ère du numérique », rapport du Haut-Commissariat des Nations Unies aux droits de l'homme, doc. A/HRC/27/37, disponible sur : http://www.un.org/french/documents/view_doc.asp?symbol=A/HRC/27/37 ; résolution de l'Assemblée générale des Nations Unies 68/167 du 18 décembre 2013, « Le droit à la vie privée à l'ère du numérique », disponible sur : http://www.un.org/fr/documents/view_doc.asp?symbol=A/RES/68/167
[64] Voir Doc. *** (2015) (rapport sur les opérations massives de surveillance), paragraphes 108 et 109. Le Parlement européen élabore à l'heure actuelle un rapport de suivi.
[65] Voir Assemblée parlementaire du Conseil de l'Europe, audition de la commission des questions juridiques et des droits de l'homme sur « Améliorer la protection des donneurs d'alerte » du 24 juin 2014.
[66] La Commission est une instance indépendante et bipartite du pouvoir exécutif, qui a été instituée par les recommandations d'application de la loi 9/11 relatives à la Commission, Pub. L. 110-53, promulguées en août 2007 ; voir son site Web sur : http://www.pclob.gov/
[67] Voir le New York Times du 23 janvier 2014, *« Watchdog report says N.S.A. Program is Illegal and Should End »*.

de surveillance, mais ciblaient des citoyens américains ordinaires et des utilisateurs étrangers d'internet qui n'étaient pas soupçonnés d'avoir commis un acte répréhensible[68].

94. Deuxièmement, M. Snowden a souligné que les citoyens, et plus particulièrement les malfaiteurs, ont toujours su que les lignes téléphoniques pouvaient être mises sur écoute, ce qui n'empêche pas les criminels du monde entier de continuer à utiliser des téléphones. De même, nous savons qu'internet est placé sous surveillance et nous continuons pourtant tous les jours à utiliser internet et à envoyer des courriers électroniques. Il est également inexact de dire que ces révélations ont perturbé les activités de la NSA. La poursuite des programmes de surveillance a été signalée même après les révélations de M. Snowden et certains d'entre eux au moins semblent continuer à fonctionner. Le fait de révéler que la NSA procède à une surveillance en ligne n'est guère susceptible d'amener les terroristes et les criminels à renoncer totalement aux communications en ligne et, même si tel était le cas, la NSA aurait toujours la possibilité de recourir aux moyens classiques de recherche et d'analyse des activités de ces cibles.

95. Enfin, comme l'a expliqué M. Snowden en se fondant sur sa propre expérience d'ancien agent de la CIA, les perturbations que ces révélations peuvent avoir causées dans les réseaux de communication des terroristes ne sont pas préjudiciables à la lutte contre le terrorisme ; la perturbation des modes de communication habituels des criminels les amène à commettre davantage d'erreurs, dont on peut tirer profit pour analyser et comprendre leurs nouveaux modes de communication.

96. Il est vrai que les révélations de M. Snowden ont causé beaucoup d'embarras et de complications politiques et diplomatiques aux États-Unis et à certains autres pays. Mais, selon moi, on ne peut en faire le reproche à M. Snowden : cette situation est la conséquence des mesures prises par la NSA et ses alliés. C'est le fait d'avoir espionné des pays amis et alliés qui a provoqué leurs réactions négatives[69], et non le fait d'avoir révélé l'existence de ces pratiques. Le Watergate a été catastrophique pour la présidence de Nixon parce que ce dernier avait autorisé le cambriolage des locaux, pas parce que l'opinion publique en a eu connaissance. Edward Lucas, qui se montre extrêmement critique à l'égard de M. Snowden en avançant des arguments particulièrement plausibles selon moi, se trompe lorsqu'il reproche à ce messager les dommages causés aux relations transatlantiques[70]. Les États-Unis sont eux-mêmes responsables du tort causé à leur image publique par l'affaire Snowden (et du profit correspondant qu'en a retiré la propagande en faveur de la Russie de M. Poutine) : en persécutant M. Snowden de façon aussi impitoyable, y compris sous la forme de menaces de mort proférées par de hauts responsables[71], le Gouvernement américain a choisi d'endosser le rôle du méchant sur la scène internationale ; de plus, en n'engageant pas un dialogue constructif avec ses alliés sur les voies et moyens de rétablir la confiance, il a accentué encore les retombées diplomatiques de ces révélations. Je regrette vivement que cette affaire ait été un cadeau pour l'image publique de M. Poutine, mais on peut difficilement en faire le reproche à M. Snowden.

