GUIDES TO GOOD GOVERN-ANCE

N° 06

Équilibre entre transparence et confidentialité dans le secteur de la défense : enseignements tirés des bonnes pratiques internationales

Centre for Integrity in the Defence Sector

NATO OTAN

CENTRE POUR L'INTÉGRITÉ DANS LE SECTEUR DE LA DÉFENSE

Le Centre pour l'intégrité dans le secteur de la défense (CIDS) favorise l'intégrité, les mesures de lutte contre la corruption et la bonne gouvernance dans le secteur de la défense. En collaboration avec ses partenaires norvégiens et internationaux, il a pour but de renforcer les compétences, de sensibiliser l'opinion et de fournir des moyens pratiques afin de limiter les risques de corruption. Le CIDS a été créé en 2012 par le ministère de la Défense norvégien.

À PROPOS DE L'AUTEUR

Francisco Cardona est un expert international associé au CIDS. Il est un spécialiste renommé de l'élaboration et l'évaluation des réformes de la fonction publique et de l'administration publique, du droit et de la justice administratifs, des politiques de lutte contre la corruption et du renforcement des institutions. Son expérience s'étend de son Espagne natale, où il a poursuivi une carrière dans la fonction publique, aux organisations internationales, notamment au programme SIGMA de l'OCDE, où il a passé 15 ans en tant qu'analyste principal de politiques dans le domaine de la gouvernance publique. Il conseillait alors 25 pays en transition et en développement d'Europe de l'Est, d'Afrique, d'Amérique latine et de la région des Caraïbes. Juriste diplômé de l'université de Valence (1976), il est titulaire de plusieurs masters d'administration publique.

AVANT-PROPOS

Les guides de bonne gouvernance du CIDS ont pour vocation première de présenter les questions clés intéressant la bonne gouvernance. Les guides se veulent concis sans pour autant simplifier à l'extrême les questions abordées.

Dans ce sixième livret, l'auteur remet en question le concept de confidentialité dans le secteur de la défense. Ce faisant, il s'interroge sur le point d'équilibre à trouver entre le libre accès à l'information et la limitation plus ou moins stricte de cet accès dans une société démocratique dotée d'un gouvernement ouvert. Il pose aussi la question de savoir à quel moment la restriction de l'accès à l'information se révèle nécessaire dans l'intérêt de la sécurité nationale, ce qui nous renvoie au droit des citoyens à bénéficier de la protection de l'État.

Le présent guide a été écrit par Francisco Cardona, expert international principal au CIDS. Je tiens à le remercier de sa contribution à l'étude de cette importante thématique touchant à la bonne gouvernance, qui s'est trouvée au cœur du débat public ces dernières années et restera probablement d'actualité dans les années à venir.

Je souhaiterais également remercier l'éditeur du CIDS, Bård Bredrup Knutsen, et notre coordonnatrice des publications, Åse Marie Fossum, pour leurs contributions au présent guide.

Le CIDS espère que le présent ouvrage intéressera un grand nombre de lecteurs du secteur public, y compris au sein de la défense, mais aussi un large public extérieur. Trouver le juste équilibre entre transparence et confidentialité est indispensable au bon fonctionnement d'une société démocratique.

Si vous avez des observations sur le guide, n'hésitez pas à en faire part au CIDS.

Oslo, le 24 avril 2018

Per Christensen
Directeur

TABLE DES MATIÈRES

Introduction

Le présent guide offre un bref aperçu des bonnes pratiques appliquées dans les pays membres de l'Union européenne (UE) et de l'Organisation de coopération et de développement économiques (OCDE) pour préserver la confidentialité de l'information publique dans le secteur de la défense et de la sécurité nationale, tout en promouvant le droit général du public à accéder à l'information détenue par les pouvoirs publics. Il vise à proposer des politiques permettant de promouvoir un gouvernement ouvert, de favoriser l'accès à l'information et de donner aux citoyens les moyens de prendre des décisions éclairées sur l'efficacité de l'action de l'État, tout en fixant les limites à respecter pour assurer la bonne protection des secrets d'État dans les domaines sensibles pour la sécurité nationale, la défense et le renseignement, ainsi que pour la lutte contre la corruption et la criminalité.

La transparence et la publicité de l'information sont d'excellents moyens de prévenir la corruption, l'incurie administrative et la mauvaise gouvernance. Une démocratie ne peut s'épanouir dans le secret. De fait, si le secret prévaut, le régime politique devient par nature antidémocratique, puisque ses citoyens sont exclus du processus politique. L'exercice du pouvoir peut alors échapper à tout contrôle, rendant impossible la reddition des comptes chère à la démocratie. Toutefois, il peut être nécessaire de restreindre l'accès du public à l'information pour préserver le bon fonctionnement de la démocratie dans un État gouverné avec efficience. Par conséquent, la divulgation d'informations publiques et les limites imposées à cet exercice devraient, au même titre, servir l'intérêt général.

Le cadre conceptuel : l'argument de la sécurité nationale pour justifier la confidentialité

Sur le plan conceptuel, nous partons de l'hypothèse qu'un gouvernement ouvert et un accès libre à l'information, au même titre que les limitations plus ou moins strictes de cet accès, servent l'intérêt public. Selon le principe général reconnu sur le plan international, les gouvernements doivent promouvoir le « droit de savoir », tout en instaurant des limites raisonnables qui lui permettront de protéger la confidentialité de certaines informations publiques. Ces limites sont indispensables à la bonne gestion de l'action de l'État dans certains domaines, notamment ceux qui concernent la sécurité et la défense nationales.

