Enjeux et limites de l'ouverture des données en matière de sécurité et de défense

Bertrand Warusfel

▶ **To cite this version:**

Bertrand Warusfel. Enjeux et limites de l'ouverture des données en matière de sécurité et de défense. Revue française d'administration publique, 2018, 2018 (n°3), pp. 551-564. hal-02020021

HAL Id: hal-02020021
https://hal.science/hal-02020021v1

Submitted on 14 May 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

CAIRN.INFO
CHERCHER, REPÉRER, AVANCER

ENJEUX ET LIMITES DE L'OUVERTURE DES DONNÉES EN MATIÈRE DE SÉCURITÉ ET DE DÉFENSE

Bertrand Warusfel

Ecole nationale d'administration | « Revue française d'administration publique »

2018/3 N° 167 | pages 551 à 564

ISSN 0152-7401

Article disponible en ligne à l'adresse :

https://www.cairn.info/revue-francaise-d-administration-publique-2018-3-page-551.htm

Distribution électronique Cairn.info pour Ecole nationale d'administration.
© Ecole nationale d'administration. Tous droits réservés pour tous pays.

La reproduction ou représentation de cet article, notamment par photocopie, n'est autorisée que dans les limites des conditions générales d'utilisation du site ou, le cas échéant, des conditions générales de la licence souscrite par votre établissement. Toute autre reproduction ou représentation, en tout ou partie, sous quelque forme et de quelque manière que ce soit, est interdite sauf accord préalable et écrit de l'éditeur, en dehors des cas prévus par la législation en vigueur en France. Il est précisé que son stockage dans une base de données est également interdit.

Document téléchargé depuis www.cairn.info - Université Paris 8 - - 193.54.174.3 - 14/02/2019 22h55. © Ecole nationale d'administration

ENJEUX ET LIMITES DE L'OUVERTURE DES DONNÉES EN MATIÈRE DE SÉCURITÉ ET DE DÉFENSE

Bertrand WARUSFEL

Professeur à l'Université de Paris VIII Vincennes-Saint-Denis

Résumé

La communication des données publiques est notamment limitée par des motifs touchant aux différentes formes de sécurité, et particulièrement à la sécurité nationale et à la sécurité des personnes et des biens. Dans certains domaines comme en matière environnementale et nucléaire, l'opposition peut être assez frontale entre le secret de la défense nationale et le principe de transparence. Il est néanmoins possible d'envisager qu'un équilibre puisse être trouvé pour que les missions régaliennes de l'État ne soient pas exclues du périmètre de l'ouverture des données et de ses bénéfices mutuels pour la puissance publique et les citoyens.

Mots-clefs

Données publiques, sécurité nationale, secret de défense, nucléaire, sécurité publique

Abstract

— Challenges and limits of open data in security and defense matters — The open data process is restricted for security concerns, including the national security and public safety concerns. In cares such as environmental and nuclear issues, there is a head-on opposition between military secrecy and transparency. A balance can nevertheless be found, enabling state security mission's to be included in the open data perimeter. This inclusion may open the door to mutual benefits for both the state and the citizen.

Keywords

Public data, national security, military secrecy, nuclear, public security

Document téléchargé depuis www.cairn.info - Université Paris 8 - - 193.54.174.3 - 14/02/2019 22h55. © Ecole nationale d'administration

Présentant la nouvelle accélération de la politique d'ouverture des données publiques après la loi Lemaire, le gouvernement précisait en 2017 que « cela ne concerne ni les informations personnelles, ni celles touchant à la sécurité nationale, ni celles couvertes par les différents secrets légaux » [1].

En se référant explicitement à la notion de « sécurité nationale » – pourtant formellement absente de la loi du 17 juillet 1978 et des dispositions qui en sont issues –, l'autorité gouvernementale a voulu englober plusieurs des exceptions légales à la communicabilité et à la réutilisation des données publiques.

Il est vrai que le code des relations entre le public et l'administration (CRPA) connaît déjà une référence à cette notion, puisque son article L. 231-4 dispose que vaut rejet implicite le silence gardé durant deux mois dans les cas qui ne seraient pas compatibles avec « la protection de la sécurité nationale ».

Pour autant la sécurité nationale n'est que l'une des dimensions sécuritaires justifiant le refus de communication des données publiques. Dans son périmètre l'un des motifs les plus difficiles à apprécier concerne la protection du secret de la défense nationale, lequel peut notamment entrer en confrontation directe avec des impératifs renforcés de transparence, comme en matière environnementale et nucléaire. Les différents impératifs sécuritaires constituent donc une source potentielle de limitation forte du mouvement de l'*open data*, même s'il est possible d'envisager qu'un équilibre puisse être trouvé pour que les missions régaliennes de l'État ne soient pas exclues du périmètre de l'ouverture des données et des bénéfices mutuels que l'autorité publique et les citoyens devraient y trouver.