97. Je partage également avec M. Snowden l'idée que, pour les terroristes et les membres de la criminalité organisée, le fait d'être certains que leurs communications puissent être surveillées ne leur est pas d'un grand secours : les criminels les plus dangereux ont toujours été conscients qu'ils risquaient d'être placés sous surveillance et cherché à s'en protéger, avec plus ou moins de succès compte tenu de l'évolution constante des méthodes de surveillance. Comme l'a déclaré M. Snowden au vu de sa propre expérience professionnelle, l'immense majorité des terroristes et des autres criminels sont des êtres simples, pour ne pas dire frustes. Ils continueront à commettre des erreurs qui permettront aux autorités d'en tirer parti. Le besoin d'utiliser les moyens de communication n'a pas disparu pour autant et, si les criminels communiquent moins par crainte d'être surveillés, ils seront moins efficaces. Personnellement, je trouve ces arguments très convaincants et je pense que M. Snowden lui-même pouvait « raisonnablement considérer » que l'intérêt général que présentait la révélation de ces informations était supérieur au préjudice qu'elle pouvait causer.

98. En résumé, il convient de considérer les révélations publiques de M. Snowden comme des divulgations protégées et il devrait, quant à lui, jouir d'une protection contre toute mesure de rétorsion. Il importe notamment qu'il ne fasse pas l'objet de poursuites pénales pour avoir révélé des informations classifiées ou confidentielles[72]. Selon les dispositions applicables à la protection des donneurs d'alerte que nous avons présentées ici, M. Snowden n'aurait pas même besoin de soulever l'exception de « défense de

[68] Voir The Washington Post du 5 juillet 2014, *« In NSA-intercepted data, those not targeted far outnumber the foreigners who are »*.
[69] Voir le Doc. *** (2015) (rapport sur les opérations massives de surveillance), paragraphes 104 à 106.
[70] Voir Edward Lucas, *The Snowden Operation, Inside the West's Greatest Intelligence Disaster*, 2014.
[71] Voir Huffington Post du 26 janvier 2014, « *Edward Snowden: There are 'significant threats'to my life* »; tech dirt du 3 octobre 2013, « *Former NSA Director jokes about putting Snowden on a 'kill list', says he 'hopes' that NSA is involved in targeted killings* ».
[72] Voir les Principes de Tshwane (note 13), principe 41 A. (1).

l'intérêt public »[73]. Comme nous l'avons expliqué plus haut[74], cette exception est une garantie qui devrait être à la disposition de tout agent public faisant l'objet de poursuites pénales ou d'autres sanctions pour avoir fait des révélations qui *n'étaient pas* protégées d'une autre manière : l'intéressé peut invoquer cette exception si l'intérêt général que présente la révélation des informations en question est supérieur à l'intérêt général qu'il y aurait à ne pas les révéler. Si M. Snowden n'était pas en mesure, par exemple, de démontrer qu'il avait tout d'abord cherché à utiliser les voies de signalement internes (et viables) dont il disposait, il aurait encore la possibilité de se prévaloir de l'exception d'intérêt général ; il appartiendrait alors aux autorités chargées des poursuites et au juge de déterminer si l'intérêt général présenté par la révélation de ces informations était effectivement supérieur à celui qu'il y aurait eu à ne pas les divulguer, en tenant compte de toutes les circonstances pertinentes[75], notamment en vérifiant si l'étendue des révélations était raisonnablement nécessaire. Selon moi, c'était le cas.