Avec le secret, le principal problème est de déterminer à quel moment et par quels moyens il devient légitime de restreindre l'accès du public à l'information. Toute démocratie en bonne santé aspire à pouvoir garantir l'accès adéquat du public à l'information, tout en fixant certaines limites légitimes qui viendront restreindre cet accès. Le juste équilibre à trouver entre ces deux considérations sera en grande partie fonction de l'histoire, des valeurs sociétales et d'autres facteurs culturels propres à chaque pays. C'est pourquoi il est difficile de déterminer s'il existe des normes internationales susceptibles d'aider les États à opérer les bons arbitrages (Transparency International UK, 2014). Dans la pratique, il n'existe pas de normes internationales ad hoc, mais les débats intellectuels et les tentatives visant à établir certains principes généraux se sont multipliés ces dernières années[1].

Si elle n'est soumise à aucun contrôle, la protection du secret et de la confidentialité épouse vite une conception très large et extensive. Certains services de l'État chargés de la sécurité nationale, de la défense, des enquêtes judiciaires, du renseignement ou de la lutte contre le terrorisme ont tendance à tenir secrètes toutes les activités qu'ils entreprennent, même si c'est, dans la pratique, une entrave au droit des citoyens de s'informer sur l'action du gouvernement. Outre les coûts élevés à supporter pour faire tourner la « machine institutionnelle du secret », le recours intensif et extensif à la confidentialité tend à mettre à mal la confiance citoyenne dans les institutions gouvernementales et finit par affaiblir la légitimité démocratique. En outre, la protection outrancière du secret tend à favoriser davantage les erreurs et les actes illicites que la transparence et le droit de regard citoyen, car le défaut de transparence complique l'exercice de la vigilance citoyenne et la correction des mauvaises pratiques. Par conséquent, à plus long terme, le recours excessif au secret est susceptible de représenter une menace plus grande

1 Voir *The Tshwane Principles* (2013) : https://www.opensocietyfoundations.org/fact-sheets/tshwane-principles-national-security-and-right-information-overview-15-points (pour la version française intégrale des principes de Tshwane, voir : https://www.justiceinitiative.org/uploads/7a3ed0c9-a694-4843-8a1a-0790e749c9d0/tshwane-french-20150209_0.pdf).

pour la sécurité nationale que l'ouverture.

Pour reprendre un argument avancé par certains responsables publics, notamment aux États-Unis, la mobilisation à l'excès du secret « est aujourd'hui un obstacle injustifié au partage de l'information au sein et à l'extérieur des instances gouvernementales, ce qui se fait au détriment de la politique de l'État » (Aftergood, 2008, page 400). On est ici face au problème de surclassification, à savoir que les services détenteurs de l'information tendent à classifier l'information à un niveau bien supérieur à ce qui est strictement nécessaire.

Tout système de classification vise à prévenir la divulgation d'informations susceptibles de mettre en péril la sécurité nationale, mais le flou entourant des notions telles que la « sécurité nationale » et les « menaces pour la sécurité de l'État » laisse le champ largement ouvert à une protection outrancière du secret. La difficile distinction à opérer entre informations factuelles et informations subjectives rend ardu l'établissement de critères bien définis pour une classification correcte de l'information.

La notion même de classification appropriée est très difficile à appréhender, mais, au plan conceptuel, nous pourrions poser pour principe qu'une classification sera jugée « appropriée » dès lors qu'elle est raisonnable et s'écarte le moins possible des valeurs démocratiques que sont l'ouverture, la transparence et le libre accès à l'information. En d'autres termes, nous pourrions convenir qu'une limitation de la transparence est raisonnable si elle a) est exceptionnelle et b) protège d'importants intérêts de sécurité nationale. Cette conclusion présuppose qu'il existe des informations dans le secteur de la défense et de la sécurité nationale dont la tenue secrète n'est pas essentielle à la protection de la sécurité nationale et qui peuvent donc être – en tout ou partie – divulguées en toute sécurité.

Dans certains pays démocratiques, il persiste à ce jour une conception traditionnelle selon laquelle la transparence ne serait qu'une simple exigence citoyenne, tandis que le secret, sur l'autel de la sécurité nationale, servirait l'intérêt public. Par exemple, en France, Jean-Marc Sauvé, vice-président du Conseil d'État, a déclaré dans un exposé présenté à l'Assemblée nationale (chambre basse du parlement français), le 5 juillet 2011 : « C'est dans de telles voies qu'il faut poursuivre pour tracer la ligne de partage entre les intérêts publics légitimes postulant le secret et la transparence requise par les citoyens » (Sauvé, 2011, page 6). Il pose en cela l'hypothèse que le sceau du secret protège l'intérêt public, tandis que la transparence, loin de servir ce même intérêt, n'est qu'une simple exigence motivée par la curiosité des citoyens et des journalistes. C'est une hypothèse très discutable. L'expérience montre que la promotion de la transparence est l'un des meilleurs moyens de protéger l'intérêt public, car elle contribue à faire en sorte que les pouvoirs publics rendent des comptes aux citoyens et aux autres mécanismes de contrôle démocratique. Ainsi, on peut voir dans la transparence, et non le secret, un moyen de combler un « fossé qui se creuse naturellement entre l'État et les citoyens » (Fenster, 2010, page 619).

Il est largement admis au plan international que la transparence de la politique publique et des mesures prises par les pouvoirs publics devrait constituer la règle, le secret faisant figure d'exception. De plus, chaque exception doit pouvoir être justifiée : elle ne sera défendable que si elle est légitime. Elle ne sera légitime que s'il peut être démontré qu'elle est destinée à protéger les intérêts réels de la sécurité nationale.

