

## De Washington à Paris, la « protection de carton » des agents secrets lanceurs d'alerte

Lanceurs d'alerte (Loi relative au renseignement)

**Jean-Philippe Foegle**

---



### Édition électronique

URL : <https://journals.openedition.org/revdh/1369>

DOI : [10.4000/revdh.1369](https://doi.org/10.4000/revdh.1369)

ISSN : 2264-119X

### Éditeur

Centre de recherches et d'études sur les droits fondamentaux

### Référence électronique

Jean-Philippe Foegle, « De Washington à Paris, la « protection de carton » des agents secrets lanceurs d'alerte », *La Revue des droits de l'homme* [En ligne], Actualités Droits-Libertés, mis en ligne le 04 juin 2015, consulté le 25 janvier 2022. URL : <http://journals.openedition.org/revdh/1369> ; DOI : <https://doi.org/10.4000/revdh.1369>

---

Ce document a été généré automatiquement le 25 janvier 2022.

Tous droits réservés

---

# De Washington à Paris, la « protection de carton » des agents secrets lanceurs d'alerte

Lanceurs d'alerte (Loi relative au renseignement)

Jean-Philippe Foegle

---

- 1 « Un peuple qui entend se gouverner lui-même doit s'armer du pouvoir que confère l'information »<sup>1</sup>. Moins de 20 mots auront suffi à Thomas Jefferson, « père fondateur » de la démocratie américaine, pour rappeler à quel point le secret d'Etat grève la démocratie d'une hypothèque. Sur le plan constitutionnel, il est un lieu commun que de souligner que la liberté d'information trouve son fondement dans les idées constitutionnelles les plus essentielles des founding fathers, qui avaient pour conviction l'existence d'un lien intime, organique, entre la transmission d'un flux adéquat d'informations (proper flow of information) au public, et la souveraineté populaire (self-gouvernement)<sup>2</sup>. En effet, s'il faut partager le postulat de certains auteurs qui rappellent que les enjeux de contrôle démocratique se situent désormais dans des mécanismes de visibilité et de surveillance citoyenne des pouvoirs publics<sup>3</sup>, force est alors de constater que **le secret déséquilibre les relations de pouvoir**. Car, comme le rappelle le politologue Frank Pasquale, « celui qui est invisible, et qui donc peut voir tout ce que font les autres à leur insu, dispose d'un avantage stratégique énorme »<sup>4</sup>. En conséquence, ce sont également les droits de l'homme qui se trouvent menacés par le secret d'Etat, car la conception rigide et extensive du « *secret de la défense nationale* » qui prévaut dans un grand nombre d'ordres juridiques conduit, précisément, à **rendre malaisée la détection de violations avérées de droits de l'homme**<sup>5</sup>. Ce n'est donc qu'en brisant le voile opaque du secret pour ménager un espace de visibilité citoyenne sur les activités de renseignement que les abus peuvent être mis à jour, car comme le rappelait le commissaire aux droits de l'homme du Conseil de l'Europe M.Hammarberg, « la menace d'une révélation freine les atteintes aux droits de l'homme »<sup>6</sup>.
- 2 Le développement des nouvelles technologies de l'information **renouvelle ces enjeux constitutionnels fort anciens et souvent pour le pire**, comme en témoigne la mise à

jour des programmes « Prism » et « Xkeyscore » par Edward Snowden<sup>7</sup>. Opérant par nature dans l'ombre et disposant de moyens de surveillance particulièrement intrusifs tels que les algorithmes prédictifs<sup>8</sup> ou les « IMSI-Catcher »<sup>9</sup>, les services de renseignement disposent désormais de toute latitude pour soumettre les citoyens à une surveillance accrue. Au risque de dénaturer l'esprit même de la démocratie délibérative, car la menace sourde d'une surveillance met gravement en péril le « *droit d'être laissé à l'écart* » qui constitue l'essence du droit à la vie privée<sup>10</sup> et la condition de possibilité d'une autonomie réelle des citoyens. Elle porte ainsi en elle **les germes de l'auto-censure et de la standardisation de la parole et donc d'une atteinte à la liberté d'expression dans toute sa diversité**<sup>11</sup>. La Cour européenne des droits de l'Homme rappelait ainsi récemment et à juste titre qu'« *un système de surveillance secrète destiné à protéger la sécurité nationale comporte le risque de saper, voire de détruire, la démocratie au motif de la défendre* »<sup>12</sup>. D'un point de vue plus prosaïque et au-delà de l'éternelle tension entre les concepts abstraits de sécurité et de liberté, le fonctionnement en vase clos des organisations favorise les erreurs et les faux jugements, et le domaine du renseignement n'échappe nullement à cette règle<sup>13</sup>.

- 3 Face aux dérives qu'autorisent l'opacité entourant les activités de renseignement l'accès du public à l'information apparaît ainsi ô combien essentielle, car seule de nature à assurer un véritable contrôle des gouvernés sur les gouvernants. En vertu du préambule des principes de Tswayne, l'accès
- 4 à l'information est non seulement « *une garantie contre les abus de la part d'agents de l'Etat, mais elle permet également au public de jouer un rôle dans la définition des politiques de l'Etat* » et constitue de ce fait « *une composante essentielle d'une véritable sécurité nationale, de la participation démocratique et de l'élaboration de politiques rationnelles* ». Mais elle est également **essentielle pour assurer l'équilibre des relations entre l'exécutif et les autres « pouvoirs »** : le lancement d'alerte est souvent - du moins dans l'espace nord-américain - l'un des seuls moyens par lequel les parlement parvient à obtenir les informations nécessaires pour **opérer un contrôle effectif sur les activités de l'exécutif**<sup>14</sup>.
- 5 Au vu d'enjeux aussi essentiels, il n'est pas surprenant que la question de la protection des lanceurs d'alerte dans le domaine du renseignement ait fait l'objet d'une attention soutenue sur le plan international des suites de l'affaire Snowden. Ainsi, en 2013, les « principes de Tswayne »<sup>15</sup>, rédigés par des acteurs associatifs en vue d'esquisser des pistes de conciliation entre sécurité nationale et accès du public à l'information ont détaillé la manière dont les Etats devraient protéger les lanceurs d'alerte dans le domaine du renseignement. Ces principes ont connu un succès certain sur le plan européen, en étant repris par le Conseil de l'Europe en 2013<sup>16</sup>, 2014<sup>17</sup> et 2015<sup>18</sup>, ainsi que par le Parlement européen en 2014<sup>19</sup>. Au niveau global, le rapport de juin 2014 du Haut-Commissariat des Nations Unies aux droits de l'homme sur « Le droit à la vie privée à l'ère du numérique »<sup>20</sup> adopte le même type d'approche, si bien que l'**on assiste timidement à la mise en place d'un véritable « standard » juridique – certes non-contraignant – en la matière**. Aux Etats-Unis, après une phase de « name-game » opposant ceux qui considèrent Edward Snowden comme « traître » et ceux qui le considèrent comme un véritable « lanceur d'alerte »<sup>21</sup>, les pouvoirs publics se sont emparés de la question, conduisant à une progression sans précédent du statut des agents secrets lanceurs d'alerte en 2012 et 2014.

- 6 C'est dans ce contexte agité qu'intervient l'article 3bis de la loi sur le renseignement qui crée avec l'article L.855-3 du Code de la Sécurité Intérieure un statut pour les lanceurs d'alerte au sein des agences de renseignement. Présenté comme une avancée notable, il s'agirait là d'un garde-fou essentiel, nous dit-on, le nec plus ultra en matière de contrôle des activités de renseignement<sup>22</sup>. En réalité, le système institué **apparaît bien éloigné du standard émergent en la matière dans le cadre des réflexions menées à l'échelon international et européen**. Inspiré des propositions du récent rapport du Conseil d'Etat<sup>23</sup> lui-même inspiré du rapport « Liberty and Security in a Changing World »<sup>24</sup> du Sénat américain, cette disposition instaure une protection calquée sur les dispositifs de lutte contre les discriminations au profit des lanceurs d'alerte dans le domaine du renseignement<sup>25</sup>. Cette disposition apparaît toutefois au milieu du gué de l'objectif supposément poursuivi par ses auteurs, à savoir celui d'assurer un réel contrôle des activités de renseignement en encourageant le lancement d'alerte. Instaurant un « droit d'alerter » sur des activités de surveillance illégales, l'article **enserme l'alerte dans la voie étroite du secret partagé, réduisant de ce fait même largement l'étendue du droit d'alerter**. Créant une Commission de Contrôle des Activités de Renseignement<sup>26</sup> (CNCTR) et prévoyant une possible saisine – indirecte – d'une autorité juridictionnelle, le législateur n'a offert ni à la première, ni à la seconde la possibilité de remédier aux comportements dénoncés, pas plus que d'enquêter de manière efficace sur ceux-ci ni même d'assurer une réelle protection aux lanceurs d'alerte. L'inefficacité prévisible des procédures nécessitant une étude qui dépasse la question des seuls lanceurs d'alerte, celle-ci sera étudié ultérieurement dans une autre lettre d'actualité.
- 7 Le caractère évanescents des protections mises en place en France pour protéger les « agents secrets » lanceurs d'alerte permet de dresser un parallèle troublant – et théâtral – avec les Etats-Unis, où l'insuffisance des protections est souvent dénoncée<sup>27</sup>. Il apparaît donc particulièrement pertinent, sur ce point, de comparer le très récent système français au système nord-américain, pour une meilleure mise en perspective des enjeux juridiques sous-jacents aux deux ordres juridiques. Dans les deux cas en effet, faute de réelle volonté politique, **les protections instituées s'apparentent à un curieux vaudeville contemporain, mêlant aux ressorts du comique de boulevard l'angoisse des huis clos des tragédies grecques**. Au risque que le droit du public à l'information apparaisse comme le mari dupé de cette fable contemporaine et que la démocratie<sup>28</sup> ne reconnaisse pas la progéniture de cet étrange ménage à trois.
- 8 Loin des projecteurs, cette tragi-comédie jouant à guichets fermés se déroule en deux actes. Le premier offre le spectacle d'un **huis clos oppressant plaçant face à face un « agent secret » lanceur d'alerte et un régulateur dépourvu de pouvoirs réels**. Faute d'élargir le champ des destinataires de l'alerte et la gamme des comportements pouvant faire l'objet d'une dénonciation, le « droit » d'alerter des lanceurs d'alerte travaillant dans le domaine du renseignement apparaît réduit à son plus simple appareil. Qui plus est, en cantonnant le droit d'alerter des agents du renseignement à un signalement à la Commission de Contrôle des Techniques de Renseignement d'atteintes à la vie privée des citoyens, le nouvel article L.855-3 du Code de la Sécurité Intérieure apparaît bien en deçà des recommandations du Conseil de l'Europe. Sur ce point, le système juridique nord-américain n'apparaît pas plus novateur. **(1°)**
- 9 Le second acte correspond quant à lui à l'entrée en scène du public et de son droit à l'information. En ne consacrant pas plus qu'aux Etats-Unis une exception de défense de

l'intérêt public au profit des lanceurs d'alerte révélant à la presse des violations graves des droits de l'homme auxquels les mécanismes de dénonciation internes n'ont pas remédié - conformément aux principes de Tswhayne - , **l'article favorise à notre sens la pratique du leaking, à savoir le fait pour des agents de faire fuiter de manière anonyme des documents confidentiels.** Et ce au détriment du public, mais aussi potentiellement au détriment des agences de renseignement elles-mêmes. Au-delà, cette « omission » expose les lanceurs d'alerte à de très lourdes sanctions pénales pour avoir simplement voulu agir dans l'intérêt du public (2°.)

## 1°/- Acte I : L'agent secret, le régulateur, le juge : un huis clos oppressant

- 10 Le droit d'alerte que pourrait instaurer la loi sur le renseignement institue un huis clos oppressant entre l'agent secret « lanceur d'alerte » et son agence. D'une part ce droit apparaît particulièrement réduit dans son champ d'application. En effet, il ne s'étend pas à l'ensemble des violations des droits de l'homme comme l'exigerait un standard international émergent, mais uniquement aux seules violations de la vie privée, comme le préconisait le Conseil d'Etat. Il s'agit donc pour le moins d'une prise en compte *a minima* – et au surplus tardive – des conséquences de « l'affaire Snowden », à rebours d'évolutions plus conséquentes outre-atlantique (A). D'autre part, les canaux d'alerte – à savoir la « liste » des personnes habilitées à recevoir l'information et à enquêter sur celle-ci – apparaissent eux-aussi enserrés dans la voie étroite du « secret-partagé ». Seule la CNCTR est habilitée à recevoir les alertes, sans qu'ait été institué au profit des agents une quelconque voie de recours dans l'hypothèse où la commission ne donnerait aucune suite à l'information fournie par un éventuel lanceur d'alerte. Ce faisant, la pertinence et l'efficacité du dispositif s'en trouvent diminuées (B).