LES EXCEPTIONS DE SÉCURITÉ, LIMITES À L'OUVERTURE DES DONNÉES

C'est l'ancien article 6 de la loi du 17 juillet 1978, aujourd'hui codifié à l'article L. 311-5 CRPA, qui exclut de la communicabilité des données publiques celles qui sont couvertes par le « secret des délibérations du gouvernement et des autorités responsables relevant du pouvoir exécutif » (2° a) ou par le « secret de la défense nationale » (2° b), celles qui concernent « la conduite de la politique extérieure de la France » (2° c) ou encore qui sont relatives « à la sûreté de l'État, à la sécurité publique ou à la sécurité des personnes » (2° d).

Une partie importante de ces motifs d'exclusion à la communicabilité des données se rattache à la mission de sécurité nationale qui, selon l'article L. 1111-1 du code de la défense, vise à identifier et répondre à « l'ensemble des menaces et des risques susceptibles d'affecter la vie de la Nation, notamment en ce qui concerne la protection de la population, l'intégrité du territoire et la permanence des institutions de la République », y compris dans sa dimension militaire puisque la politique de défense (désormais uniquement en charge de protéger la Nation des « agressions armées »), est partie intégrante de la sécurité nationale (Warusfel, 2011).

Certes, les délibérations gouvernementales ou la politique extérieure peuvent avoir d'autres objets et les questions de sécurité des personnes et des biens sont bien hors du champ de la sécurité nationale. Le *Livre blanc* sur la défense et la sécurité nationale de 2008 précise ainsi que la politique de sécurité intérieure ne concourt à la sécurité nationale que

1. Voir www.gouvernement.fr/action/l-ouverture-des-donnees-publiques, 15 mai 2017.

Document téléchargé depuis www.cairn.info - Université Paris 8 - - 193.54.174.3 - 14/02/2019 22h55. © Ecole nationale d'administration

« pour tout ce qui ne relève pas de la sécurité quotidienne et individuelle des personnes et des biens, et la politique de sécurité civile » (Livre blanc, 2008, tome 1, p. 62-63). Ces dernières ont plutôt à voir avec deux autres exceptions portant respectivement sur le « déroulement des procédures engagées devant les juridictions ou d'opérations préliminaires à de telles procédures » (2° f) ou sur « la recherche et à la prévention, par les services compétents, d'infractions de toute nature » (2° g).

Pour mettre un peu d'ordre dans ces exceptions dont la formulation date pour l'essentiel de quarante ans, on peut considérer que la communication des données publiques et leur réutilisation connaissent donc deux catégories de limitations justifiées par des motifs sécuritaires : d'une part celles imposées par les impératifs de sécurité nationale ; de l'autre des limitations liées aux missions de sécurité publique et de répression pénale. Le droit de l'Union européenne retient d'ailleurs comme motif d'incommunicabilité d'une information la « protection de la sécurité nationale (autrement dit, la sûreté de l'État), de défense ou de sécurité publique » [2].

Sur ces bases textuellement et juridiquement assez imprécises, la pratique de la Commission d'accès aux documents administratifs (CADA) et la jurisprudence administrative ont, sans beaucoup de surprise, identifié différents types de documents administratifs jugés non communicables pour ces différentes raisons de sécurité.

C'est ainsi qu'au titre de la conduite de la politique extérieure ne sont pas communicables des documents laissant deviner la position de la France dans une négociation [3] ou pouvant avoir une incidence sur les négociations internationales en cours [4]. Inversement, la communication de pièces d'archives diplomatiques concernant les relations entre la France et la RDA ne contenant pas « de secrets relatifs à la sûreté de l'État ou à la défense nationale » donne lieu à un avis favorable en raison des évènements survenus en Allemagne (chute du mur de Berlin et réunification) qui ont eu pour effet d'« atténuer sensiblement le caractère secret des informations contenues dans ceux-ci et [justifient] qu'il puisse être dérogé au délai de protection institué par la loi » [5].