Face à la nécessité de distinguer le secret légitime de celui qui ne l'est pas, un certain contrôle doit être assuré par des autorités indépendantes du classificateur. Cette fonction de contrôle indépendant peut être exercée par les juridictions ou par

des instances publiques plus spécialisées, dont le rôle sera de déterminer si les intérêts de la sécurité nationale invoqués pour classifier l'information sont bien réels et revêtent une importance suffisante. Sans mécanismes de contrôle externe, la décision de classifier ou non l'information est entièrement suspendue à l'exercice d'un pouvoir discrétionnaire, fort probablement doublé d'un caractère arbitraire. Toutefois, comme nous le verrons ci-après, les juridictions ont de tout temps abordé avec une extrême retenue – et elles tendent encore à le faire – la rétention d'informations par les agences de sécurité ou de renseignement.

D'un point de vue théorique, une totale transparence n'est pas souhaitable et n'est probablement pas possible, comme nous l'avons vu plus haut. En outre, l'État interviendra toujours dans certains domaines obscurs ou ambigus. Comme le souligne Fenster (2010, page 623), il y a souvent un espace intermédiaire entre le secret et la transparence, si bien que l'un n'est pas nécessairement l'antithèse de l'autre. Dans la pratique, secret et transparence ne renvoient pas à des réalités contrastées et opposées, car ces deux notions reposent sur des bases institutionnelles séparées, structurellement différentes (Riese, 2014, page 14).

Plus de transparence ne signifie pas forcément moins de secret, mais l'amélioration de la qualité assurera une meilleure protection de la confidentialité. En revanche, plus de transparence signifie que la protection s'étendra exclusivement aux besoins réels en matière de confidentialité. Les politiques de transparence sont relativement nouvelles dans le paysage institutionnel de la plupart des pays, tandis que le secret est ancré dans des traditions établies de longue date. Les valeurs et intérêts sous-tendant ces différentes traditions demeurent à ce jour hétérogènes et quelque peu contradictoires. La difficulté réside donc dans l'harmonisation progressive de l'institutionnalisation du droit de savoir et de la protection des besoins réels en matière de confidentialité, à la fois dans les structures organiques compétentes et dans la pratique des gouvernements. La recherche d'une cohérence accrue entre ces deux pendants politiques devrait idéalement conduire à la mise en place d'une politique unique intégrée et à l'institutionnalisation plus harmonieuse au sein du gouvernement d'une politique d'accès à l'information, qui soit conforme aux besoins nationaux en matière de sécurité.

Néanmoins, la notion de « sécurité nationale » est extrêmement fuyante, revêtant des acceptions variables selon les contextes nationaux, ce qui la rend encore plus complexe. Dans la majorité des pays européens étudiés par Jacobsen (2013), la sécurité nationale s'étend à des degrés divers aux relations internationales et aux menaces pour la sécurité intérieure. En d'autres termes, il n'existe pas forcément une ligne de partage évidente.

Pour déterminer si le secret est ou non légitime au sein de l'État, Afterwood (2009, pages 402-403) propose trois catégories pratiques de secret, tout en reconnaissant que, dans le cadre de l'action publique, il est toujours difficile de distinguer le secret légitime de celui qui ne l'est pas et de protéger le premier tout en dénonçant le second :

1. **Secret réel de la sécurité nationale :** secret destiné à protéger des informations qui exposeraient la sécurité du pays à une menace identifiable, en compromettant sa défense ou la conduite de ses relations extérieures. La rétention de ces informations n'est pas sujette à controverse, la logique sous-tendant tous les systèmes de classification étant respectée et l'usage du secret étant de nature à servir au mieux l'intérêt public.

2. **Secret bureaucratique :** tendance des bureaucrates à protéger l'information, parce que c'est plus commode ou qu'il est vaguement présumé

qu'il y a sans doute plus de risques à divulguer l'information qu'à la tenir secrète. Cette tendance bureaucratique donne généralement lieu à une surclassification et à l'inflation inutile des informations classifiées. Elle alourdit également les coûts budgétaires du secret et, souvent, elle contribue à faire émerger un sentiment de suffisance bureaucratique et une réticence à révéler la façon dont l'institution gouvernementale concernée fait son travail.

3. **Secret politique :** tendance à recourir à la classification pour obtenir un avantage politique. Cette forme de secret est la plus contestable, dans la mesure où elle exploite la légitimité reconnue des intérêts réels de la sécurité nationale pour servir des intérêts personnels, éviter la controverse politique ou se soustraire à l'obligation de rendre des comptes aux citoyens. Dans des cas extrêmes, le secret politique est utilisé pour dissimuler des violations du droit ou des droits de la personne, des faits de corruption ou une mauvaise gestion, et menace l'intégrité du processus politique.

LE RÔLE GÉNÉRALEMENT MINEUR JOUÉ PAR L'APPAREIL JUDICIAIRE DANS LE CONTRÔLE DES SYSTÈMES DE CLASSIFICATION

Comme indiqué ci-dessus, les juridictions ont de tout temps fait montre d'une grande retenue, et elles le font toujours, lorsqu'elles ont affaire aux autorités classificatrices et au « privilège de l'exécutif à l'égard des secrets d'État ». Cette déférence de l'appareil judiciaire a contribué à forger l'idée selon laquelle la sécurité nationale est si sensible que les informations la concernant échappent même aux juridictions (Setty, 2012). On en trouve une bonne illustration dans l'affaire *États-Unis c. Reynolds*, qui a marqué l'histoire des États-Unis pendant la Guerre froide[2].

Cette propension de l'appareil judiciaire à l'égard de la puissance publique s'est exacerbée depuis les attentats terroristes qui ont frappé les États-Unis le 11 septembre 2001. Dans le prétoire, l'argument gouvernemental de la protection de la sécurité nationale l'a toujours emporté sur des principes tels que l'obligation de rendre compte, la transparence et le gouvernement ouvert. L'abondante jurisprudence développée aux États-Unis, au Royaume-Uni, en France et dans d'autres démocraties, sans même parler des pays où la démocratie est plus fragile, traduit l'adhésion tacite à une vision étroite du rôle joué par l'appareil judiciaire dans le contrôle des décisions de l'exécutif en matière de sécurité. Malheureusement, cela se fait peut-être au détriment de la protection des droits fondamentaux des personnes, de l'État de droit et du respect des intérêts réels en matière de sécurité.