### A – Un champ matériel et personnel d'application restrictivement défini

- 11 Réduite à la seule dénonciation d'atteintes à la vie privée (1), le droit d'alerte apparaît réduit dans son champ d'application, ce qui tranche avec les standards internationaux et les expériences étrangères pertinentes en la matière (2).

#### 1) Une alerte réduite à la dénonciation d'atteinte à la vie privée.

- 12 Le nouvel article prévoit que « *Tout agent d'un service spécialisé de renseignement mentionné à l'article L. 811-2 ou d'un service désigné par le décret en Conseil d'État prévu à l'article L. 811-4* » peut lancer l'alerte dès lors qu'il a connaissance « *dans l'exercice de ses fonctions* » de « *faits susceptibles de constituer une violation manifeste du présent livre* »<sup>29</sup>. L'identification des agents auxquels cette disposition a vocation à s'appliquer ne suscite pas d'interrogation particulière : il s'agit de l'ensemble des agents de ce qu'il est désormais convenu de nommer depuis 2009 la « *communauté française du renseignement* »<sup>30</sup>, regroupant désormais près de 6 services dépendant de 3 ministères différents<sup>31</sup>.
- 13 Soulignons toutefois ici la première insuffisance de cette nouvelle disposition : celle-ci ne s'applique qu'aux agents statutaires de la fonction publique *stricto-sensu*, et ne

**s'étend pas aux contractants de l'administration**, malgré une tentative de leur étendre les protections par le biais d'un amendement parlementaire. La mention « *dans l'exercice de ses fonctions* » ne porte pas non plus à confusion : la disposition se contente ici de reprendre une mention figurant dans la majorité des dispositifs français de protection des lanceurs d'alerte<sup>32</sup>. Elle inscrit ceux-ci dans la continuité naturelle des obligations professionnelles des agents publics, ce qui tranche avec l'approche désormais consacrée outre-atlantique<sup>33</sup>. En revanche, la mention d'une « *violation manifeste du présent livre* » mérite un examen plus approfondi. Le « présent livre » fait référence au livre VIII du Code de la Sécurité Intérieure, qui crée un article L. 811-1 du Code de la Sécurité Intérieure disposant de manière quelque peu grandiloquente que le « *respect de la vie privée, dans toutes ses composantes, notamment le secret des correspondances, la protection des données personnelles et l'inviolabilité du domicile, est garanti par la loi* ». L'autorité publique ne peut y porter atteinte que « *dans les seuls cas de nécessité d'intérêt public prévus par la loi, dans les limites fixées par celle-ci et dans le respect du principe de proportionnalité* ».

- 14 Largement superfétatoire, cette disposition se contente bien évidemment de reprendre la jurisprudence de la Cour européenne des droits de l'Homme relative à l'article 8 de la Conv. EDH. Rappelons que la Cour exige, pour qu'une ingérence dans le droit à la vie privée et familiale soit justifiée, que celle-ci soit nécessaire dans une société démocratique, prévue par la loi, et proportionnée aux buts recherchés. Celle-ci considère depuis 1978 que « *l'État doit être capable, pour combattre efficacement ces menaces, de surveiller en secret les éléments subversifs opérant sur son territoire* »<sup>34</sup> tout en exigeant que ces mesures soient soumises à un contrôle juridictionnel -ou à tout le moins d'un organisme indépendant et impartial<sup>35</sup>- et que la loi use de termes assez clairs pour indiquer à tous de manière suffisante en quelles circonstances et sous quelles conditions elle habilite la puissance publique à prendre de type de mesures.<sup>36</sup>
- 15 L'ensemble des dispositions suivantes de la loi prévoient et encadrent, précisément, **les hypothèses dans lesquelles des mesures de surveillance peuvent être mises en œuvre** (Titre I) et **selon quelles procédures** (Titre II). Les faits qui pourraient faire l'objet d'une alerte concernent donc des cas dans lesquels le droit à la vie privée serait violé soit parce qu'une mesure de surveillance serait mise en œuvre hors des hypothèses - très larges - dans lesquelles celles-ci peuvent être mises en place (art. L. 811-3); soit parce que les services n'auraient pas sollicité l'autorisation du Premier ministre en bonne et due forme (art. L. 821-2); soit, encore, parce que les données collectées n'auraient pas été supprimées à l'issue du délai prévu par la loi (art. L. 822-2).

## 2) Une étendue des protections *en deçà* des standards internationaux

- 16 Le champ matériel sur lequel peut porter l'alerte couvre ainsi *a priori* l'ensemble des hypothèses de surveillance illégale des communications, ce qui est cohérent avec la possibilité déjà évoquée par un rapport du Conseil d'État d'instaurer un droit d'alerter en matière de protection des données personnelles et de reconnaître aux agents du renseignement le droit de signaler l'existence de programmes illégaux de surveillance selon des « *modalités sécurisées* »<sup>37</sup>. En revanche, la disposition n'étend aucunement le droit d'alerte à l'ensemble des violations des droits humains qui pourraient être commises par les agences de renseignement et passées sous silence. Or, précisément, les « *Principes de Tshwane* » élaborés au plan international et auxquels l'Assemblée parlementaire a souscrit **tendraient à une approche globale du lancement d'alerte**,

**étendant celui-ci à l'ensemble des signalements d'intérêt général.** Dans ce cadre, le principe 37 prévoit un champ bien plus large de divulgations protégées, qui devaient *a minima* couvrir l'ensemble des crimes, des violations des droits de l'homme et du droit humanitaire international mais également 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 des deniers publics ou le gaspillage des ressources.

- 17 La protection des agents secrets lanceurs d'alerte aux Etats-Unis offre, comme point de comparaison, un tableau mitigé, mais néanmoins plus réjouissant. Outre-atlantique, le *Whistleblower Protection Act* (WPA)<sup>38</sup> protège l'ensemble des agents publics par le biais d'un système quasi-juridictionnel extrêmement perfectionné, mais prend le soin d'en exclure les agents travaillant au sein des agences du renseignement<sup>39</sup>. Les lanceurs d'alerte dans le domaine du renseignement et de la défense ont donc obtenu protection par le biais d'autres textes, et en particulier l'*Intelligence Community Whistleblower Protection Act* de 1998 (ICWPA)<sup>40</sup> qui ouvre au employés et contractants de la CIA et du FBI le droit de lancer l'alerte auprès de l'Inspection générale de l'agence ou auprès du Congrès à propos de faits qui constituent des « *questions urgentes à résoudre* »<sup>41</sup>. Cette loi avait toutefois « *omis* » de protéger ces personnes contre les mesures discriminatoires les visant. Les évolutions récentes en la matière dressent un **tableau en clair-obscur de la protection des whistleblowers au sein des agences de renseignement**, qui témoigne du « dilemme » de l'administration « Obama » en la matière<sup>42</sup>. D'une part, la décision *Kaplan v. Conyers* du circuit fédéral américain<sup>43</sup> a largement restreint le nombre de personnes ne pouvant bénéficier des protections instaurées par le *Whistleblower Protection Act*. Dans cette décision, la Cour a en effet exclu des protections du WPA non seulement les agents dont la position professionnelle implique d'avoir accès de manière habituelle à des informations classifiées, mais également ceux qui pourraient avoir besoin d'y accéder de manière occasionnelle. Mais, d'un autre côté, une directive présidentielle de 2012<sup>44</sup>, saluée par les fondations de défense des whistleblowers a également largement étendu les protections dont peuvent bénéficier les agents travaillant dans le domaine du renseignement, en étendant, notamment, le droit d'alerter à l'ensemble des violations de la loi, mais également aux abus d'autorités, aux erreurs manifestes de gestion et au gaspillage de fonds publics, ainsi qu'aux dangers à la santé publique ou à l'environnement ( v. infra partie I,B,2.).

## **B - Des voies de recours et canaux de l'alerte enserrés dans la voie étroite du secret partagé**

- 18 La protection des lanceurs d'alerte dans le domaine du renseignement en France apparaît profondément entravée par les exigences du secret-défense, ce qui laisse planer des doutes quant à son efficacité (1). Le tableau n'est pas plus réjouissant aux Etats-Unis où la faiblesse des garanties procédurales dont bénéficie le lanceur d'alerte rend sa protection illusoire (2).

### **1) En France, une procédure prise au piège dans le carcan du secret de la défense nationale**

- 19 Le nouvel article L.855-3 du Code de la Sécurité Intérieure encadre drastiquement l'exercice concret du droit d'alerte en ne prévoyant qu'un seul et unique canal

permettant aux agents de la « communauté française du renseignement » de lancer l'alerte. En effet, cette nouvelle disposition prévoit qu'un lanceur d'alerte souhaitant signaler des faits susceptibles de constituer une violation du droit à la vie privée peut porter ceux-ci à la connaissance que de la seule Commission nationale de contrôle des techniques de renseignement. C'est précisément sur ce point que la nouvelle disposition apparaît incomplète : Anna Myers<sup>45</sup> et Richard Moberly<sup>46</sup> soulignent en ce sens que les lanceurs d'alerte font généralement le choix - risqué à la fois pour leur personne et pour la réputation de l'organisation à laquelle ils appartiennent - de porter l'alerte auprès des médias lorsque les canaux internes de dénonciation n'ont pas été efficaces, ou que l'organisme de régulation ayant été destinataire de l'alerte n'a pas apprécié l'information communiquée à sa juste valeur et procédé à une enquête à son sujet. A cet égard, **la définition de plusieurs canaux de dénonciation apparaît fondamentale** : plus un nombre important d'organismes seront amenés à porter une appréciation sur le contenu de l'alerte, moins celle-ci sera susceptible d'être enterrée.

- 20 Or, les prérogatives de la commission et des juges sont à ce point enserrées dans le carcan du « secret-défense » qu'il paraît peu probable qu'elle puisse conduire à des résultats probants. Celle-ci, peut, en réaction au signalement, soit « faire application de l'article L. 821-6<sup>47</sup> et en informer le Premier ministre », soit, lorsque la CNCTR estime que l'illégalité constatée est susceptible de constituer une infraction d'en aviser le procureur de la République sur le fondement de l'article 40 du Code de procédure pénale et de « transmettre l'ensemble des éléments portés à sa connaissance à la Commission consultative du secret de la défense nationale afin que celle-ci donne au Premier ministre son avis sur la possibilité de déclassifier tout ou partie de ces éléments en vue de leur transmission au procureur de la République. ». Or, d'une part, rien n'oblige *stricto-sensu* la Commission à saisir le Premier Ministre ou le Procureur de la République qui eux-mêmes n'ont aucune obligation de réagir aux signalements. Par ailleurs, **aucune voie de recours n'a été prévue pour permettre aux lanceurs d'alerte d'exercer un recours contre une décision de la commission de ne pas mettre en œuvre ses pouvoirs**. D'autre part et comme nous aurons l'occasion d'y revenir rien ne garantit que le procureur ou le Premier ministre pourront être amenés à réagir efficacement aux divulgations du lanceur d'alerte. Le rôle du procureur dans le cadre de cet article apparaît même largement neutralisé, car la possibilité pour ce dernier d'enclencher l'action publique est doublement subordonnée à la décision de la Commission Nationale du Secret de la Défense Nationale d'une part, et du Premier ministre d'autre part.
- 21 Dans le cadre de l'article 40 du Code de procédure pénale, cette commission consultative - dont l'institution en 1998 avait été présentée comme un grand progrès<sup>48</sup> - devrait émettre dans les deux mois un avis sur la déclassification au Premier ministre : « favorable », « favorable à une déclassification partielle » ou « défavorable », sans pour autant que son avis soit obligatoire<sup>49</sup>. Dans la pratique les avis de la Commission sont en majorité suivis. Toutefois celle-ci souligne dans ses rapports son manque d'indépendance budgétaire<sup>50</sup>. Mais dans l'hypothèse où l'avis de la CNCTR ne serait pas suivi par le Premier ministre, **le Parquet serait placé dans l'impossibilité de faire suite aux signalements**, faute d'avoir un accès légitime à l'information dont le signalement est l'objet. Cette neutralisation de l'intervention de l'autorité judiciaire du fait du caractère quasi-absolu du secret de la défense nationale **entrave également la possibilité pour d'éventuels lanceurs d'alerte discriminés d'assurer leur défense devant le juge administratif**. En effet, dans le cas où un agent des services de

renseignement souhaiterait contester une mesure de rétorsion le visant, encore faudrait-il que celui-ci prouve sa bonne foi<sup>51</sup>, à savoir qu'il n'avait pas lancé l'alerte en ayant « *la connaissance au moins partielle de l'inexactitude des faits rendus publics ou diffusés* »<sup>52</sup>. Or, dans la mesure où la résolution d'un litige entre l'agent et son administration aurait vocation à impliquer des informations couvertes par le secret de la défense nationale, le juge administratif devrait à nouveau saisir la Commission par un jugement avant-dire droit faute de pouvoir ordonner à l'administration de lui communiquer des documents ou des informations couverts le secret<sup>53</sup>. Par suite et dans l'hypothèse où le Premier ministre refuserait la communication des informations classifiées, le juge pourrait tout au plus ordonner, par un même jugement avant dire droit, que soient versés au dossier d'instruction tous les éléments d'information sur les raisons de la classification des documents en cause, et ce dans des formes préservant le secret de la défense nationale<sup>54</sup>.