En matière de sécurité publique, la CADA ne refuse pas systématiquement la communication de documents concernant ce domaine mais uniquement ceux dont la divulgation serait de nature à lui porter atteinte, soit parce qu'elle affaiblirait directement la protection des personnes ou des biens, soit parce qu'elle gênerait l'action publique en matière de maintien de l'ordre et de sécurité publique. C'est ainsi que la localisation des caméras de vidéosurveillance d'une commune est non communicable [6] ou le plan concernant une installation classée de stockage d'hydrocarbures et qui comporte des indications sur sa sécurité [7], ou encore la base de données « Cezar » recensant les incidents sur le réseau ferroviaire [8]. Plus récemment, ce sont les notes et rapports sur le fondement desquels le préfet a refusé une autorisation d'acquisition et de détention d'arme qui ont été jugés non communicables [9], ou encore les noms des magistrats ayant suivi des formations de l'École de la magistrature portant sur les dérives sectaires [10].

2. Article 1er 2c) de la directive du 17 novembre 2003 concernant la réutilisation des informations du secteur public (texte conservé sans changement par la directive du 26 juin 2013).
3. Avis n° 20032193 du 22 mai 2003.
4. Avis n° 20072905 du 26 juillet 2007.
5. Avis n° 20053874-LV du 22 septembre 2005.
6. Avis n° 20044361 du 20 janvier 2005.
7. Conseil n° 20072710 du 26 juillet 2007.
8. TA Paris, 8 février 2007, *SA Le Point*.
9. Avis n° 20153249 du 8 octobre 2015, confirmé par CE, 21 septembre 2015, *M. Rossin*, n° 369808.
10. CE, 8 novembre 2017, *Église de scientologie Celebrity Center*, n° 375704.

Document téléchargé depuis www.cairn.info - Université Paris 8 - - 193.54.174.3 - 14/02/2019 22h55. © Ecole nationale d'administration

Parallèlement, ont été considérés comme comportant des indications sur l'organisation de l'action publique en matière de sécurité et non communicables de ce fait certains passages d'un contrat et ses annexes touchant la télésurveillance et le transport de fonds [11], une circulaire relative à l'organisation d'escortes pénitentiaires des détenus [12] ou encore des procédures internes de la Commission bancaire en vue de prévenir le blanchiment de capitaux [13].

Mais c'est en matière de secret de la défense nationale que la doctrine de la CADA et la jurisprudence administrative ont eu plus de difficultés à déterminer quelle marge d'appréciation pouvait exister s'agissant de la non-communication de documents pour ce motif prévu à l'article L. 311-5 CRPA 2° b. Il en résulte encore aujourd'hui (et malgré les différentes réformes intervenues depuis 1978 en la matière) une source permanente d'ambiguïtés sur le périmètre des documents et informations susceptibles d'être exclus de toute communication pour des motifs de sécurité nationale.

UNE APPRÉCIATION LARGE DU SECRET DE DÉFENSE COMME MOTIF DE RESTRICTION

Défini par l'article 413-9 du code pénal et protégé par ses articles 413-10 à 413-12 CP tout en étant organisé administrativement par application du code de la défense, le secret de la défense nationale est l'un des secrets les mieux protégés et qui concerne les domaines les plus sensibles de l'action publique, non seulement (comme sa dénomination pourrait encore le laisser croire) en matière militaire et stratégique mais plus largement dans tout le périmètre que recouvre désormais la sécurité nationale (Warusfel, 2013, 76-78).

On pourrait donc penser qu'en la matière l'incommunicabilité (qui va de soi s'agissant d'un secret aussi absolu) est automatique et que la CADA ou le juge administratif (saisi d'un éventuel recours contre le refus de communication) ne peut que la confirmer au vu du caractère classifié de tel ou tel document ou information. Cela ne fait autant moins de doute que, dans la tradition juridique française, aucun juge ne peut accéder à des éléments couverts par le secret de défense (Warusfel, 2000, 361-380) [14]. Par ailleurs, on peut noter qu'à la différence de certaines autres autorités administratives indépendantes – par exemple la Commission nationale de l'informatique et des libertés (CNIL), la Commission du secret de la défense nationale (CSDN) et la Commission nationale de contrôle des techniques du renseignement (CNCTR) –, les membres de la CADA ne sont pas habilités à connaître des secrets de la défense nationale.

Pour autant la pratique de la CADA est plus complexe, notamment sur deux aspects dont l'un au moins pourrait susciter quelques difficultés et notamment justifier certaines pratiques de rétention abusive d'informations par l'autorité gouvernementale.

11. CE, 3 février 1992, *Société Sécuripost et Min. P&T c/Sté Libertés-Services*.
12. Avis n° 20073882 du 11 octobre 2007.
13. Avis n° 20090087 du 15 janvier 2009.
14. La seule exception récente – significative mais limitée – à cette interdiction d'accès du juge au secret de défense résulte des dispositions de la loi relative au renseignement du 24 juillet 2015 (qui a créé les articles L. 773-3 à L. 773-8 du code de justice administrative, autorisant l'accès d'une formation spéciale du Conseil d'État aux éléments classifiés concernant la mise en œuvre d'une technique de renseignement ou au contenu d'un fichier classifié).