Le « *state secrets executive privilege* » (privilège de l'exécutif à l'égard des secrets d'État) aux États-Unis, le « *public interest immunity certificate* » (privilège de non-divulgation au nom de l'intérêt public) au Royaume-Uni ou encore le « *secret-défense* » en France sont très fréquemment invoqués par les autorités classificatrices relevant de l'exécutif pour se prémunir d'un contrôle judiciaire ou le rendre moins efficace. Les exceptions au principe d'ouverture, justifiées par des expressions telles que celles utilisées ci-dessus, sont régulièrement admises devant les juridictions nationales, même si – parfois – il est vaguement précisé que cette prérogative ne saurait s'étendre au-delà des cas touchant aux intérêts réels de la sécurité nationale. Cette position assez courante dans les instances judiciaires révèle de façon générale « une indifférence judiciaire à la notion de contre-pouvoirs, une abdication de la responsabilité judiciaire et un mépris de la nécessité structurelle de préserver les voies de recours des demandeurs contre la toute-puissance du gouvernement » (Setty, 2012, page 1 573).

Fuchs (2006, page 168), dans une remarquable étude sur le rôle des juridictions, a constaté que

2 https://supreme.justia.com/cases/federal/us/345/1/case.html

« compte tenu des importantes valeurs portées par le droit d'accès à l'information gouvernementale, celui-ci ne devrait être sacrifié que lorsque le secret répond à un besoin légitime [...] Seuls, les parlements et les citoyens ne sont pas en mesure de contester l'usage excessif du secret. Le contrôle indépendant participe à la responsabilité incombant à l'appareil judiciaire de s'assurer que l'action gouvernementale est dûment autorisée ». Les juridictions sont seules à jouir de l'indépendance nécessaire pour remettre en cause l'usage excessif du secret, mais il semblerait, selon les observations de Fuchs, qu'elles refusent de tenir ce rôle.

Dans la quasi-totalité des pays européens étudiés par Jacobsen (2013), les juridictions ont l'autorité nécessaire pour examiner les informations classifiées que le gouvernement cherche à tenir secrètes pour des motifs de sécurité nationale. Il faut toutefois noter que, dans certains pays, seul un nombre limité d'instances ou de magistrats détenteurs d'une habilitation particulière sont autorisés à consulter les informations classifiées. En Allemagne, le tribunal administratif fédéral est le seul habilité à accéder aux informations classifiées. En Espagne, bien que la loi sur les secrets officiels ne prévoie pas, comme elle le fait pour le congrès ou le sénat, de dispositions particulières concernant l'accès des magistrats aux informations classifiées, la cour suprême espagnole a décidé qu'elle seule pouvait examiner le matériel classifié du gouvernement. Le seul pays où les juridictions sont totalement privées d'accès direct aux informations classifiées est la France (Sartre et Ferlet, 2010). Il semble impossible pour un magistrat français d'examiner directement des informations classifiées. Pour limiter les effets de cette interdiction, il a été institué par voie de loi en 1998 la Commission du secret de la défense nationale (CSDN), commission indépendante autorisée à accéder à des informations classifiées à la demande d'un juge, afin d'évaluer s'il est ou non raisonnable de les déclassifier[3]. Comme c'est le cas aux États-Unis, dans la majorité des pays européens, l'autorité judiciaire s'en remet généralement à l'avis rendu par les pouvoirs publics sur le préjudice que la divulgation des informations concernées causerait aux intérêts de la sécurité nationale (Jacobsen 2013)

LES CRITÈRES ET LES NIVEAUX DE CLASSIFICATION

Les niveaux de classification ont été normalisés, si bien que le même système s'applique dans de nombreux pays de l'OCDE. Parmi eux, la Nouvelle-Zélande nous offre un bon exemple du traitement réservé aux secrets d'État. Dans ce pays, l'information officielle est protégée en fonction de différents critères établis sur la base d'une définition stricte du besoin de protection : l'information doit être protégée dans les limites prescrites par l'intérêt public et le respect de la vie privée. L'autorité classificatrice s'efforce de déterminer le niveau de classification en fonction du préjudice qui résulterait de la compromission de l'information et précise les mesures de protection qui s'appliquent[4]. Selon les orientations publiées par la Nouvelle-Zélande, la classification n'autorise pas en soi la rétention d'informations officielles ; cette question doit être tranchée au fond à l'aide des critères fixés par la loi[5]. Le système de classification de l'Australie est intéressant, en ce qu'il définit des orientations claires sur la classification et la déclassification des informations secrètes[6].

En Nouvelle-Zélande, comme le prévoit la pratique internationale courante, les niveaux de classification dépendent de l'intérêt public à protéger :

3 http://www.defense.gouv.fr/sga/le-sga-en-action/droit-et-defense/secret-defense/secret-defense.
4 Loi de 1983 sur les informations officielles, Nouvelle-Zélande.
5 Lignes directrices pour la protection des informations officielles, Nouvelle-Zélande. Voir https://protectivesecurity.govt.nz/home/information-security-management-protocol/new-zealand-government-security-classification-system/.
6 Australie (2014) : Lignes directrices sur la gestion de la sécurité des informations. Système de classification du Gouvernement australien. Accessible à l'adresse : https://www.protectivesecurity.gov.au/informationsecurity/Documents/AustralianGovernmentclassificationsystem.pdf.

- Sécurité nationale : La divulgation de l'information mettrait en péril la sécurité, la défense ou les relations internationales du pays ou de gouvernements amis.