- 22 Ce système permettant d'opposer le secret-défense aux autorités juridictionnelles n'est pas sans susciter des interrogations quant à sa compatibilité aux exigences de l'article 6§1 de la Conv. EDH<sup>55</sup>. Certes, la Cour de Strasbourg considère que les Etats-membres ont une certaine marge de manœuvre pour soustraire des informations du regard du juge lorsque la sécurité nationale est en jeu<sup>56</sup>. Cependant, la décision de classification doit en toute hypothèse être soumise à l'appréciation d'un juge et approuvée par celui-ci sur la base d'une mise en balance de l'intérêt invoqué par le gouvernement et des intérêts du requérant<sup>57</sup>. Et, en principe, le préjudice causé au défendeur doit être contre-balancé par les procédures suivies devant le juge<sup>58</sup>. Celles-ci peuvent, par exemple, impliquer que le défendeur ait accès une version résumée et expurgée des informations qui n'ont pas été révélées, mais qui sont indispensables pour assurer sa défense<sup>59</sup>. **Faute de ménager un droit de regard des juges sur les décisions de classification des informations, le système institué pourrait fort bien s'exposer, à l'avenir, à une censure de la Cour sur le fondement de l'article 6§1 de la Conv.EDH.**

## 2) Aux Etats-Unis, un mécanisme peu effectif faute de garanties procédurales adéquates

- 23 Le tableau n'apparaît guère plus réjouissant outre-atlantique. Certes, l'*Intelligence Whistleblowers Protection Act* ouvre aux *whistleblowers* deux canaux pour divulguer des « *inquiétudes urgentes* »<sup>60</sup>, à savoir l'inspection générale de l'agence dans un premier temps<sup>61</sup>, et la commission du renseignement du Congrès dans un second<sup>62</sup>. Ces canaux sont hiérarchisés : l'agent doit en premier lieu lancer l'alerte auprès de l'Inspection Générale qui a 14 jours pour évaluer la crédibilité des allégations du lanceur d'alerte<sup>63</sup>. Si l'information est jugée crédible, l'Inspection doit alors envoyer un rapport à la direction de l'agence qui doit par la suite réagir dans un délai de 7 jours francs en transmettant l'alerte à la commission du renseignement du congrès américain qui prendra par la suite les mesures jugées appropriées<sup>64</sup>. Dans l'hypothèse où l'Inspection ne jugerait pas crédibles les allégations du lanceur d'alerte, l'*ICWPA* prévoit que celui-ci peut saisir directement la commission du renseignement du Congrès, ce qui est une garantie contre l'étouffement de l'alerte. Toutefois, cette garantie est extrêmement limitée car, d'une part, un employé souhaitant alerter la commission du renseignement du congrès doit au préalable faire part de son intention à la direction de l'agence<sup>65</sup>. Deuxièmement, le lanceur d'alerte doit suivre les directives de l'agence s'agissant des

« *bonnes pratiques* » en matière de révélation d'informations classifiées au Congrès pour pouvoir obtenir protection<sup>66</sup>. En réalité, l'agence garde la mainmise sur l'alerte, ce qui apparaît **particulièrement dissuasif pour le lanceur d'alerte et l'expose très probablement à des risques**. Edward Snowden soulignait d'ailleurs qu'il avait fait part à ses collègues de sa volonté d'utiliser ces mécanismes, mais que réponse qui lui avait été donnée était que le système n'était pas prévu pour résoudre les problèmes, mais pour les enterrer<sup>67</sup>.

24 Au surplus, l'ICWPA n'avait pas, jusqu'à une période récente, prévu de protection spécifique pour les lanceurs d'alerte victimes de discriminations pour avoir lancé l'alerte dans le cadre des procédures sus-mentionnées. Il a fallu attendre octobre 2012 et la directive présidentielle PPD-19<sup>68</sup> pour que les « *agents secrets* » lanceurs d'alerte obtiennent une protection. Sous l'empire de cette directive, aucun de ces agents ne peut faire l'objet d'une mesure de rétorsion, ni se voir retirer son habilitation secret-défense. La directive prévoit en outre que les agences de renseignement doivent mettre en œuvre des dispositifs d'alerte interne et autoriser l'inspection générale à enquêter pour s'assurer de la réalité des mesures discriminatoires prises à l'égard du lanceur d'alerte, et recommander le cas échéant à l'agence de prendre des mesures pour mettre fin à la discrimination constatée, **sans que l'agence ne soit obligée de se conformer aux recommandations de l'Inspection générale**. Les employés victimes de discrimination peuvent en outre demander à l'inspection générale de réunir un « *panel externe* » composé de membres d'autres inspections pour examiner à nouveau, dans un délai de 90 jours, la réalité des agissements discriminatoires de l'agence et le cas échéant recommander à nouveau à cette dernière de mettre fin à ces agissements. Sans qu'une fois de plus ces recommandations n'aient une quelconque force contraignante ! L'*Intelligence Authorization Act for Fiscal Year* de 2014<sup>69</sup> a repris ce mécanisme, lui conférant force de loi là où une directive présidentielle peut en principe être retirée à tout moment par le président.

25 Si ces dispositions constituent un progrès indéniable, elles présentent deux défauts majeurs : **elles ne s'appliquent pas aux contractants de ces agences** – ce qui était le cas d'Edward Snowden – et interdisent au juge de se prononcer sur des mesures discriminatoires prises à l'égard d'un lanceur d'alerte, renvoyant la protection de ceux-ci à un système quasi-juridictionnel dont l'indépendance est contestée. L'effectivité de cette disposition est d'ailleurs d'ores et déjà mise en cause : comme le rappelle Peter Omzigt<sup>70</sup>, « *certaines 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* »<sup>71</sup>.

\*

26 Faute de garantie quant à leur effectivité, les protections accordées aux lanceurs d'alerte ressemblent fort à ce que le *Government Accountability Project* nomme les « *protections de carton* » (*cardboard shield*)<sup>72</sup>, à savoir des mécanismes offrant l'illusion d'une protection, mais mettant en réalité les lanceurs d'alerte en danger car les exposant de manière certaine à des représailles. Reste alors la possibilité pour les agents publics lanceurs d'alerte de saisir la presse pour alerter directement le public.

Or, en l'absence de définition d'une véritable exception d'intérêt public, ce dernier et ultime recours apparaît bien difficile à mettre en œuvre.

\*

## 2°/- Acte II : Le public, grand dupé du *ménage à trois* de la loi renseignement ?

- 27 La loi, ne consacrant pas une exception de défense de l'intérêt public au profit des lanceurs d'alerte, se trouve de ce fait en retrait d'un standard international émergent (A.). Le silence apparaît d'autant plus imposé aux lanceurs d'alerte que ceux-ci risquent de très lourdes sanctions sur le plan pénal (B.).

### A - L'absence d' « *exception de défense de l'intérêt public* », une situation en contradiction avec les standards internationaux

- 28 L'omission d'une exception d'intérêt public est une occasion manquée de favoriser les fuites responsables et donc de préserver à la fois l'intérêt du public et celui des agences (1.). Sur ce point, les Etats-Unis et la France gagneraient donc grandement à s'inspirer du droit international (2.).

#### 1) Une omission favorisant les fuites irresponsables

- 29 Les lanceurs d'alerte travaillant dans le domaine du renseignement en France et aux Etats-Unis ne disposent d'aucune voie de droit pour alerter directement le public de violations graves et manifestes des droits de l'homme. En France, comme nous le rappelions récemment<sup>73</sup> en collaboration avec un auteur précurseur en matière de droit d'alerte dans la fonction publique<sup>74</sup>, le juge administratif s'est toujours montré extrêmement sévère à l'égard des fonctionnaires s'exprimant publiquement. Mentionnons à titre d'exemple un arrêt concernant un agent d'une maison d'arrêt qui avait accordé un entretien en 2007 à un journal local dans lequel il dénonçait le système carcéral, et dont la sanction disciplinaire a été validée par la CAA de Bordeaux<sup>75</sup>. Dans le même sens, a été jugée légale la sanction infligée à un fonctionnaire du service de santé des armées ayant écrit un livre et participé à des émissions de télévision, sans autorisation de sa hiérarchie, pour dénoncer des dysfonctionnements qu'il estimait répréhensibles au regard des dispositions du code pénal<sup>76</sup>. Plus récemment, la CAA de Paris a confirmé la sanction infligée à une policière qui avait publié un livre dénonçant le racisme et le sexisme au sein de la police, en relevant notamment que l'agent en question – qui avait saisi le Défenseur des Droits et le Procureur de la République – avait publié le livre en cause alors que réponses à ces dénonciations ne lui étaient pas toutes parvenues<sup>77</sup>.
- 30 Faute d'avoir « épuisé » toutes les voies de dénonciation interne efficaces, un lanceur d'alerte ne pourra virtuellement jamais saisir les médias de ce qu'il estime être une violation grave d'un droit de l'homme, bien que la jurisprudence de Cour de Strasbourg apparaisse à même de changer, timidement, cet état du droit (voir note analyse *supra*, II.A.1). Et, au-delà du devoir de réserve, il est évident qu'une alerte au publique

heurterait de plein front l'obligation de se conformer au secret professionnel (art. 26, al. 1er de la loi du 13 juillet 1983.), défini comme l'obligation faite à tout agent public de ne pas révéler à autrui des renseignements confidentiels recueillis dans l'exercice de ses fonctions sur des personnes ou des intérêts privés.

- 31 Aux Etats-Unis, la jurisprudence de la Cour Suprême des Etats-Unis laisse subsister ce que le professeur Bickel appelait une « *situation désordonnée* »<sup>78</sup>, à savoir un état du droit dans lequel toute tentative gouvernementale de « censure » d'une publication journalistique révélant des informations classifiées serait grevée d'une « *forte présomption d'inconstitutionnalité* », mais où le même gouvernement pourrait sans nul doute sanctionner l'agent ayant communiqué à la presse ces mêmes informations. En effet, depuis arrêt *Near v. United States* de 1931<sup>79</sup>, la Cour Suprême des Etats-Unis considère que « *la Constitution impose que toute restriction préalable à la liberté d'expression soit justifiée par des preuves conséquentes du danger que constituent les propos visés* »<sup>80</sup>. Elle précise toutefois que « *la protection de la liberté d'expression contre les restrictions préalables n'est pas absolue* »<sup>81</sup>, et qu'en temps de guerre, « *certaines choses qui peuvent être dites en temps de paix sont susceptibles, en temps de guerre, de nuire aux efforts de guerre à un tel point que celles-ci ne peuvent être acceptées tant que des hommes continueront de se battre* »<sup>82</sup>. Plus précisément, personne ne saurait mettre en doute, aux yeux de la Cour, que le gouvernement puisse prévenir, par exemple, « *la publication du nombre de soldats déployés ou de la position exacte des troupes* »<sup>83</sup>; une telle publication constituerait, sans aucun doute possible, un « *danger immédiat* ».
- 32 Ainsi pour le professeur Melissa Opper, « *la conclusion de la Cour selon laquelle les documents contenant des précisions sur les opérations militaires s'applique au cas de Wikileaks* »<sup>84</sup>. Au regard en revanche de l'arrêt *New York Times Co v. United States*<sup>85</sup>, plus connu sous le nom de la « *jurisprudence des Pentagon Papers* », le gouvernement doit apporter la « *preuve irréfutable* » du danger imminent que causerait une publication<sup>86</sup>. Bien que la portée réelle de la jurisprudence des *Pentagon Papers* soit toujours discutée et que nombre de questions restent en suspens<sup>87</sup>, il semble peu douteux au vu de cette unique jurisprudence qu'une tentative d'interdire à un journal de publier les révélations faites par Edward Snowden eût été inconstitutionnelle.
- 33 En revanche, la Cour suprême américaine a également et de longue date, reconnu que le gouvernement a « *un intérêt légitime à réglementer la liberté d'expression de ses employés, qui diffère grandement de ceux que ces mêmes agents lorsqu'ils s'expriment en tant que citoyens de manière générale* »<sup>88</sup>. Le problème est alors, soulignait la Cour, de trouver « *un équilibre satisfaisant entre le droit l'agent public à émettre un avis sur des sujets d'intérêt public en tant que citoyen d'une part, et les intérêts de l'Etat-employeur à assurer l'efficacité des services publics* ». Or, comme le souligne Stephen Vladeck, ce type de raisonnement juridictionnel indique nécessairement qu'il « *puisse y avoir des hypothèses dans lesquelles l'intérêt public présenté par les divulgations d'un employé puisse primer sur l'intérêt légitime du gouvernement à maintenir le secret sur ses actions* »<sup>89</sup>.
- 34 S'agissant des employés des services de renseignement, la même Cour Suprême avait d'ores et déjà, en 1980, considéré qu'un ancien employé de la CIA pourrait être lié à son engagement de ne « *publier aucune information ou aucun document en lien avec la CIA sans accord préalable* »<sup>90</sup>, en estimant notamment qu'« *une publication de documents liés à des activités d'espionnage par un ancien agent apparaît susceptible de nuire aux intérêts vitaux de la nation* ». Certes, il ne ressort pas de cette décision que toute divulgation d'informations liées à des activités de renseignement ne serait pas protégée, et l'on

peut considérer, comme certains membres de la doctrine nord-américaine, que « *selon ce standard [le standard adopté dans la décision Pickering], une majorité des révélations faites par des agents depuis le 11 septembre présenteraient un intérêt public prépondérant* »<sup>91</sup>..