99. Aux États-Unis, M. Snowden demeure sous la menace de poursuites pénales très lourdes engagées au titre des dispositions de la loi relative à l'espionnage et pourrait être condamné à perpétuité, sans possibilité de libération anticipée. La loi relative à l'espionnage adoptée en 1917 a été appliquée de façon très limitée, et à trois reprises seulement à l'encontre d'agents publics qui avaient divulgué des informations confidentielles, jusqu'au début de l'administration Obama (à l'encontre de Daniel Ellsberg et Anthony Russo en 1973 pour la publication de *Documents du Pentagone* (« Pentagon Papers »), le jugement ayant finalement été entaché de vice de procédure ; à l'encontre de Samuel Morison en 1985, pour la publication d'informations relatives à une surenchère navale soviétique, qui visait à « réveiller » l'opinion publique américaine ; et en 2005, à l'encontre de Lawrence Franklin, qui avait transmis des informations sur le programme nucléaire iranien aux lobbyistes du Congrès)[76]. Mais la loi relative à l'espionnage de 1917 a été utilisée beaucoup plus souvent ces derniers temps, non pas pour des faits d'espionnage classique comme cela avait été le plus souvent le cas auparavant, mais pour sanctionner les auteurs de fuites organisées au profit des médias traditionnels. Sur 12 poursuites au total engagées à l'encontre d'agents publics accusés d'avoir fourni des informations secrètes aux médias, neuf ont eu lieu depuis la prise de fonction du Président Obama[77]. Parmi celles-ci figurent les poursuites engagées à l'encontre des donneurs d'alerte de la NSA que nous avons évoqués plus haut, Thomas Drake et Chelsea (anciennement Bradley) Manning, qui ont divulgué de nombreux documents par l'intermédiaire de Wikileaks, et plus récemment les cas d'Edward Snowden, Donald Sachtleben et Jeffrey A. Sterling. La loi de 1917 relative à l'espionnage ne permet pas de soulever la moindre forme d'exception d'intérêt général. Cela signifie que, si M. Snowden retournait aux États-Unis, il serait passible d'une très lourde peine. Conformément aux recommandations faites plus haut, je préconiserais en conséquence vivement que l'un des États européens qui ont bénéficié des révélations sur les activités de surveillance de la NSA visant leurs citoyens, leurs entreprises et même leurs élus octroie à M. Snowden l'asile.

100. En guise de post-scriptum à cette étude de cas, j'aimerais aborder les allégations selon lesquelles M. Snowden serait sciemment ou involontairement de connivence avec le FSB russe. L'argument le plus solide et le plus crédible est avancé par Edward Lucas[78], qui prétend que M. Snowden a été recruté par les services de renseignement russes agissant sous une fausse identité, c'est-à-dire manipulé par des agents qui s'étaient présentés comme des militants du respect de la vie privée sur internet et l'ont amené à agir en tirant parti des idées un peu confuses qu'il avait exprimées sur internet lorsqu'il travaillait pour la CIA. M. Lucas fait un parallèle avec ceux qui, en Occident, manifestaient en faveur de la paix pendant la guerre froide et affirme que M. Snowden a joué le rôle d'un « imbécile utile », en sabotant efficacement l'action des services de renseignement occidentaux alors qu'il pensait défendre la cause du respect de la vie privée. Dans le même esprit, l'ancien commandant du KGB Boris Karpichkov prétend que des espions du SVR russe (service de renseignement extérieur), qui s'étaient fait passer pour des diplomates, ont amené par la ruse M. Snowden, que le SVR considérait comme un transfuge possible depuis son affectation à la CIA à Genève, à demander l'asile à la Russie. M. Karpichkov pense que le Kremlin gardera M. Snowden pendant trois ans encore, jusqu'à ce qu'il n'ait plus d'informations à obtenir de lui, parce qu'il tient à savoir exactement comment les Américains et les Britanniques cryptent et décryptent les informations secrètes[79]. L'ancien général du KGB Oleg Kalugin, qui serait toujours en contact avec le FSB, a affirmé que les Russes « étaient très contents des cadeaux qu'Édouard Snowden leur avait faits » en échange de son séjour en

[73] Voir les Principes de Tshwane (note 13), principe 43.
[74] Au paragraphe 71.
[75] Voir les Principes de Tshwane (note 13), principe 43 (b) (i) – (v).
[76] Voir Jim Snyder, *The Espionage Act, A spy-fighting tool is now aimed at U.S. leakers*, Bloomberg Quick Take, 3 octobre 2014, disponible sur : http://www.bloombergview.com/quicktake/the-espionage-act
[77] Voir Jim Snyder (note 76 ci-dessus) et le Tampa Bay Times, The Pundit Fact « *CNN's Tapper : Obama has used Espionage Act more than all previous administrations* » (consulté le 25 février).
[78] Voir la note 70 ci-dessus.
[79] Voir le Mirror du 7 juillet 2014, « *Edward Snowden was targeted by Russian spies 6 years before he exposed US secrets* ».

Russie. Il est allé jusqu'à dire que M. Poutine disposait de tous les documents auxquels M. Snowden avait eu accès, y compris les documents militaires, malgré les affirmations de M. Snowden, qui assure avoir transmis tous ces fichiers aux journalistes avant de quitter Hong Kong et n'avoir conservé aucune information confidentielle lors de son entrée sur le territoire russe. Enfin, l'ancien directeur des opérations de la CIA, Jack Devine, a estimé qu'il serait « tout à fait inhabituel qu'il [M. Snowden] soit autorisé à rester là-bas [en Russie] sans contrepartie »[80].