- Politique du gouvernement et/ou respect de la vie privée : La divulgation de l'information mettrait en danger la fonction du gouvernement ou pourrait causer un préjudice à une personne privée.

1. **Top Secret** : information dont la divulgation est de nature à nuire de manière exceptionnellement grave aux intérêts du pays. Elle pourrait :

    - menacer directement la stabilité interne de la Nouvelle-Zélande ou de pays amis ;
    - causer directement la perte d'un grand nombre de vies humaines ;
    - causer un préjudice exceptionnellement grave à la sécurité des forces néo-zélandaises ou de forces alliées ;
    - causer un préjudice exceptionnel à l'efficacité opérationnelle des forces néo-zélandaises ou de forces amies ;
    - causer un préjudice exceptionnel à l'efficacité continue d'opérations de sécurité ou de renseignement d'une extrême importance ;
    - causer un préjudice exceptionnel aux relations avec d'autres gouvernements ;
    - causer un préjudice grave à long terme à d'importantes infrastructures nationales.

2. **Secret** : information dont la divulgation est de nature à nuire sérieusement aux intérêts du pays. Elle pourrait :

    - susciter des tensions internationales ;
    - nuire sérieusement aux relations que la Nouvelle-Zélande entretient avec des gouvernements amis ;
    - nuire sérieusement à la sécurité des forces néo-zélandaises ou de forces amies ;
    - nuire sérieusement à l'efficacité opérationnelle des forces néo-zélandaises ou de forces amies ;
    - nuire sérieusement à l'efficacité d'importantes opérations de sécurité ou de renseignement ;
    - nuire sérieusement à la stabilité interne de la Nouvelle-Zélande ou de pays amis ;
    - provoquer l'arrêt ou de fortes perturbations d'importantes infrastructures nationales.

3. **Confidentiel** : information dont la divulgation est de nature à nuire considérablement aux intérêts du pays. Elle pourrait :

    - nuire sensiblement aux relations diplomatiques – donner lieu à une réclamation officielle ou à des sanctions ;
    - nuire à l'efficacité opérationnelle des forces néo-zélandaises ou de forces amies ;
    - nuire à la sécurité des forces néo-zélandaises ou de forces amies ;
    - nuire à l'efficacité d'importantes opérations de sécurité ou de renseignement ;
    - nuire à la stabilité interne de la Nouvelle-Zélande ou de pays amis ;
    - déstabiliser d'importantes infrastructures nationales.

4. **Diffusion restreinte** : information dont la divulgation est de nature à porter atteinte aux intérêts du pays. Elle pourrait :

    - porter atteinte aux relations diplomatiques ;
    - compromettre l'efficacité opérationnelle des forces néo-zélandaises ou de forces amies ;
    - compromettre la sécurité des forces néo-zélandaises ou de forces amies ;
    - porter atteinte à la stabilité interne de la Nouvelle-Zélande ou de pays amis ;
    - porter atteinte à la santé économique de la Nouvelle-Zélande ou de pays amis.

La politique du gouvernement et la vie privée des personnes sont protégées à différents niveaux, en application des critères ci-dessous :

1. **Sensible et diffusion restreinte** : information dont la divulgation pourrait nuire aux intérêts du gouvernement ou mettre en danger les citoyens :

    - mettre en danger la sécurité de toute personne ;
    - nuire sérieusement à l'économie de la Nouvelle-Zélande ;
    - interférer avec les négociations du gouvernement.

2. **Confidentiel** : information dont la divulgation pourrait entraver l'ordre public, interférer avec les affaires du gouvernement, porter atteinte à la vie privée des citoyens :

    - entraver le maintien de l'ordre ;
    - porter atteinte à la vie privée d'une personne physique ;
    - compromettre les renseignements commerciaux revenant aux citoyens ;
    - compromettre les obligations de confidentialité ;
    - compromettre les mesures de protection de la santé ou de la sécurité du public ;
    - compromettre les intérêts économiques de la Nouvelle-Zélande ;
    - compromettre les mesures de prévention ou d'atténuation des pertes matérielles du public ;
    - violer des conventions constitutionnelles ;
    - interférer avec la conduite efficace des affaires publiques ;
    - violer le secret professionnel tel que reconnu par la loi ;
    - interférer avec les activités commerciales du gouvernement ;
    - servir à divulguer ou utiliser des informations pour en tirer des gains ou avantages indus.

Comme indiqué plus haut, des mentions et critères de classification similaires se retrouvent dans de nombreux pays de l'OCDE. Même en Turquie, où les règles de classification ne sont pas accessibles au public, certains niveaux de classification sont réputés en vigueur (Jacobsen 2013). La Suède est le seul pays, parmi les répondants à l'enquête analysée par Jacobsen (2013), où la loi ne précise pas les niveaux de classification, car la classification y revêt une fonction purement administrative.

Les autres aspects liés à la classification de l'information (procédures de classification, mentions obligatoires, autorité classificatrice, obligation de préciser les motifs justifiant la classification, obligation de rendre des comptes en cas de classification incorrecte, instances de supervision, etc.) varient considérablement d'un pays européen à l'autre (voir Jacobsen 2013 et Transparency International UK, 2014).

LES CRITÈRES DE DÉCLASSIFICATION

Dans les pays européens, la déclassification répond à trois grands critères : la durée de validité, l'événement déclencheur ou la période de révision obligatoire. Il s'agit avant tout d'éviter la classification de l'information à perpétuité. Toutefois, il n'est pas rare de trouver des pays où aucun critère de déclassification n'est défini dans la législation ou les pratiques administratives. La durée médiane de classification, selon les calculs effectués par Jacobsen (2013), est de 30 ans dans les pays européens, la fourchette s'étendant de 10 ans aux Pays-Bas à 100 ans en Roumanie, ou encore à une durée indéfinie en Espagne et en Turquie. Cette période indéfinie fait toutefois figure d'exception en Europe.