- 35 Toutefois, la révision du « *Standard Pickering* » par la décision *Garcetti c. Ceballos* en 2006 semble définitivement exclure les employés des protections instituées par le premier amendement puisque la Cour Suprême a considéré que « *[le fait de] réduire le droit à la liberté d'expression d'agents publics s'exprimant sur des faits dont il n'a pu avoir connaissance que dans le cadre de ses responsabilités professionnelles ne porte atteinte à aucune des libertés dont jouit cet agent en tant que citoyen* ». Or, les informations portant sur des secrets liés à la sécurité nationale sont par définition des informations auxquelles le citoyen moyen n'a pas accès. Il semble donc raisonnable d'affirmer au vu de ces jurisprudences qu'un agent public divulguant à des journalistes ou à d'autres médias des informations classifiées « *violerait ses obligations professionnelles et pourrait être renvoyé ou faire l'objet de sanctions pénales sans que cela ne viole le premier amendement* ». <sup>92</sup>
- 36 Faute de favoriser les alertes au public responsables - *i.e* les alertes ciblées sur des faits précis et non les alertes -en les encadrant, le droit américain et le droit français favorise la pratique du *leaking*, à savoir la divulgation publique illégale d'information confidentielle réalisée hors des voies et procédures prévues à cet effet par un employé gouvernemental qui s'attend, en retour, à bénéficier de l'anonymat<sup>93</sup>. Et ce au détriment à la fois des agences, mais également des lanceurs d'alerte eux-mêmes, car la protection des sources journalistiques aux Etats-Unis<sup>94</sup> comme en France n'apparaît pas suffisante pour garantir un réel anonymat<sup>95</sup>.

## 2) Une « omission » en contradiction avec un standard international émergent

- 37 Ne serait-il pas alors préférable, conformément à un standard international émergent, de se saisir des fuites des agents du renseignement pour mieux les encadrer, et ce en instaurant une exception d'intérêt public au profit des lanceurs d'alerte ? Le rapport de Peter Omzigt rappelle que le principe 43 des « *Principes de Tshwane* » exigent « *que les agents publics bénéficient d'une exception de « défense de l'intérêt public » et ce « 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<sup>96</sup>. Organisée selon un principe de rationalisation de l'alerte commun à de nombreuses législations, cette exception d'intérêt public ne jouerait que de manière subsidiaire, lorsque les voies d'alertes internes et externes auprès des autorités de régulation n'ont pas abouti. Surtout, le lanceur d'alerte doit avoir eu la conviction que l'étendue de la divulgation ne dépassait pas ce qui était nécessaire pour que celle-ci soit efficace ainsi que la conviction que la divulgation était d'intérêt général. Dans ce cadre, la sensibilité des informations et le préjudice que pourrait causer leur révélation seraient, souligne Peter Omzigt<sup>97</sup>, pris en compte pour déterminer si l'intérêt général de cette divulgation prévalait sur le risque de préjudice, mais le caractère confidentiel des informations ne saurait interdire d'emblée une divulgation protégée. Une telle exception de défense de l'intérêt public serait donc bien loin de favoriser les fuites irresponsables !
- 38 Aux Etats-Unis, le professeur Benkler a proposé une défense similaire pour les lanceurs d'alerte en distinguant les « *fuites* » tolérées et encouragées par les agences pour façonner l'opinion, et les « *fuites de responsabilité* » (accountability leaks) qui mettent

en évidence des dysfonctionnements graves de ces agences - et conduisent généralement à ce que les auteurs de ces « fuites de responsabilité » soient poursuivis et harcelés<sup>98</sup>. Benkler souligne que ce type de mécanisme devrait se focaliser sur la nature et la gravité du comportement dénoncé, et non sur les motivations du lanceur d'alerte. Ce mécanisme, à l'instar de celui proposé par les principes de Tshwayne, serait donc fondé sur un élément objectif -celui de l'intérêt qu'a le public à recevoir l'information en cause- et non sur un élément subjectif. Dans ce cadre, il ne serait exigé du lanceur d'alerte qu'une croyance raisonnable que sa dénonciation porte bien sur une « erreur systémique » et que la révélation se soit faite de manière raisonnable, à savoir sans révéler plus d'informations que nécessaire pour mettre en évidence la situation dénoncée<sup>99</sup>. Ainsi, les révélations faites à Wikileaks seraient plus difficilement considérées comme des « fuites de responsabilité » que les révélations faites à des médias traditionnels, mais les juges devraient prendre en compte la nature spécifique des médias en ligne pour apprécier le caractère raisonnable de la divulgation, à savoir le fait que la duplication à l'infini des contenus sur Internet n'est pas nécessairement de la responsabilité du média en cause, sauf à lui refuser toute protection sur le fondement du premier amendement<sup>100</sup>.

- 39 Dans le cadre de cette exception de défense de l'intérêt public, il appartient au gouvernement, s'il souhaite poursuivre le lanceur d'alerte sur le plan pénal, de démontrer de manière « claire et évidente » d'une part -ce qui ressemble beaucoup, en réalité, au « Standard Pickering » que certains auteurs ont proposé de remettre au goût du jour<sup>101</sup> que la révélation cause bien un mal « imminent, spécifique et substantiel » au public et que l'ampleur de celle-ci dépasse manifestement ce qui est nécessaire pour mettre fin aux faits dénoncés<sup>102</sup>. Une telle administration de la preuve nécessiterait sans aucun doute une révision du « Classified Information Act »<sup>103</sup> pour permettre au juge d'avoir accès à l'ensemble des documents relatifs aux faits dénoncés, y compris ceux qui n'ont pas été révélés publiquement : en effet, pour s'assurer que l'ampleur de la révélation ne dépasse pas le nécessaire, encore faut-il avoir accès à l'ensemble des informations relatives aux faits dénoncés.

## B – Des agents réduits au silence par la pénalisation de la divulgation publique d'informations classifiées

- 40 En France, la protection pénale du secret de la défense nationale condamne d'avance les lanceurs d'alerte, mais pourrait se trouver sous le feu des juges de Strasbourg (1.). Aux Etats-Unis, la situation est encore nettement plus préoccupante, à telle enseigne qu'un documentaire a pu décrire celle-ci comme une véritable « guerre » contre les lanceurs d'alerte (2.).

### 1) En France, la pénalisation du secret-défense sous le feu de la CEDH

- 41 En France également, nombre de dispositions du Code pénal sanctionnent les divulgations d'informations classées « *secret-défense* ». Les principales sont les articles 413-10 et 413-11 du Code pénal, qui sanctionnent de cinq ans d'emprisonnement et de 75.000 euros d'amendes fait de détruire, reproduire ou diffuser de telles informations. Dans ce cadre, le ministère de l'intérieur a relevé que : « 677 affaires d'atteinte aux intérêts fondamentaux de la Nation - catégorie dans laquelle entre la compromission d'informations classifiées - pour 461 en 2007 »<sup>104</sup>. Selon le professeur André Vitu, l'article 413-9 du code

pénal reprend la distinction ancienne entre « *secrets par nature* », à savoir les informations couvertes en elles-mêmes par le secret et les « *secrets par extension* », à savoir les informations qui ne sont pas en elles-mêmes classifiées, mais dont la révélation peut indirectement conduire à la révélation d'un fait couvert par le secret-défense<sup>105</sup>. Cette rédaction assez large ouvre, sans conteste, une très large marge de manœuvre aux pouvoirs publics pour sanctionner d'éventuels « *Snowden à la française* » qui tenteraient d'alerter le public sur des faits couverts par le secret de la défense nationale. En effet, au sein des informations dont la révélation peut être pénalisée, figurent les renseignements militaires au sens large<sup>106</sup>, les instructions adressées en temps de paix aux officiers de réserve, mais également la quasi-totalité des renseignements d'ordre diplomatique<sup>107</sup>. Y figurent également l'intégralité des objets ou documents que l'intérêt de la défense nationale commande de ne pas diffuser<sup>108</sup>, ainsi que les données informatisées.

- 42 Plus largement, ce sont l'ensemble des divulgations portant sur des informations que l'exécutif juge opportun de classer qui sont susceptibles d'être pénalisées. L'article L. 413-9 renvoie à un décret le soin de prendre à l'égard de ces informations les "*mesures de protection destinées à restreindre leur diffusion*", à savoir de classer les informations dans des catégories juridiques interdisant leur divulgation sous peine de poursuites pénales. ». Les mesures de protection du secret-défense consistent actuellement, depuis le décret n° 98-608 du 17 juillet 1998, en une réglementation de l'accès des lieux où sont conservés les documents et un marquage particulier de ceux-ci en fonction de trois niveaux de protection : le « *Très Secret-Défense* »<sup>109</sup>, le « *Secret-Défense* »<sup>110</sup> et le « *Confidentiel-Défense* »<sup>111</sup>. L'accès aux informations ou supports protégés est réservé aux personnes titulaires d'une décision d'habilitation ayant besoin de les connaître pour l'accomplissement de sa fonction ou de sa mission<sup>112</sup>. La décision d'habilitation précise en outre le niveau de classification des informations auxquels la personne habilitée et intervient à la suite d'une procédure définie par le Premier ministre. Actuellement, cette décision est prise par le Premier ministre pour le niveau « *Très Secret-Défense* »<sup>113</sup> tandis que pour les niveaux de classification « *Secret-Défense* » et « *Confidentiel-Défense* », la décision d'habilitation est prise par chaque ministre pour le département dont il a la charge.
- 43 Les mécanismes français de protection des informations « *secret-défense* » permettent donc de condamner de manière parfaitement indiscriminée l'ensemble des « *lanceurs d'alerte* » diffusant des informations classifiées, qu'il y ait ou non un intérêt général prépondérant à ce que le public prenne connaissance de ces informations. Or, ce système pourrait fort bien se trouver, à l'avenir, sous le feu de la Cour EDH en raison de l'émergence – certes timide embryonnaire – mise en évidence par le professeur Dirk Voorhof<sup>114</sup>, d'un véritable « *droit à l'information* » du public à l'égard des informations détenues par le gouvernement, et ce sur le fondement de l'article 10 de la Conv. EDH.
- 44 La Cour de Strasbourg a en effet rappelé de manière constante 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* »<sup>115</sup> et, dans ce contexte, comme le souligne Dirk Voorhof, un journaliste, un fonctionnaire, un militant ou un employé d'une ONG ne devrait pas pouvoir être poursuivi ou sanctionné pour avoir enfreint une obligation de confidentialité ou pour avoir publié des documents obtenus de manière illégale »<sup>116</sup>. Car, comme l'a déjà souligné la Cour, « *il y a un intérêt public prépondérant à ce que [ces personnes] puissent s'exprimer auprès du public en diffusant des informations sur*

des idées sur des question d'intérêt public », notamment lorsque les pratiques gouvernementales mises en lumière sont susceptibles d'être illégales ou nuisibles à l'intérêt général. Dans ce cadre, la Cour prendra en compte le poids respectif du dommage que la divulgation litigieuse risquait de causer à l'autorité publique et de l'intérêt que le public pouvait avoir à obtenir cette divulgation<sup>117</sup> ainsi l'objet de la divulgation et la nature de l'autorité administrative concernée.

- 45 D'autre part surtout, il semble désormais possible que la Cour Européenne puisse interdire la mise en place de poursuites pénales contre d'éventuels lanceurs d'alerte divulguant auprès du public des informations classifiées. En effet, dans un arrêt de 2013, la Cour EDH a invalidé, sur le fondement de l'article 10 de la Conv EDH, la condamnation d'un agent des services secret roumains ayant révélé à l'occasion d'une conférence de presse des informations classifiées démontrant la mise sur écoute de journalistes, de personnalités politiques et d'hommes d'affaire. Dans cette décision, la Cour avait notamment relevé l'intérêt public des révélations, rappelant qu'un « système de surveillance secrète destiné à protéger la sécurité nationale comporte le risque de saper, voire de détruire, la démocratie au motif de la défendre »<sup>118</sup>. L'application des critères énoncés par l'arrêt « Guja » semble donc de nature à protéger les lanceurs d'alerte dans le domaine du renseignement. Notons toutefois que si la Cour a conclu, à l'unanimité, que, dans les circonstances de l'espèce, la divulgation des faits dénoncés directement à l'opinion publique pouvait se justifier, elle ne l'a fait qu'après avoir conclu sans appel que le requérant ne disposait d'aucun autre moyen efficace pour procéder à la divulgation. A cet égard, l'institution du système sus-mentionné pourrait bien constituer un « piège » pour les lanceurs d'alerte en ce qu'il risque de rendre plus difficile la reconnaissance d'une violation de l'article 10 de la Conv. EDH.