Document téléchargé depuis www.cairn.info - Université Paris 8 - - 193.54.174.3 - 14/02/2019 22h55. © Ecole nationale d'administration

En premier lieu, la CADA ne s'est pas contentée de s'incliner automatiquement devant l'invocation par l'administration du caractère classifié d'un document dont la communication est sollicitée auprès de la Commission. Même si la création de la Commission consultative du secret de la défense nationale (CCSDN, aujourd'hui dénommée seulement CSDN) par la loi du 17 juillet 1998 l'a conduit un temps à décliner sa compétence, estimant que seule la CSDN avait compétence en la matière [15], elle s'est vue finalement reconnaître par le Conseil d'État la compétence de pouvoir, sans accéder elle-même au secret de défense invoquée, « rendre un avis, sur le fondement du livre III du code des relations entre le public et l'administration, sur la communication de documents administratifs couverts par le secret de la défense nationale » [16].

La CADA fait d'ailleurs désormais référence à cet arrêt de 2012 pour affirmer sa compétence en la matière [17]. Elle rappelle également que la classification d'un document administratif « ne fait pas échapper ce document à la compétence de la commission pour émettre un avis sur sa communication éventuelle » [18].

Ainsi, par exemple, sollicitée en 2009 sur l'accès à des documents classifiés concernant l'accident de la Caravelle d'Air France en 1968, la CADA a estimé que « s'agissant des documents classifiés par les autorités françaises, notamment ceux qui se rapportent à des exercices effectués dans le cadre de l'OTAN, la commission estime que, eu égard à l'échéance de libre communicabilité (2018 en vertu du 3° du I de l'article L. 213-2 du code du patrimoine), à la nature de ces documents, dont elle n'a toutefois pu prendre connaissance, et au sérieux des recherches entreprises par le demandeur, qui a déjà pu accéder à nombre de documents classifiés, la commission émet un avis favorable à leur consultation, à l'exception d'éventuels documents classifiés "Très secret défense" » [19].

Elle estime également qu'il « lui appartient dans ce cadre de vérifier qu'avant que ne soit refusée la communication du document sollicité, qui ne serait possible qu'après déclassification par l'autorité compétente, celle-ci s'est assurée que le maintien de la classification est justifié » [20].

Ainsi, la CADA estime être en mesure de se prononcer « au vu, notamment, de tout élément d'information que l'administration destinataire de la demande lui communique dans des formes préservant le secret de la défense nationale, de façon à lui permettre d'émettre son avis en connaissance de cause sans porter directement ou indirectement atteinte à ce secret » [21].

En procédant ainsi, la CADA se donne la possibilité d'obliger l'administration concernée à réexaminer la pertinence du maintien de la classification, ce qui peut contribuer à lutter contre les risques récurrents de « sur-classification » résultant du maintien d'une classification au-delà de la période durant laquelle la divulgation du contenu protégé était encore susceptible de porter atteinte aux intérêts de la défense nationale (ou désormais à

15. Voir notamment CADA, avis n° 20010012 du 8 mars 2001.
16. CE, 20 février 2012, *Min. de la défense*, n° 350382, *Rec. Lebon*, p. 54.
17. Voir par exemple, son avis n° 20143973 du 11 décembre 2014.
18. Avis n° 20153938 du 19 novembre 2015.
19. Avis n° 20091147 du 30 avril 2009. Cela n'empêche pas que la communication de ces documents classifiés à laquelle elle donne un avis favorable nécessite ensuite une déclassification, éventuellement précédée par une saisine de la CSDN (dans ce sens, par exemple son avis n° 20165807 du 9 mars 2017). C'est d'ailleurs ce qu'a jugé le Conseil d'État dans son arrêt précité du 20 février 2012. Dans le dossier de la Caravelle, la justice a fini par demander en 2017 la déclassification de certains documents militaires, entraînant la saisine de la CSDN.
20. Avis n° 20153938 du 19 novembre 2015 précité.
21. Avis n° 20124117 du 10 janvier 2013.