Le plus souvent, la période de révision obligatoire de la classification est fixée à cinq ans. En Suède, aucune révision obligatoire n'est préétablie, mais, quel que soit le type d'information protégée, la classification doit faire l'objet d'un réexamen dès lors qu'une demande de divulgation est déposée.

Les modalités de déclassification automatique (à la survenue d'un événement déterminé) varient selon les pays, mais, dans la majorité d'entre eux, il s'agit surtout d'une décision discrétionnaire du gouvernement de déclassifier diverses classes d'information. Une telle décision peut également intervenir suite à l'introduction par un citoyen ou une organisation de la société civile d'une procédure au titre de la loi sur l'accès à l'information.

LES CRITÈRES DE CONTRÔLE DE L'UTILISATION DU SECRET : LE PRÉJUDICE ET L'INTÉRÊT PUBLIC

D'après *Right2INFO.org*, organisation non gouvernementale qui promeut la mise en place de lois et de pratiques de qualité, les critères du préjudice et de l'intérêt public trouvent leur origine dans les obligations de proportionnalité et de nécessité qui s'appliquent aux restrictions du droit d'accès à l'information[7]. Le Programme SIGMA de l'OCDE (2010) propose une approche conceptuelle étendue et exhaustive des notions sous-tendant ces critères d'évaluation, laquelle découle de la distinction faite entre les restrictions absolues et relatives touchant l'accès à l'information. Dans la classe des restrictions absolues, on trouve généralement celles en rapport avec la défense et la sécurité nationale.

LE CRITÈRE DU PRÉJUDICE

Selon le critère du préjudice, l'autorité publique doit démontrer que la divulgation de certaines informations pourrait porter préjudice à l'intérêt protégé, ce qui explique que les informations concernées ne devraient pas être divulguées. Pour satisfaire à ce critère, l'État doit valider qu'il existe un risque de préjudice important et manifeste contre un intérêt légitime particulier. Il doit pouvoir être démontré que la limitation d'accès se justifie à l'égard d'un intérêt légitime déterminé, auquel la divulgation de l'information causerait un préjudice substantiel. Le préjudice en cause doit être suffisamment spécifique, concret, imminent et direct ; il ne peut être spéculatif ou éloigné.

LE CRITÈRE DE L'INTÉRÊT PUBLIC

Le critère de l'intérêt public renvoie à la notion de proportionnalité. Il suppose de mettre en balance, d'une part, le préjudice qui serait associé à la divulgation de l'information et, d'autre part, la mesure dans laquelle une telle divulgation servirait l'intérêt public. Les conditions dans lesquelles un intérêt public explicite et détaillé est susceptible de prévaloir sur l'invocation du secret ou de la confidentialité doivent être précisées dans la législation nationale. Selon de nombreux modèles de classification nationaux, y compris les modèles interaméricain et africain, l'intérêt public devient impérieux et l'emporte sur les autres intérêts en jeu lorsque les informations concernées ont trait à des violations des droits de la personne ou à des crimes contre l'humanité. Pour satisfaire au critère de l'intérêt public, l'autorité publique, ou l'organe de supervision, met en balance, d'une part, le préjudice que la divulgation de l'information causerait à un intérêt protégé donné et, d'autre part, la mesure dans laquelle une telle divulgation sert l'intérêt public.

La définition de l'intérêt public varie d'un pays à l'autre et exige souvent une évaluation au cas par cas. En général, les intérêts publics pour lesquels une divulgation des informations est préférable concernent les questions soumises au débat public, la participation publique au débat politique, l'obligation de rendre compte de l'allocation des fonds publics et des dépenses publiques, ainsi que la sécurité publique. L'on considère généralement que les questions relatives à la sécurité publique et à l'environnement, les menaces sérieuses pour la santé et les informations touchant à de graves violations des droits de la personne justifient que la priorité impérieuse soit donnée à l'intérêt public associé à la divulgation des informations.

7 http://www.right2info.org/exceptions-to-access/harm-and-public-interest-test.

Certains pays ont publié des orientations concernant les procédures administratives que doivent suivre les fonctionnaires. Par exemple, en Nouvelle-Galles du Sud (Australie), les fonctionnaires doivent s'en remettre au critère de l'intérêt public lorsqu'ils décident si certaines informations seront ou non diffusées. Ainsi, ils doivent mettre en balance les facteurs plaidant pour une divulgation de l'information et les facteurs touchant aux intérêts publics allant à l'encontre d'une telle divulgation[8]. Selon les orientations en vigueur, le critère de l'intérêt public est évalué en trois étapes :

1. Recensement des motifs d'intérêt public justifiant la divulgation.

2. Recensement des motifs d'intérêt public justifiant la non-divulgation.

3. Détermination du poids relatif des motifs d'intérêt public évoqués en faveur et à l'encontre de la divulgation et détermination de leur point d'équilibre.

Si la législation australienne se positionne clairement en faveur de la divulgation de l'information, les lois provinciales sur l'accès à l'information précisent un certain nombre de situations où la présomption bénéficie à la rétention de l'information et à la protection du secret. Le cas le plus notoire concerne les informations soumises à une loi contenant une clause dérogatoire sur le secret. Vingt-six lois sont spécifiquement citées. L'Australie n'échappe pas à la tendance générale observée dans de nombreux pays de l'OCDE, où, dans la pratique, les lois sur la liberté d'information perdent toute pertinence face aux législations traditionnelles sur les secrets d'État. Ces derniers sont systématiquement écartés du champ d'application des lois sur la liberté d'accès à l'information. En outre, de manière générale, dans la plupart des pays, peu d'efforts ont été déployés pour harmoniser la législation sur la sécurité des États et les nouvelles lois relatives à la liberté d'accès à l'information publique.