## 2) Aux Etats-Unis, un contexte de « guerre » contre les lanceurs d'alerte

- 46 Aux Etats-Unis, la divulgation publique d'informations classifiées est susceptible de faire l'objet d'une lourde sanction pénale sur trois fondements différents. Le premier fondement est celui de la trahison, crime qui « plus qu'un autre excite les passions »<sup>119</sup> et qui se trouve également être le seul crime défini par la Constitution américaine. Celui-ci peut être puni de mort. L'article III section 3 définit le crime de trahison comme le fait de « déclencher une guerre contre les Etats-Unis » ou « d'aider ou rejoindre les rangs de l'ennemi »<sup>120</sup>. Pour le professeur Papandrea<sup>121</sup>, cette disposition constitutionnelle pourrait à l'avenir servir de fondement aux poursuites contre les lanceurs d'alerte d'autant plus facilement que cette disposition ne définit pas ce qu'est un « ennemi »<sup>122</sup> et n'exige pas une déclaration de guerre en bonne et due forme<sup>123</sup>. Au surplus, certains arrêts des cours du circuit fédéral et de la Cour suprême ont suscité le trouble en considérant qu'un défendeur ne pouvait s'exonérer de ses responsabilités en invoquant le fait qu'il n'avait pas l'intention d'aider l'ennemi<sup>124</sup>.
- 47 Dans ce cadre, toujours selon le professeur Papandrea, Al Qaeda pourrait sans aucun doute être considérée comme un « ennemi » au sens de cette disposition<sup>125</sup> et une interprétation large de la notion de trahison pourrait potentiellement permettre de condamner des « lanceurs d'alerte », qui tels que Chelsea Manning, n'ont pas eu l'intention d'aider directement l'ennemi – ici Al Qaeda – mais ne pouvaient ignorer que celui-ci tirerait profit des informations divulguées au public et visibles sur internet. Toutefois, soulignons que le crime de trahison n'a été utilisé comme fondement à des poursuites qu'une seule fois depuis 1947<sup>126</sup>. Et qu'une accusation de trahison dirigée

contre un citoyen américain se trouverait probablement frappée d'inconstitutionnalité au regard de la jurisprudence développée au cours des soixante dernières années par la Cour suprême des Etats-Unis en matière de liberté d'expression<sup>127</sup>.

- 48 En revanche, le chef d'accusation de « trahison » prévu par l'article 104 du Code uniforme de justice militaire<sup>128</sup> - qui est également passible de la peine de mort - apparaît bien plus susceptible de constituer le fondement de poursuites pénales engagées contre des « lanceurs d'alerte », et a servi de fondement aux accusations portées contre Chelsea Manning<sup>129</sup>. Largement similaire aux dispositions constitutionnelles de l'article III section 3 de la Constitution Américaine, cet article n'exige néanmoins aucune communication « directe » avec l'ennemi, et interdit toute forme de communication, même indirecte, avec celui-ci, ce qui permet la poursuite des lanceurs d'alerte divulguant par voie de presse des informations classifiées. Dans ce cadre, comme le souligne à juste titre le professeur Papandrea, Chelsea Manning aurait pu être condamné sur le fondement de l'article 104 quand bien même celui-ci aurait divulgué les informations en sa possession au *New-York Times* plutôt qu'à *Wikileaks*<sup>130</sup>. Certes, la Cour ayant jugé Manning a refusé de le condamner sur le fondement de cet article, mais sans expliquer son raisonnement. Or, si certaines cours ont considéré que l'article 104 impliquait nécessairement que la personne poursuivie ait eu l'intention de divulguer - même indirectement - des informations à l' « ennemi » une décision *United States v. Batchelor*<sup>131</sup> de la Cour d'Appel militaire avait au contraire énoncé qu'un citoyen américain pouvait parfaitement être poursuivi pour trahison quand bien même son intention n'aurait pas été de révéler des informations à l'ennemi. Il paraît donc possible que le chef d'espionnage prévu par l'article 104 puisse servir de fondement à la condamnation de lanceurs d'alerte divulguant publiquement des informations classifiées, quand bien même cette divulgation ne conduirait qu'indirectement et accidentellement à fournir à l' « ennemi » des informations sensibles.
- 49 S'il n'est pas exclu que le chef d'accusation de trahison puisse être utilisé contre les lanceurs d'alerte, c'est avant tout sur le fondement de l'*espionnage act* que les lanceurs d'alerte dans le domaine du renseignement ont été poursuivis. L'*Espionage Act* de 1917<sup>132</sup>, créé dans le cadre de l'entrée des États-Unis dans la première guerre mondiale<sup>133</sup>, visait notamment à punir les agents ou soldats américains ayant obtenu ou divulgué des informations relatives à la défense nationale à une personne non habilitée à recevoir ce type d'information. Amendée à de multiples reprises et désormais codifiée<sup>134</sup>, après une tentative de lui substituer un texte plus répressif qui avaient buté sur le veto du président Clinton<sup>135</sup>, cette loi prévoit des peines de prison pouvant aller jusqu'à dix ans<sup>136</sup> pour tout agent qui, possédant des informations liées à la défense nationale susceptibles de causer un dommage aux Etats-Unis ou d'avantager une nation étrangère, et qui « *communique, délivre ou transmet celles-ci* », ou tente de le faire.
- 50 Longtemps peu utilisée, cette loi a servi de fondement juridique aux poursuites engagées contre Bradley/ Chelsea Manning<sup>137</sup>, Edward Snowden<sup>138</sup> et d'autres lanceurs d'alerte<sup>139</sup>. Plus précisément, ceux-ci sont généralement - à l'exception notable de John Kiriakou<sup>140</sup> - poursuivis sur le fondement du §793(d) de l'*Espionage Act*, qui interdit la communication « *volontaire* » d'informations classifiées à « *toute personne non habilitée à les recevoir* » - ce qui, aux yeux de nombre de membres de la doctrine, inclut la presse<sup>141</sup>. Est indifférent, à cet égard, que la divulgation ait ou non causé un tort aux Etats-Unis<sup>142</sup> ou que le lanceur d'alerte ait eu pour intention de contribuer au débat public<sup>143</sup>. En pratique, cette disposition n'a servi de fondement à des poursuites qu'à onze reprises

(dont les époux Rosenberg), mais l'administration Obama a, à elle seule, poursuivi huit lanceurs d'alerte sur ce fondement. Cette « criminalisation » soudaine du lancement d'alerte – qui s'explique par un changement radical d'attitude de l'administration américaine à l'égard d'un phénomène autrefois implicitement toléré car participant de l'« illusion » de la transparence gouvernementale<sup>144</sup> – fait peser une menace inédite sur l'effectivité de la protection instaurée par le Premier Amendement<sup>145</sup> du fait de son effet fortement dissuasif sur les sources des journalistes.

\*

\*\*

## Conclusion : Du vaudeville à la tragédie, une mise à mort programmée des lanceurs d'alerte dans le domaine du renseignement

51 « *Un secret est un secret, et nous ne pouvons vous dire pourquoi il s'agit-il d'un secret ni qui décide qu'il s'agit d'un secret, car il s'agit d'un secret* »<sup>146</sup>. Les idées les plus complexes s'expriment généralement de manière simple. Dès lors, comment mieux clore un propos sur le secret de meilleure manière qu'en citant une pensée du personnage d'Alice créé par Lewis Carroll ? La frustration enfantine d'Alice témoigne en effet de la manière la plus simple et naturelle du **caractère parfois absurde du secret**, qui conduit bien souvent à placer *hors-contrôle* nombre de faits et comportements pourtant d'importance cruciale pour la bonne marche d'un régime se concevant comme démocratique. Ce n'est sans doute pas un hasard si des auteurs de philosophie morale et non des moindres ont proposé, à l'instar de Kant<sup>147</sup> et de Norberto Bobbio<sup>148</sup>, de **supprimer purement et simplement les services de renseignement**. Mais il est également vrai que la démocratie doit s'accommoder d'une certaine dose de secret et que la transparence portée à ses extrémités porte en elle les germes de l'autoritarisme voire d'une tentation totalitaire : comme le rappelait Guy Carcassonne, la transparence comme idéologie « *confond la fin et les moyens et, dans son absolutisme, se rattache beaucoup plus étroitement au totalitarisme qu'à la démocratie* »<sup>149</sup>. Il ne fait ainsi aucun doute que « *les démocraties constitutionnelles ne peuvent s'accommoder vivre avec le secret, mais ne peuvent pas non plus vivre sans* » comme l'ont rappelé les professeurs Cole, Fabbrini et Vedaschi<sup>150</sup>.

52 Les rapports entre secret et liberté apparaissent toutefois, en France comme aux États-Unis, renversés. Dans l'espace juridique et politique nord-américain en particulier, l'augmentation exponentielle du nombre de « lanceurs d'alerte » dans le domaine du renseignement n'a pas tant pour fondement l'émergence des nouvelles technologies – qui certes favorisent le lancement d'alerte<sup>151</sup> – qu'une **profonde crise des mécanismes de contrôle démocratique**. L'Amérique « *post 11 septembre* » ressemble ainsi fort à celle des années 1970, où une profonde crise démocratique, marquée par une perte de confiance dans les mécanismes traditionnels de ce que certains auteurs ont nommé la démocratie « *Post-Westminster* »<sup>152</sup>, favorise l'émergence de personnages comme Daniel Ellsberg ou Edward Snowden. Ceux-ci, hier<sup>153</sup> comme aujourd'hui, permettent de **corriger les abus les plus importants du pouvoir exécutif et de faire évoluer le droit**. Et, hier comme aujourd'hui, ces courageux personnages font l'objet de sanctions

pour avoir adhéré plus que d'autres aux valeurs constitutionnelles, renvoyant leur action à une pratique opérant aux marges du droit. Ce type de pratique, intervenant, comme la désobéissance civile, lorsque les citoyens « ont acquis la conviction de l'évolution ne fonctionnent plus ou que leurs réclamations ne seront pas entendues ou suivies d'effets »<sup>154</sup> vient alors tester l'aptitude du système politique et des droits de l'homme à s'adapter aux changements. Il s'agit alors d'un « test-limite » pour l'état constitutionnel<sup>155</sup>.

- 53 Cette absence de reconnaissance institutionnelle du rôle des lanceurs d'alerte en période de crise démocratique est néanmoins, dans des sociétés « saturées par l'information »<sup>156</sup> particulièrement préoccupante. En effet, en pénalisant indistinctement l'ensemble des atteintes au secret d'Etat sans distinguer le bon grain de l'ivraie, l'état actuel du droit noie les révélations d'importance cruciale pour la démocratie dans le flux incessant des fuites émanant des agences. Or, la majorité d'entre elles – qu'on songe par exemple en France à la « mare aux canards » du Canard Enchaîné – ne correspondent pas tant à un intérêt général qu'à **un appétit du public éclairé pour le gossip, et bénéficient principalement à des cadres des agences du renseignement soucieux de modeler l'opinion publique en leur faveur**. A rebours d'une vision dominante, il paraît peu plausible que le renforcement du secret soit réellement l'objectif poursuivi par les dirigeants des agences. **Il semble s'agir surtout, en étendant le champ de celui-ci, de contrôler les flux d'informations parvenant au public**. Serait-ce pour s'assurer plus aisément l'« hégémonie culturelle » dont parlaient certains auteurs ?
- 54 Or, pour Rahul Sagar<sup>157</sup>, cet état du droit présente le risque de faire peser sur des personnes privées par définition non élues - les médias et leurs sources « lanceurs d'alerte » - un fardeau trop lourd, celui de pallier aux insuffisances institutionnelles et de trouver un le nécessaire équilibre entre sécurité nationale et intérêt général dont parlait Edward Snowden<sup>158</sup>. Parce qu'il est un acteur politique<sup>159</sup> dans un monde - l'organisation, qu'elle soit secrète ou non- qui ne l'est pas et où il représente des valeurs externes - celles d'une société se pensant comme fondée sur les droits de l'Homme - le lanceur d'alerte doit être protégé pour que soit protégée la société toute entière.
- 55 Encore faut-il pour cela effectuer un retour à la source des dérives suscitées. La nécessité de protéger les lanceurs d'alerte ne tient pas tant à l'intérêt qu'il y a à protéger des individus *stricto sensu* qu'à assurer un véritable équilibre des pouvoirs. A cet égard, et comme nous avons eu l'occasion de l'examiner, le caractère absolu du secret n'entrave pas uniquement l'action des lanceurs d'alerte, mais court-circuite également la mission des parlements et des juges. Il faut alors envisager le secret dans une perspective constitutionnelle, comme un **privilège de l'exécutif qui ne peut s'étendre au-delà d'une certaine limite sans faire naître de réels déséquilibres institutionnels**. Plus qu'une cause, le secret est de ce fait une conséquence d'un déséquilibre des pouvoirs jouant, aux Etats-Unis comme en France, au profit du « pouvoir » exécutif. Le professeur Heidi Kitrosser a ainsi souligné de manière brillante et savante que la correction des effets les plus néfastes du secret **ne pouvait se passer d'une redéfinition des équilibres démocratiques**.
- 56 **Cette exigence implique, nécessairement, de réformer les mécanismes de contrôle traditionnels de l'exécutif** - qui sont devenus des mécanismes de contrôle formel faute de pouvoirs - pour en faire des mécanismes de contrôle réel de ces activités<sup>160</sup>.