101. Mais il convient de noter que les affirmations des deux anciens agents du KGB, qui sont aujourd'hui tous deux des transfuges vivant respectivement au Royaume-Uni et aux États-Unis, peuvent fort bien avoir été dictées par le désir de plaire à leurs hôtes occidentaux. L'avis exprimé par M. Devine est une pure spéculation. Par ailleurs, la présence de M. Snowden à Moscou a profité à l'image publique du Kremlin, indépendamment du fait qu'il ait dévoilé ou non des secrets au SVR. J'aimerais également rappeler que M. Snowden a souligné au cours de son audition par notre commission en juin dernier qu'il s'était initialement rendu à Moscou pour y faire escale à destination de l'Amérique latine. Il a finalement été bloqué à Moscou parce que les États-Unis avaient résilié son passeport et qu'aucun des plus de 20 pays auxquels il avait demandé l'asile ne lui avait répondu favorablement, à l'exception de la Russie[81]. À sa décharge, même si M. Snowden a été amené, par la ruse des services de renseignement russes, à faire les révélations en question, son geste restait motivé par l'objectif idéaliste de protéger le droit au respect de la vie privée en dévoilant les programmes d'opérations massives de surveillance et d'intrusion de la NSA. J'aimerais par ailleurs rappeler que, selon le principe de Tshwane n° 38(b), le motif d'une divulgation protégée importe peu, sauf s'il est démontré que l'intéressé savait que l'information divulguée était inexacte.

102. Enfin, la question ne devrait pas être de savoir si M. Snowden a agi en héros ou en traître, mais si les préoccupations qu'il a soulevées par l'intermédiaire de ses révélations sont bien fondées et quelles mesures il convient de prendre pour remédier aux problèmes posés par les fichiers de la NSA, ainsi que pour rétablir la confiance entre les alliés et, plus généralement, la confiance des citoyens dans la sécurité des communications légales.

7. Conclusion

103. Comme nous l'avons vu, un certain nombre d'avancées ont été réalisées depuis le premier rapport consacré par l'Assemblée à la protection des donneurs d'alerte, notamment sur le plan de la sensibilisation générale à l'importante contribution de l'action des donneurs d'alerte à la transparence et à l'obligation de rendre des comptes, dans le secteur public comme dans le secteur privé. Les organes intergouvernementaux, tels que le G20 et l'OCDE, mais également le Comité des Ministres du Conseil de l'Europe, ont rejoint sur cette question des ONG comme Transparency International, Public Concern at Work ou Whistleblower International Network, qui font campagne depuis longtemps pour le renforcement de la protection des donneurs d'alerte. La jurisprudence de la Cour européenne des droits de l'homme mérite également une attention particulière : les États devraient tenir compte des principes énoncés par la Cour dans les affaires qui concernent différents pays et ne pas attendre d'être eux-mêmes condamnés pour violation de la Convention.

104. Nous avons également constaté que la législation et les instruments internationaux en vigueur ne suffisent pas encore à assurer la protection efficace que les donneurs d'alerte méritent. C'est particulièrement vrai pour les donneurs d'alerte qui travaillent dans les domaines en rapport avec la sécurité nationale, qui sont actuellement, pour la plupart, exclus des dispositions générales relatives à la protection des donneurs d'alerte. Les révélations d'Édouard Snowden et d'un certain nombre d'autres donneurs d'alerte moins en vue ont montré que rien ne permettait de penser que le secteur de la sécurité avait moins besoin de l'action menée par les donneurs d'alerte pour défendre la bonne gouvernance et l'obligation de rendre des comptes que toute autre composante du secteur public. Comme nous l'avons expliqué dans le rapport sur Les opérations massives de surveillance adopté par la commission en janvier 2015, « l'épée de Damoclès » que représente la divulgation de tout abus par des donneurs d'alerte présents au sein même des services de renseignement pourrait bien être le moyen de dissuasion et de sanction le plus efficace contre les violations, compte tenu de la faiblesse notoire des mécanismes de surveillance parlementaire et judiciaire de la plupart des pays. L'étude de cas que nous avons brièvement consacrée à Edward Snowden offre une illustration supplémentaire des questions en jeu. Les conclusions et recommandations d'amélioration qui en découlent, notamment l'appel à la négociation d'une Convention du Conseil de l'Europe sur la protection des donneurs d'alerte, sont reprises dans l'avant-projet de résolution et l'avant-projet de recommandation qui précèdent le présent rapport.

[80] Ibid.
[81] Voir Business Insider du 27 mai 2014, *« Two Top Cold War Spies Made The Same Troubling Prediction About Edward Snowden ».*