Étant donné que la question du secret lié à la sécurité nationale est à peine effleurée dans nombre de lois sur la liberté d'information, la législation et les voies de recours judiciaires n'ont à ce jour guère été efficaces pour réduire la tendance universelle à l'usage croissant de la confidentialité et du secret dans les travaux des agences de sécurité et de renseignement. Au fond, ces institutions, qui traitent l'information confidentielle de façon conservatrice et souvent opaque, échappent encore au champ d'application des lois sur la liberté d'information, en dépit d'un large mouvement international prônant plus de transparence publique et de la revendication d'un « droit de savoir » par la société civile.

Cela montre bien que, tant en théorie qu'en pratique, il est difficile de promulguer une législation générale où le juste équilibre est trouvé entre secret et ouverture. L'une des raisons en est que les instances ou agences publiques les plus susceptibles de classifier des informations poursuivent généralement des objectifs et des motivations bien distinctes dans leur travail et dans leurs pratiques. Cela favorise l'émergence d'une multitude de cultures administratives de la sécurité. Par exemple, les instances militaires tendent à se concentrer avant tout sur la sécurité de la technologie des armements et les plans opérationnels, là où les agences de renseignement privilégient la protection des sources et des modes opératoires, les diplomates s'intéressent aux conséquences internationales de la classification et de la déclassification des informations diplomatiques et la police a à cœur de protéger ses informateurs et plans opérationnels. Ainsi, chaque agence ou institution élabore ses propres orientations, procédures et protocoles, qui restent généralement en vigueur pendant des années, échappant aux regards et à toute forme d'examen sérieux. De surcroît, on

8 http://www.ipc.nsw.gov.au/fact-sheet-what-public-interest-test.

peut comprendre que, dans des agences telles que celles mentionnées ci-dessus, les agents préfèrent miser sur la prudence pour éviter des problèmes inutiles, ce qui se manifeste souvent par une surclassification (Aftergood, 2009).

Par conséquent, ainsi que le laissent entendre des observateurs et praticiens éclairés, même si la classification incombe à l'agence compétente, le pouvoir de déclassifier ne devrait pas lui revenir. C'est la meilleure façon de contrer les motivations intéressées d'une agence et de la purger de ses classifications excédentaires (Aftergood, 2009, page 412). Les États-Unis s'y sont essayés avec succès, notamment par le biais de deux dispositifs : le *Interagency Security Classification Appeal Panel* (ISCAP)[9] et les *Fundamental Classification Policy Reviews* (FCPR)[10]. La France et sa Commission de la sécurité de la défense nationale en sont un autre exemple (voir ci-dessus). L'expérience américaine, telle que décrite par Aftergood (2009), montre en essence que « si une agence n'est pas en mesure d'expliquer avec succès les motifs de sécurité nationale justifiant la classification obligatoire d'un matériel donné et d'en convaincre un haut responsable ou un groupe d'experts d'une autre agence, il y a lieu de douter de la nécessité de tenir le matériel secret ».

CONCLUSIONS

1. La législation régissant la confidentialité de l'information dans les domaines de la sécurité et de la défense répond à une nécessité et doit être aussi précise que possible. Elle devrait définir les critères permettant de classifier et de déclassifier l'information, étant toutefois noté que toute législation revêt par nature un caractère général, qui transparaîtra de fait dans les critères établis. La législation sur la confidentialité, antérieure dans de nombreux pays à la législation sur le libre accès à l'information, devrait être harmonisée avec cette dernière, afin d'éviter d'introduire des contradictions dans l'ordre juridique national.

2. En parallèle de ce cadre juridique solide, une gestion délibérée et compétente s'impose au sein de chaque agence pour que les critères de classification définis par la loi soient appliqués de manière judicieuse ou raisonnée, dans l'optique de promouvoir dans toute la mesure possible les valeurs démocratiques et le principe de la transparence publique. La compréhension éclairée de la nécessité de mettre en balance différentes considérations devrait faire partie intégrante de la culture organisationnelle. Les responsables des agences compétentes devraient considérer que c'est à eux de trouver le juste équilibre entre la confidentialité légitime et la transparence légitime.

3. Réduire l'inflation injustifiée des documents classifiés et mettre en balance le droit de savoir du public et les impératifs de la sécurité nationale – auxquels s'ajoutent les autres raisons légitimes du recours au secret – sont des entreprises complexes. Il n'est probablement pas envisageable dans un avenir immédiat de convertir la culture du secret en culture de la transparence dans le secteur de la défense de la plupart des pays de l'UE et de l'OCDE[11].

4. La loyauté, le respect des procédures établies et la discrétion sont attendus des salariés et autres personnes travaillant dans le secteur de la sécurité et de la défense. Ces qualités sont en effet indispensables, mais il convient aussi d'encourager un certain degré d'innovation et l'apport d'idées nouvelles, même s'il y a peu de place pour le changement. Il est néanmoins nécessaire de porter un regard critique sur la façon de parvenir à un équilibre optimal entre le secret légitime, d'un côté, et l'accès légitime à l'information, de l'autre.

9 https://www.archives.gov/declassification/iscap.

10 https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/ODNI%20FY2017%20FCGR.pdf. Voir aussi l'examen pionnier mené en 1994 au sein du Département de l'énergie : https://www.osti.gov/opennet/forms.jsp?formurl=od/fcprsum.html.

11 La Roumanie y est toutefois parvenue (Matei, 2007).

5. Il convient en particulier de former les personnes chargées de faire respecter les lois sur le secret ou les politiques sur la confidentialité afin qu'elles puissent faire peser dans la balance l'impératif démocratique d'ouverture et de transparence au sein du gouvernement, tout en discernant clairement, à la lumière de la législation en vigueur, ce qui doit rester caché du public. Renoncer à l'usage sans limites du secret ne revient pas nécessairement à embrasser une ouverture sans limites. La qualité et la compétence du personnel du secteur de la sécurité et de la défense sont de la plus haute importance, car elles ont des incidences directes sur la société démocratique et les relations entre les agences de sécurité et la société civile.