Certes, une lecture « *originaliste* » de la Constitution aux Etats-Unis <sup>161</sup> et une jurisprudence constructive de la Cour EDH en Europe peuvent constituer des palliatifs à la situation que nous dénonçons, mais ceux-ci ne corrigeront jamais qu'à la marge les excès du secret d'Etat. Faute de corriger ce déséquilibre fondamental et de renforcer le rôle du juge et du parlement, il y a à notre sens **un danger à faire du lanceur d'alerte un « héros de la démocratie »** désormais seul en piste sur le front de la défense des valeurs libérales.

- 57 Le projet de loi renseignement est à vrai dire une **occasion manquée pour instaurer une véritable protection des lanceurs d'alerte**. En effet, les révélations des programmes de surveillance menés par les agences de renseignement nord-américaines ont suscité une vague d'indignation mondiale, qui a elle-même donné naissance à de nombreuses pistes de réforme envisageables pour mieux articuler sécurité et liberté. Faute de s'inscrire dans ce mouvement, le projet de loi maintient un *statut quo* préjudiciable à la fois à la sécurité nationale et au droit du public à l'information. Il s'agit d'un état de fait « *implicitement négocié* »<sup>162</sup>, laissant à voir une situation dans laquelle l'absence de reconnaissance en bonne et due forme du droit à la liberté d'expression des agents du renseignement lanceurs d'alerte favorise les abus de pouvoir et encourage *in fine* les fuites anonymes non responsables. Mais peut-être est-ce le prix à payer pour pouvoir **présenter le secret d'Etat comme une citadelle assiégée** et justifier d'autant plus son renforcement ultérieur ?
- 58 Faute de réelle protection juridique, l'action des lanceurs d'alerte relève donc en dernière analyse du **domaine de l'éthique, et non du domaine du droit**. Le dilemme du lanceur d'alerte, partagé entre la loyauté à l'organisation d'une part, et la loyauté à une certaine forme d'éthique de la conviction **se résout bien souvent et tôt ou tard, comme le rappelle Jens Jensen<sup>163</sup>, par une prise de parole**. Gageons donc que, si d'aventure le secret d'Etat servait de prétexte pour masquer des violations des droits humains, un lanceur d'alerte finirait par faire le choix du « *courage de la vérité* » et de parler sans crainte. Car, comme le rappelait Hannah Arendt, le mensonge en démocratie est toujours moins puissant que la vérité brute<sup>164</sup>.

\*

- 59 **Loi relative au renseignement, votée le 5 mai 2015 par l'Assemblée nationale (petite loi), article 3bis – Dossiers législatifs sur le site du Sénat et celui de l'Assemblée nationale**
- 60 **Peter Omzigt, « La protection des donneurs d'alerte », Conseil de l'Europe, CDCJ(2014), AS/Jur (2015) 06, Strasbourg, mars 2015 (provisoire).**

\*

Les Lettres « Actualités Droits-Libertés » (ADL) du CREDOF (pour s'y abonner) sont accessibles sur le site de la Revue des Droits de l'Homme (RevDH) – Contact

---

## NOTES

1. Cité par Alan Katz, "Government information leaks and the First Amendment." *Cal. L. Rev.* 64 (1976) : 108, p. 11
2. Comme l'a souligné le professeur Alexander Meiklejohn, le premier amendement a d'ailleurs être interprété en ce sens par la Cour Suprême des Etats-Unis. V. Alexander Meiklejohn, "The First Amendment is an Absolute." *Sup. Ct. Rev.*, 1961, p. 245.
3. Pierre Rosanvallon, « *La contre-démocratie, la politique à l'âge de la défiance* ». Paris, Seuil, 2006, 345 p
4. Frank Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information* , Harvard University Press, janvier 2015.
5. Après avoir passé en revue 23 législations d'États-membres du Conseil de l'Europe, le rapport du 25 septembre 2006 portant sur l'équité des procédures judiciaires dans les affaires d'espionnage ou de divulgation de secrets d'Etat » souligne que « tous les systèmes législatifs passés en revue sont susceptibles de donner lieu à des abus » en matière de classification des informations. V. Christos Pourgourides, « Equité des procédures judiciaires dans les affaires d'espionnage ou de divulgation de secrets d'Etat », CDCJ(2006), Doc. 11031, Strasbourg, septembre 2006
6. Paul Stephenson, Michael Levi, « La protection des donneurs d'alerte », Rapport d'étude sur la faisabilité d'un instrument juridique sur la protection des employés qui divulguent des informations dans l'intérêt public, Conseil de l'Europe, CDCJ(2012)9FIN, Strasbourg, décembre 2012, p. 40
7. V., pour une description détaillée de ces programmes et leurs implications sur les droits consacrés par la Conv.EDH : Peter Omzigt, « Les opérations massives de surveillance », Conseil de l'Europe, AS/Jur (2015) 01, Strasbourg, 26 janvier 2014.
8. Ces algorithmes, dont l'explosion des usages correspond à l'explosion parallèle du « Big Data », sont utilisés de manière croissante par les pouvoirs publics en vue d'identifier des profils « à risques ». L'on peut citer par exemple, en France, l'exemple du fichier « PNR » prévu par l'article 17 de la **Loi de programmation militaire du 18 décembre 2013**, qui permet d'identifier les passagers aériens « à risques ».
9. V. Pierre Alonso, Amaelle Guiton, « **Imsi-catchers, des valises aux grandes oreilles** », *Libération*, 15 avril 2015.
10. Il s'agit d'une expression mentionnée pour la première fois par les juges Brandeis et Warren dans un article de 1890, duquel l'on fait dater formellement l'idée de « droit à la vie privée ». V. Neil M. Richards, "The Puzzle of Brandeis, Privacy, and Speech", *Vanderbilt Law Review*, v.63, n.5, pp. 1295-1352. V. également, sur les mutations contemporaines du droit à la protection de la vie privée : Antoinette Rouvroy et Yves Poullet. "Le droit à l'autodétermination informationnelle et la valeur du développement personnel : une réévaluation de l'importance du droit à la protection de la vie privée pour la démocratie.", *Etat de droit et virtualité*. Ed. Karim Benyekhlef & Pierre Trudel. Montréal : Thémis, 2009.
11. V, sur l'effet dissuasif de la surveillance de masse sur la liberté d'expression, l'excellente étude de l'association Pen America : *Global Chilling: The Impact of Mass Surveillance on International Writers*
12. Cour EDH, 8 janvier 2013, Bucur et Toma c. Roumanie, n° 40238/02, §117.
13. Cass Sunstein, « Group Judgments: Statistical Means, Deliberation, and Information Markets » *N.Y.U. L. R EV.* 962, pp. 964-67, 2005.
14. Louis Fischer. "National security whistleblowers", Library of Congress Washington DC Congressional Research Service, 2005.
15. Il s'agit des « Principes globaux de la sécurité nationale et du droit à l'information », publiés le 12 juin 2013, élaborés par 17 ONG et cinq centres universitaires.
16. Arcadio Diaz Terera, « La sécurité nationale et l'accès à l'information », Conseil de l'Europe, CDCJ(2013)13293, Strasbourg, Septembre 2013
17. Comité des Ministres du Conseil de l'Europe, 30 avril 2014, Recommandation CM/Rec(2014)7 aux Etats membres sur la protection des lanceurs d'alerte et exposé des motifs

18. Peter Omtzigt, « Les opérations massives de surveillance en Europe », Conseil de l'Europe, CDCJ(2014), AS/Jur(2015)01, Strasbourg, janvier 2015 ; « La protection des donneurs d'alerte », Conseil de l'Europe, CDCJ(2014), AS/Jur (2015) 06.
19. Parlement Européen, Résolution P7\_TA-PROV(2014)0230 du 12 mars 2014 sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures ».
20. Assemblée générale des Nations Unies, document 68/167 du 18 décembre 2013, « Le droit à la vie privée à l'ère du numérique ».
21. Katy Steinmetz, « The Edward Snowden Name Game: Whistle-Blower, Traitor, Leaker », *Time*, 10 juin 2013.
22. Au cours de la séance du jeudi 16 avril 2015 à l'Assemblée nationale, la députée Isabelle Attarda défend cet amendement de la manière suivante « Cet amendement du rapporteur tel que sous-amendé par notre amendement no 403 est extrêmement respectueux, protecteur et conscient que l'illégalité peut être requise par la hiérarchie elle-même - c'est le cas de l'affaire Snowden. Et s'il colle à la réalité d'une affaire révélée par un agent de la NSA, ce n'est pas pour rien ! Cette affaire a quand même suscité la colère de Mme Merkel, quand celle-ci a su que son pays était écouté, ainsi que celle de nombreux autres gouvernements étrangers ».
23. Conseil d'Etat, Etude annuelle 2014, Le numérique et les droits fondamentaux, adoptée le 17 juillet 2014 par l'assemblée générale du Conseil d'Etat, publiée le 9 septembre 2014.
24. V. Liberty and Security in a Changing World, décembre 2013.
25. La protection dont pourraient bénéficier les lanceurs d'alerte est ainsi calquée sur celles de l'article 6ter du statut général des fonctionnaires qui prévoit un mécanisme de partage de la charge de la preuve en matière discriminatoire.
26. La loi rejoint en cela la proposition du Conseil d'Etat qui suggérait de faire de la Commission Nationale de Contrôle des Interceptions de Sécurité (CNCIS) une Autorité de contrôle des services de renseignement, dotée de moyens et de prérogatives renforcées V. Conseil d'Etat, Etude annuelle 2014, Le numérique et les droits fondamentaux, adoptée le 17 juillet 2014 par l'assemblée générale du Conseil d'Etat, publiée le 9 septembre 2014. Proposition n° 41, p. 323
27. V., pour une critique des récentes évolutions en la matière : R. Perry, « Intelligence Whistleblower Protections : In Brief », Congressional Research Service, 2014.
28. Il ne s'agit là que d'une clause de style car il serait problématique d'essentialiser le terme de « démocratie » dans la mesure où il existe une infinité de conceptions de la « démocratie ».
29. Au cours de la séance du jeudi 16 avril 2015 à l'Assemblée Nationale, le rapporteur de la loi Jean-Jacques Urvoas les décrivait comme « des comportements délictueux, un usage inopportun, voir a-légal, des techniques de renseignement ».
30. V., pour une présentation détaillée, l'on pourra consulter le Rapport d'information sur l'évaluation du cadre juridique applicable aux services de renseignement (14 mai 2013)
31. *Ibid.*
32. V. sur ces textes : Anna Billard, Marc Duranton, Jean-Philippe Foegle et Tristan Martin-Teodorczyk, « Le « milieu du gué » de la protection législative des lanceurs d'alerte », *La Revue des droits de l'homme [En ligne], Actualités Droits-Libertés*, 20 mai 2014.
33. Dans l'arrêt « Garcetti contre Ceballos », la Cour suprême américaine a en effet estimé que, lorsque les agents publics divulguent des informations « Dans le cadre/en vertu [pursuant to] de leurs obligations officielles », ceux-ci ne sont pas à considérer comme des « citoyens » pouvant bénéficier des protections du premier amendement. Les agents publics, s'ils veulent bénéficier d'une protection, doivent donc s'exprimer « en tant que citoyens », et donc, en dehors de l'entreprise.
34. Cour. EDH, Plen., 6 septembre 1978, Klass et autres c. Allemagne, Req. n° 5029/71.
35. Dans l'arrêt Klass, la Cour avait été satisfaite de l'existence d'une commission composée de parlementaires de la majorité et de l'opposition et par une commission dite « G10 » dont les membres sont nommés par la commission parlementaire et exercent leurs fonctions en toute indépendance.
36. Cour EDH, 4e Sect. 18 mai 2010, Kennedy c. Royaume-Uni, Req. n° 26839/05 – ADL du 20 mai 2010. V. Plus largement, sur la jurisprudence de la Cour relative à la surveillance policière : Cour EDH, Division de la recherche, National Security and European case-law, 2013. V. également Isabella Georgieva, « The Right to Privacy under Fire –

Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR », *Utrecht Journal of International and European Law*, n° 31, p. 104

37. Conseil d'Etat, *Etude annuelle 2014, préc.*, Proposition n° 42.

38. V. pour une présentation de ce texte: Thomas Devine, « The Whistleblower Protection Act of 1989: Foundation for the Modern Law of Employment Dissent. », *Administrative Law Review*, 1999, p. 531-579; Paige Whitaker, « The Whistleblower Protection Act: An Overview. » *Law and Law Enforcement Issues*, 2007, p. 213; Shelley Peffer, Aleksandr Bocheko, Rita Del Valle, *et al.* « Whistle Where You Work? The Ineffectiveness of the Federal Whistleblower Protection Act of 1989 and the Promise of the Whistleblower Protection Enhancement Act of 2012 » *Review of Public Personnel Administration*, 2013.