6. Une institution indépendante, par exemple une commission interagences de déclassification, ne relevant pas du domaine de compétence exclusif des plus importantes autorités classificatrices, à savoir l'appareil militaire, le renseignement et la police, devrait avoir compétence pour examiner et déclassifier périodiquement des informations tenues secrètes par les différentes agences. En général, les juridictions se sont montrées trop révérencieuses vis-à-vis du privilège que détient l'exécutif à l'égard des secrets d'État, et il y a peu de raisons de penser que les choses vont changer.

7. Une bonne pratique semble se dégager à cet égard : il s'agit de réduire le pouvoir discrétionnaire dont l'usage étendu caractérise à ce jour les pratiques de classification traditionnelles. La décision de classifier ou de déclassifier une information devrait revenir non pas à un individu, mais à une commission ou à un comité indépendant, capable d'émettre un jugement impartial sur la nécessité de classifier ou de déclassifier une information donnée, en tout ou partie. Cette unité spécialisée devrait suivre les critères établis par la loi pour évaluer le critère du préjudice et celui de l'intérêt public. Un tel comité ou commission indépendant devrait avoir une composition limitée, restreinte par exemple à cinq à sept membres, et pourrait comprendre des experts en sécurité relevant du pouvoir exécutif, du parlement, des députés, du médiateur public et du pouvoir judiciaire.

RÉFÉRENCES

Aftergood, Steven (2009), *Reducing Government Secrecy: Finding What Works*, dans Yale Law & Policy Review, Vol. 27, N° 2 (Spring, 2009), pp. 399-416. Disponible à l'adresse : https://www.jstor.org/stable/40239716?seq=1#page_scan_tab_contents

Fenster, Mark (2010), *Seeing the State: Transparency as Metaphor*, dans Administrative Law Review, pages 617-672. Disponible à l'adresse : http://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1571&context=facultypub

Fuchs, Meredith (2006), *Judging Secrets: The Role Courts Should Play in Preventing Unnecessary Secrecy*, dans Administrative Law Review, Volume 58, numéro 1, Winter 2006, pages 131-176.

Jacobsen, Amanda L. (2013), *National Security and the Right to Information in Europe*. Disponible à l'adresse : http://www.right2info.org/resources/publications/national-security-page/national-security-expert-papers/jacobsen_nat-sec-and-rti-in-europe

Matei, Florina Cristiana (2007), *Reconciling Intelligence Effectiveness and Transparency: The Case of Romania*, dans Strategic Insights, Volume VI, n° 3 (mai 2007). Disponible à l'adresse : https://calhoun.nps.edu/bitstream/handle/10945/11297/mateiMay07.pdf?sequence=1

OCDE (2010), *Le droit à des administrations publiques ouvertes en Europe : Normes juridiques émergentes*, document SIGMA n° 46, Éditions OCDE, Paris. Disponible à l'adresse : http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=GOV/SIGMA(2010)2/REV1&docLanguage=Fr

Riese, Dorothée (2014), *Secrecy and Transparency*, document présenté à la conférence du Consortium européen de recherches en sciences politiques tenue à Glasgow, 3-6 septembre 2014. Disponible à l'adresse : https://ecpr.eu/Filestore/PaperProposal/2cedead9-5191-42de-ae36-7d320a28a304.pdf

Sartre, Patrice et Ferlet, Philippe (2010), *Le secret de défense en France*, dans Revue Études 2010/2, Tome 412, février, pages 165-175. Disponible à l'adresse : https://www.cairn.info/revue-etudes-2010-2-page-165.htm

Sauvé, Jean-Marc (2011), *Culture du secret contre transparence sans limite : quel équilibre pour garantir l'intérêt général ? Transparence, valeurs de l'action publique et intérêt général*, discours à l'Assemblée nationale prononcé le mardi 5 juillet 2011 au colloque organisé par Transparence Internationale France. Disponible à l'adresse : http://www.conseil-etat.fr/content/download/2597/7819/version/1/file/discours-transparence-international.pdf

Setty, Sudha (2012), *The Rise of National Security Secrets*, dans Connecticut Law Review, volume 44, numéro 5, juillet 2012, pages 1563-1582.

Transparency International UK (2014), *Classified Information: A Review of 15 Countries*. Disponible à l'adresse : http://ti-defence.org/wp-content/uploads/2016/03/140911-Classified-Information.pdf

Série des guides de bonne gouvernance


GUIDES TO GOOD GOVERN-ANCE
N° 04
Accès à l'information et limites de la transparence vis-à-vis du public
Centre for Integrity in the Defence Sector
NATO OTAN


GUIDES TO GOOD GOVERN-ANCE
N° 05
Gestion des risques de corruption et de fraude immobilière dans le secteur de la défense
Centre for Integrity in the Defence Sector
NATO OTAN

Les **Guides de bonne gouvernance** sont une série de petits livrets dédié chacun à un thème spécifique important pour la bonne gouvernance dans le secteur de la défense. Ils s'adressent aux personnes qui souhaitent en apprendre davantage sur un ou plusieurs sujets présentant un intérêt direct pour la bonne gouvernance dans le secteur de la défense, ou dans le secteur public en général. Ils peuvent également être utilisés à des fins pédagogiques.

Publié par : Centre pour l'intégrité dans le secteur de la défense
Infographie : www.melkeveien.no
Traduction : Service Traduction du Secrétariat international de l'OTAN

CENTRE FOR INTEGRITY
IN THE DEFENCE SECTOR

www.cids.no

1069-16 NATO GRAPHICS & PRINTING-FR