39. La loi ne trouve pas à s'appliquer, selon ses propres termes, aux employés des agences suivantes: “the Federal Bureau of Investigation, the Central Intelligence Agency, the Defense Intelligence Agency, the National Geospatial-Intelligence Agency, the National Security Agency, the Office of the Director of National Intelligence, and the National Reconnaissance Office.”. V. 5 U.S.C. §2302(a)(2)(C).

40. Pub. Law No: 105-272, Title VII. Ce texte amende le *Central Intelligence Agency Act* de 1949 ainsi que l'*Inspector General Act* de 1978 pour y insérer des dispositions protectrices des lanceurs d'alerte. Pour une présentation: Thomas Newcom, « In from the Cold: The Intelligence Community Whistleblower Protection Act of 1998 » *Administrative Law Review*, 2001, p. 1235-1272.

41. La loi définit la « question urgente à résoudre » comme « un problème sérieux ou flagrant, un abus une violation d'une loi ou d'un executive order, ou des manquements liés au financement, à la gestion ou à la mise en œuvre d'une activité de renseignement ». 5 U.S.C. app. 3 §8H(h)(1) ; 50 U.S.C. § 3517(d)(5)(G) (i)

42. Richard Moberly, *The Workplace Law Agenda of the Obama Administration: Whistleblowers and the Obama Presidency: The National Security Dilemma. Empl. Rts. & Employ. Pol'y J.*, 2012, vol. 16, p. 51-629.

43. V., Pour une présentation de la décision et de ses implications: Linda Lewis, « Decision in Kaplan v. Conyers will have “profound” impact on federal government », *Whistleblowing Today*, 21 août 2013. V. également: Alexandra Cumings, « Kaplan v. Conyers: Preventing the Grocery Store Clerk from Disclosing National Security Secrets » *Penn St. L. Rev.*, 2014, vol. 119, p. 553; Charles Pollack., « A Delicate Balance: Federal Employees, Security Clearances, and the Role of the Federal Circuit », *Fed. Cir. BJ*, 2013, vol. 23, p. 133.

44. Presidential Policy Directive 19/PPD-19, 10 octobre 2012. Pour une critique de cette directive: Owen Dunn, Presidential Policy Directive on Whistleblowers Draws Criticism, *WHISTLEBLOWER'S PROTECTION BLOG*, Octobre 2012.

45. V. 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.

46. Richard Moberly, To persons or organizations that may be able to effect action: Whistleblowing recipients, in AJ Brown, David Lewis, Richard Moberly (dir), *International Handbook on Whistleblowing Research*, juillet 2014

47. « Lorsque la Commission nationale de contrôle des techniques de renseignement estime qu'une autorisation a été accordée en méconnaissance du présent livre ou qu'une technique de recueil de renseignement a été mise en œuvre en méconnaissance du présent livre, ainsi que dans les autres cas prévus au présent livre, elle adresse au service concerné ainsi qu'au Premier ministre une recommandation tendant à ce que la mise en œuvre de la technique concernée soit interrompue et les renseignements collectés détruits.

« Le Premier ministre informe sans délai la commission des suites données à ses recommandations.

« Lorsque le Premier ministre ne donne pas suite à ses avis ou recommandations ou lorsqu'elle estime que les suites qui y sont données sont insuffisantes, la commission peut décider, après délibération, de saisir le Conseil d'État »

48. V. Marc Guillaume, « La réforme du droit du secret de la défense nationale », *RFDA* 1998 p. 1223. V, plus largement : François Gauvin, « Regard critique sur la loi 8 juillet 1998 portant création de la commission secret défense », *Dr. pén.* 1999, chron. N° 12 ; Christophe Guettier, « Une nouvelle autorité administrative indépendante : la commission consultative du secret de la défense nationale » *Les Petites affiches*, 22 janv. 1999, p. 5 ; Dominique Richard, « Secret défense : entre comitologie et État de droit », *D.* 1999, chron. p. 270.

49. V. Art. L. 2312-1 et suivants du Code de la défense. V. également Roseline Letteron, « Le secret de la défense nationale bientôt devant la cour européenne ? », *Libertés Liberté Chérie*, 7 novembre 2012.

50. Rapport de la commission consultative du secret de la défense nationale, bilan 1998/2004, La Documentation française, Paris, 2005 p. 23

51. Comme le souligne Christian Vigouroux, « l'agent public ne doit pas se complaire dans l'alerte de précaution » et la notion de « bonne foi », commune à la loi du 11 octobre 2013 et à la loi du 6 décembre 2013, exige que le salarié ou agent public apporte des éléments de nature à démontrer la réalité de l'atteinte. V. Christian Vigouroux, *Déontologie des fonctions publiques*, Paris, Dalloz, 2006, p. 141.

52. La Recommandation CM/Rec(2014)7 aux Etats membres sur la protection des lanceurs d'alerte du 30 avril 2014 estime néanmoins que la personne ayant fait un signalement ou ayant révélé des informations « ne devrait pas

perdre le bénéfice de sa protection au seul motif qu'elle 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. » (Recommandation précitée, p. 41).

53. C'est la solution adoptée de longue date par le Conseil d'État : CE, Ass., 11 mars 1955, secr. d'État guerre c/ Coulon, Rec. CE 1955, p. 149 et, plus récemment : CE, ass., 6 nov. 2002, Moon Sun Myung, Rec. CE 2002, p. 380. V, sur ce système : Danièle Lochak, « Secret, sécurité et liberté », *Cahiers du CURAPP*, 1988, Information et transparence administratives, PUF, p. 51-70 ; Vincent Tchen, « Le juge et les données couvertes par la loi de 1978 », *Droit administratif*, n° 12, décembre 2001, pp. 23-25.

54. CE, 20 févr. 2012, Min. Défense, req. n° 350382.

55. V., Dovydas Vitkauskas, Grigoriy Dikov,, « Protecting the right to a fair trial under the European Convention on Human Rights », Conseil de l'Europe, 2012; D. Jočienė, Overview of the Standards Regarding Evidence in Court Proceedings According to Art. 6 of the ECHR, 2015.

56. Cour EDH, 3e sect., 12 mai 2000, Khan c. Royaume-Uni, Req. 35394/97, §§34-40.

57. Cour EDH, Gr. Ch, 16 février 2000, Rowe et Davis c. Royaume-Uni, Req. n° 28901/95 ; Cour EDH, 4e sect. 5 février 2002, Atlan c. Royaume-Uni, Req. n° 36533/97 ; Cour EDH, 2e sect., 24 juin 2003, Dowsett c. Royaume-Uni, Req. n° 39482/98.

58. Cour EDH, Gd Ch. 16 février 2000, Fitt c. Royaume-Uni, Req. n° 29777/96, §§45-46.

59. Cour EDH, 4e sect., 7 juin 2007, Botmeh et Alami c. Royaume-Uni, Req. n° 15187/03, §§42-45.

60. 50 U.S.C. §3517(d)(5)(A) ; 5 U.S.C. app. §8H(a)(1)(A), (B).

61. 50 U.S.C. §3517(d)(5)(A) ; 5 U.S.C. app. §8H(a)(1)(A), (B). L'inspection générale doit fournir un audit indépendant et objectif des activités dénoncées. Si ces inspections jouent un rôle croissant dans le contrôle interne des activités de renseignement, certains professeurs soulignent le manque d'indépendance de celles-ci. V sur ce point: Shirin Sinnar, « Protecting Rights from Within? Inspectors General and National Security Oversight », *Inspectors General and National Security Oversight (June 11, 2013)*, 2013, vol. 65.

62. 50 U.S.C. §3517(d)(5)(C); 5 U.S.C. app. §8H(c). V., sur le rôle de ces commissions et les insuffisances du contrôle qu'elles opèrent : Heidi Kitrosser, « Congressional Oversight of National Security Activities : Improving Information Funnels », *Cardozo L. Rev.*, 2007, vol. 29, p. 1049.
63. 50 U.S.C. §3517(d)(5)(B) ; 5 U.S.C. app. §8H(b).
64. 50 U.S.C. §3517(d)(5)(C) ; 5 U.S.C. app. §8H(c).
65. 50 U.S.C. §3517(d)(5)(D)(ii)(I) ; 5 U.S.C. app. §8H(d)(2)(A)
66. *Ibid.*
67. V. Peter Omzigt ; « La protection des donneurs d'alerte », Conseil de l'Europe, CDCJ(2014), AS/Jur (2015) 06,, Strasbourg, mars 2015 (provisoire), §86.
68. Presidential Policy Directive 19/PPD-19, 10 octobre 2012.
69. S. 1681 ; Pub.L. 113-126.
70. V. Peter Omzigt ; « La protection des donneurs d'alerte », *préc.*, §68
71. V. Deutsche Welle du 10 juillet 2014, « Whistleblower law expands protection to US intelligence agents ». Cité par V. Peter Omzigt ; « La protection des donneurs d'alerte », *préc.*, §68
72. V. Tom Devine, Shelley Walden, « International best practices for Whistlelower protection », Government Accountability Project, Mars 2013, p. 2.
73. V. sur ce point, Jean-Philippe Foegle, Stephen Pringault, « Les 'lanceurs d'alerte' dans la fonction publique, les mutations contemporaines d'une figure traditionnelle de l'agent public », *AJDA*, 2014, p. 2256.
74. V. not. Stephen Pringault, « L'obligation de réserve des agents publics face au devoir de dénonciation d'infractions pénales. Une inadaptation du droit français à la problématique du whistleblowing », *DA* 2012, étude 8.
75. CAA Bordeaux, 5 nov. 2011, *M. Eric Carré*, req.n° 11BX00204.
76. CE 27 juill. 2005, Stéphane X., n° 260139.
77. V. CAA Paris, 31 décembre 2014, Mme Souid, n° 13PA00914. V. également les conclusions du rapporteur public : Christelle Oriol, « Les contours du devoir d'alerte des agents publics » *AJDA*, 30 mars 2015, pp. 639-645.
78. V. Alexander Bickel, « Domesticated civil disobedience: the First Amendment, form Sullivan to the Pentagon Papers », *The morality of consent*, 1975, p. 55-88. V. également: Joel M. Gora, « The Pentagon Papers Case and the Path Not Taken: A Personal Memoir on the First Amendment and the Separation of Powers », *Cardozo L. Rev.*, 1997, vol. 19, p. 1311; John Cary Sims, « Triangulating the Boundaries of Pentagon Papers » *Wm. & Mary Bill Rts. J.*, 1993, vol. 2, p. 341; Vincent Blasi, « The checking value in First Amendment theory », *Law & Social Inquiry*, 1977, vol. 2, no 3, p. 521-649.
79. 283 U.S. 697 (1931).
80. *Ibid.*
81. *Id.*
82. *Id.*
83. *Id.*
84. Melissa Opper, « WikiLeaks: Balancing First Amendment Rights with National Security. *Loy. LA Ent. L. Rev.*, 2010, vol. 31, p. 237. V., dans un sens contraire: Janelle Allen, « Assessing the First Amendment as a Defense for WikiLeaks and Other Publishers of Previously Undisclosed Government Information », *USFL Rev.*, 2011, vol. 46, p. 783;Christina Wells, « Contextualizing Disclosure's Effects: WikiLeaks, Balancing, and the First Amendment » *Iowa L. Rev. Bull.*, 2012, vol. 97, p. 51.
85. *New York Times Co. v. Sullivan*, 376 U.S. 254 (1964 )
86. *ibid* (opinion concordante du juge Potter Stewart)
87. V. B. Nimmer, "National Security Secrets v. Free Speech: The Issues Left Undecided in the Ellsberg Case", *Stanford Law Review*, 1974, p. 311-333.
88. *Pickering v. Board of Education* , 391 U.S. 563 (1968)

89. Stephen Vladeck, « The Espionage Act and National Security Whistleblowing after Garcetti », *Am. UL Rev.*, 2007, vol. 57, p. 1531.
90. *Snepp v. United States* 444 U.S. 507 (1980)
91. *Ibid.*, note 95
92. *Id.*
93. V. Martin Linski, « *Impact: How the press affects federal policymaking* », New York, WW Norton, 1986. Cité dans: David Pozen E. , « The Leaky Leviathan: Why the Government Condemns and Condone Unlawful Disclosures of Information », *Harv. L. Rev.*, 2013, vol. 127, p. 512.
94. V. William E. Lee, « Deep Background: Journalists, Sources, and the Perils of Leaking » , *Am. UL Rev.*, 2007, vol. 57, p. 1453 ; Bejesky, Robert. "National Security Information Flow : From Source to Reporter's Privilege." . *Thomas L. Rev.* 24, 2011, p39 ; , RonNell Andersen Jones, « Media Subpoenas : Impact, Perception, and Legal Protection in the Changing World of American Journalism » *Wash. L. Rev.*, 2009, vol. 84, p. 317.
95. V. Anna Billard, Marc Duranton, Jean-Philippe Foegle et Tristan Martin-Teodorczyk: « Le « milieu du gué » de la protection législative des lanceurs d’alerte », *préc.*
96. V. Peter Omzigt ; « La protection des donneurs d'alerte », *préc.* §34
97. *Ibid.*
98. V. Yochai Benkler, « A Public Accountability Defense for National Security Leakers and Whistleblowers. *Harv. L. & Pol'y Rev.*, 2014, vol. 8, p. 281-471.
99. *Ibid.*
100. *Id.* V également, du même auteur: Yochai Benkler, « A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate », *Harv. CR-CLL Rev.*, 2011, vol. 46, p. 311.
101. Heidi Kitrosser, « Free Speech Aboard the Leaky Ship of State: Calibrating First Amendment Protections for Leakers of Classified Information » *J. Nat'l Sec. L. & Pol'y*, 2012, vol. 6, p. 409.
102. *Ibid.*, note 104.
103. Pub.L. 96-456, 94 Stat. 2025.
104. François Delon, « Une publication du secrétaire général de la défense et de la sécurité nationale dans la revue Défense de l’IHEDN (mars-avril 2009), sur le thème du « Secret de la défense nationale ».
105. André Vitu, « Crimes et délits contre la sûreté de l’État », *JCL Pénal*, Art. 70-103, Code pénal, fascicule 8-196.
106. Cass. crim., 11 juin 1935 : Bull. crim., n° 91 ; S. 1937, 1, p. 119 ; Gaz. Pal. 1935, 2, p. 503. Cité par : André Vitu, *ibid*
107. Cass. crim., 1er févr. 1935 : *DH 1935*, p. 181 cité par André Vitu, *ibid.*
108. CA Paris, 13 juill. 1911 : Gaz. Pal. 1911, 2, p. 250 ; Journ. Parquets 1911, 1, p. 160 cité par André Vitu, *ibid.*
109. Qui concerne les « priorités gouvernementales en matière de défense et de sécurité nationale et dont la divulgation est de nature à nuire très gravement à la défense nationale » (Article R.2311-3 du Code de la défense).
110. C’est-à-dire les « informations et supports dont la divulgation est de nature à nuire gravement à la défense nationale » (*ibid.*).
111. C’est-à-dire les « informations et supports dont la divulgation est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d’un secret de la défense nationale classifié au niveau Très Secret-Défense ou Secret-Défense ». (*ibid.*).
112. Article R. 2311-7 du Code de la défense.
113. Article R 2311-5 et R 2311-6 du Code de la défense.
114. V. Dirk Voorhoof, “The right to freedom of expression and information under the European Human Rights system: towards a more transparent democratic society”, *EUI Working Paper* (Florence: EUI RSCAS 2014/12) 22 p.. V. également: Wouter Hins, Dirk Voorhoof, « Access to state-

held information as a fundamental right under the European Convention on Human Rights », *European Constitutional Law Review*, 2007, vol. 3, no 01, p. 114-126.

**115.** Cour EDH, GC, 12 février 2008, Guja c. Moldavie, req. N° 14277/04 ; Cour EDH, 2e Sect., 8 janvier 2013, Bucur et Toma c. Roumanie, Req. n° 40238/02.

**116.** V. en ce sens, Cour EDH, Gr. Ch., 21 janvier 1999, Fressoz et Roire c. France, Req. n° 29183/95 ; Cour EDH, Radio Twist c. Slovaquie, Req. n° 62202/00 ; Cour EDH, 4e Sect., 7 juin 2007, Dammann c. Suisse, req. n° 77551/01, Cour EDH, 2e Sect., 28 juin 2011, Pinto Coelho c. Portugal, Req. n° 28439/08.

**117.** Cour EDH, 16 décembre 1992, Hadjianastassiou c. Grèce, Req. N° 12945/8 ; Cour EDH, Gr.Ch., 10 décembre 2007, Stoll c. Suisse, Req. n° 69698/01, § 130.

**118.** Cour EDH, 2e Sect., 8 janvier 2013, Bucur et Toma c. Roumanie, Req. n° 40238/02. §102

**119.** V. Gabriel Schoenfeld, « Necessary secrets: National security, the media, and The Rule of Law », 2010.

**120.** U.S. CONST. art. III, § 3, cl. 1. : “Whoever, owing allegiance to the United States, levies war against them or adheres to their enemies, giving them aid and comfort within the United States or elsewhere, is guilty of treason and shall suffer death, or shall be imprisoned not less than five years and fined under this title but not less than \$ 10,000 ; and shall be incapable of holding any office under the United States.”.

**121.** V. Mary-Rose Papandrea, « .Leaker Traitor Whistleblower Spy: National Security Leaks and the First Amendment », *BUL Rev.*, 2014, vol. 94, p. 478.

**122.** V. Carlton F.W. Larson, « The Forgotten Constitutional Law of Treason and the Enemy Combatant Problem » 154 U.P.A. L. REV., 2006, P.863.

**123.** V. d'ailleurs, plaidant en ce sens: Benjamin Lewis, « An Old Means to a Different End: The War on Terror, American Citizens... and the Treason Clause » *Hofstra L. Rev.*, 2005, vol. 34, p. 1215.

**124.** Haupt v. United States, 330 U.S. 631, 644 (1947).

**125.** Carlton F.W. Larson, art. Préc.

**126.** V. Eric Litchblau, American in Qaeda Tapes Accused of Treason, *NY Times*, 12 octobre 2006

**127.** Tom Bell, « Treason, Technology, and Freedom of Expression », 37 *ARIZ. ST. L.J.* 999, 2005, p. 1002

**128.** 10 U.S.C. § 904

**129.** Charlie Savage, Soldier Admits Providing Files to WikiLeaks, *N.Y. Times*, 1er mars 2010

**130.** V. Mary-Rose Papandrea, « Leaker Traitor Whistleblower Spy: National Security Leaks and the First Amendment », *BUL Rev.*, 2014, vol. 94, p. 506.

**131.** 22 C.M.R. 144, 157 (C.M.A. 1956)

**132.** Pub.L. 65-25, 40 Stat. 217.

**133.** Pour un historique et une présentation (critique) de cette loi, voir: Timothee Ericson, "Building Our Own "Iron Curtain": The Emergence of Secrecy in American Government", *American Archivist*, 2005.

**134.** U.S.C. Titre 18, Partie 1, Chapitre 37.

**135.** H.R. DOC. NO. 106-309, at 1-2 (2000).

**136.** 18 U.S.C. §793(a)-(f).

**137.** C. Dewey, « Manning was charged under the Espionage Act. It doesn't have a proud history. », *Washington Post*, 31 juillet 2013.

**138.** P. Finn, S. Horwitz, « U.S charges Snowden with espionage », *Washington Post*, 21 juin 2013.

**139.** V., pour une présentation complète des « cas » de lanceurs d'alerte poursuivis sur ce fondement : Daniel D'isidoro, « Protecting Whistleblowers and Secrets in the Intelligence Community », *Harvard National Security Journal Online*. Septembre 2014; Jesselyn Radack et Kathleen McClellan « The Criminalization of Whistleblowing », *Am. U. Labor & Emp. LF*, 2011, vol. 2, p. 57.

140. V. Charlie Savage, « Former CIA Operative Pleads Guilty in Leak of Colleague's Name », *NY Times*, 23 octobre 2012.
141. *United States v. Morison*, 844 F.2d 1057, 1063-64 (4th Cir. 1988)
142. *Ibid.*
143. *Id.*
144. V. En ces sens: David E Pozen « The Leaky Leviathan: Why the Government Condemns and Condone Unlawful Disclosures of Information », *Harv. L. Rev.*, 2013, vol. 127, p. 512.
145. En ce sens: Vincent Blasi, « *The Checking Value in First Amendment Theory* » 1977 AM. B. FOUND. RES. J. 521, p. 609
146. Référence au livre « Alice au pays des merveilles » de Lewis Carroll. Le livre est consultable en ligne sur le site de la British Library [www.bl.uk](http://www.bl.uk)
147. Emmanuel Kant, « *Vers la paix perpétuelle : (suivi de) Que signifie s'orienter dans la pensée ? ; (suivi de) Qu'est-ce que les Lumières ? : et autres textes* », Flammarion, 2006.
148. Norberto Bobbio, « *Le futur de la démocratie* » Seuil, 2007 (V. Le chapitre sur le « pouvoir occulte »)
149. V. Guy Carcassonne, « Le trouble de la transparence », *Pouvoirs* 2/2001 (n° 97) , p. 17-23
150. David Cole, Federico Fabbrini, Arianna Vedeschi (dir.), « *Secrecy, National Security and the Vindication of Constitutional law* », Edward Elgar Publishing, 1er janvier 2013
151. Margaret Kwoka, « Leaking and Legitimacy. », *UC Davis Law Review, Forthcoming*, 2014, p. 14-49.
152. V. John Keane, « *The life and death of democracy* », Simon and Schuster, 2009.
153. Heidi Kitrosser, « What if Daniel Ellsberg Hadn't Bothered », *Ind. L. Rev.*, 2011, vol. 45, p. 89.
154. Hannah Arendt, « *Du mensonge à la violence* », Presses Pocket, 1991, p. 46.
155. Jürgen Habermas, « Civil disobedience: litmus test for the democratic constitutional state ». *Berkeley Journal of Sociology*, 1985, pp. 95-116.
156. V. John Keane et al. « *Monitory democracy and media-saturated societies* », 2009.
157. V. Rahul Sagar, « *Secrets and leaks: the dilemma of state secrecy* » Princeton University Press, 2013, p. 275
158. Extrait de l'audition d'Edward Snowden par l'Assemblée parlementaire du Conseil de l'Europe.
159. Fred Alford, « *Whistleblowers: Broken lives and organizational power* », Cornell University Press, 2002, p. 97
160. Kheidi Kitrosser, « *Reclaiming Accountability: Transparency, Executive Power, and the US Constitution* », University of Chicago Press, 2015.
161. *Ibid.*
162. David McCraw et , Stephen Gikow, « The End to an Unspoken Bargain: National Security and Leaks in a Post-Pentagon Papers World » *Harv. CR-CLL Rev.*, 2013, vol. 48, p. 473.
163. J. Jensen, « Ethical tension points in whistleblowing. » *Journal of Business Ethics*, 1987, vol. 6, no 4, p. 321-328.
164. Hannah Arendt, « *Du mensonge à la violence* », préc.

---

## RÉSUMÉS

*Le 5 mai 2015, l'Assemblée Nationale a adopté en première lecture le projet de loi sur le renseignement, souvent présenté comme un « Patriot Act » à la française. Cette loi, qui devrait être adoptée le 9 juin 2015 par le Sénat, insère au sein du Code de la Sécurité Intérieure un article L.855-3 qui crée un statut pour les lanceurs d'alerte travaillant au sein des agences de renseignement. L'article prévoit une protection contre les discriminations et instaure un système ad hoc de dénonciation des atteintes à la vie privée des citoyens. Il s'agit d'un renforcement inédit du statut du lanceur d'alerte, qui doit être sans nul doute salué à l'heure où un rapport du Conseil de l'Europe se prononce pour la première fois en faveur d'une protection accrue pour les « agents secrets » donneurs d'alerte. Mais le caractère illusoire de cette protection doit également être souligné : une comparaison de récentes évolutions législatives aux États-Unis permet d'en souligner aisément les limites. A rebours d'un standard international émergent, le champ de la protection ainsi instaurée enserme le lancement d'alerte dans l'étroit carcan de mécanismes de régulation trop entravés par les exigences du secret pour être réellement efficace. Aux États-Unis comme en France, la protection des « agents secrets » lanceurs d'alerte reprend bon gré mal gré le ressort comique du « triangle amoureux » des vaudevilles. Ici, le public apparaît comme le mari trompé d'une relation ambiguë entre le lanceur d'alerte et les organismes de contrôle des activités de renseignement. Au risque que cette curieuse comédie se mue en une véritable tragédie pour les lanceurs d'alerte et pour la société toute entière.*

## AUTEUR

**JEAN-PHILIPPE FOEGLE**

Doctorant en droit public (CREDOF - Université Paris Ouest Nanterre) et allocataire doctoral (Conseil régional d'Ile de France)