Document téléchargé depuis www.cairn.info - Université Paris 8 - - 193.54.174.3 - 14/02/2019 22h55. © Ecole nationale d'administration

ceux de la « sécurité nationale ») [22]. Allant plus loin, elle n'hésite même pas à considérer qu'elle peut estimer « que la communication d'un document classifié ne porterait atteinte ni au secret de la défense nationale, ni à un autre intérêt protégé par l'article 6 de la loi du 17 juillet 1978 » [23]. Autrement dit, loin de se déclarer incompétente, la CADA estime désormais avoir toute liberté pour apprécier, dans la limite des informations non classifiées que l'autorité administrative doit lui fournir, la pertinence de la classification concernée.

Pour autant, cette évolution favorable de la pratique de la CADA face au secret de défense est en partie contrebalancée par le fait que la Commission maintient toujours son interprétation extensive des dispositions de la loi du 17 juillet 1978 aujourd'hui intégrées à l'article L. 311-5 CRPA qui l'amène à appliquer l'exclusion pour secret de défense dans des situations où, paradoxalement, il n'existe matériellement pas de classification.

Nous avions depuis longtemps soulevé la difficulté qui était apparue dès l'un des premiers avis rendus par la CADA sur ces questions, à savoir l'avis Lalonde (du nom d'un leader écologiste de l'époque). Dans cet avis, la CADA avait formulé un avis défavorable à la communication d'un rapport de sûreté concernant l'usine nucléaire de La Hague estimant qu'elle pourrait porter notamment atteinte au secret de la défense nationale, puisqu'un « lecteur averti de ces extraits pourrait connaître assez précisément […] la capacité nucléaire nationale, c'est-à-dire la quantité de plutonium à usage militaire fabriqué » [24].

Or, il apparaissait à la lecture de cet avis que le document concerné n'était pas formellement classifié, ce qui dès lors rendait difficile l'invocation de la protection du secret de défense dans un tel cas. Au vu de la réforme du nouveau code pénal qui a introduit en 1994 une condition formelle de classification dans l'article 413-9 CP, nous avions donc estimé qu'on devrait voir « la CADA restreindre en conséquence son invocation du secret de défense, sauf à ce qu'elle utilise d'autre notions mal définies – comme par exemple, l'exception liée à la conduite de la politique extérieure – pour continuer à considérer comme secrets des documents administratifs non classifiées qu'elle aurait précédemment couverts par le secret de défense » (Warusfel, 2000, 297).

La pratique de la CADA à ce sujet n'a pourtant pas changé et s'appuie désormais sur une regrettable confusion des motifs. Dans un avis de 2015 déjà cité, elle affirme notamment que « le secret des documents classifiés au titre du secret de la défense nationale en application de l'article 413-9 du code pénal revêt le secret d'un caractère protégé par la loi, au sens du h du 2° du I de l'article 6 de la loi du 17 juillet 1978. En outre, en vertu du b du même 2°, ne sont pas communicables les documents dont la communication porterait atteinte au secret de la défense nationale, même quand ils ne sont pas classifiés, pendant le délai de cinquante ou cent ans fixé au 3° du I de l'article L. 213-2 du code du patrimoine » [25].

Dans un autre avis récent concernant la communication d'archives du renseignement militaire durant la guerre d'Algérie, la Commission va même jusqu'à parler de « documents dont la communication porterait atteinte au secret de la défense nationale, même quand ils n'ont fait l'objet d'aucune classification à ce titre » [26].

Pour s'autoriser ainsi à refuser non seulement la communication de documents effectivement classifiés mais aussi (comme dans l'avis Lalonde de 1981) celle de documents non classifiés dont le contenu pourrait, selon elle, porter atteinte à un secret de défense,

22. Comme le SGDSN l'a annoncé récemment (dans son 2e rapport sur le secret de la défense nationale en France, paru en 2018), on devrait parler désormais du « secret de la défense et de la sécurité nationale ».
23. Voir par exemple, son avis n° 20143973 du 11 décembre 2014 précité.
24. Avis n° 2467 du 4 mars 1981.
25. Avis n° 20153938 du 19 novembre 2015.
26. Avis n° 20153438 du 24 septembre 2015.

Document téléchargé depuis www.cairn.info - Université Paris 8 - - 193.54.174.3 - 14/02/2019 22h55. © Ecole nationale d'administration

elle a en effet décalé sa motivation. Elle considère désormais que la non-communicabilité des données classifiées repose sur l'exclusion des « autres secrets protégés par loi » (article L. 311-5 CRPA 2° h) et non sur celle prévue au b) du même article qui exclut la communication pour un motif de « protection du secret de la défense nationale », motif qu'elle invoque au contraire pour justifier l'exclusion de documents non classifiés.

Ce décalage de motivation nous paraît doublement injustifié. Tout d'abord, les « autres secrets » protégés par la loi que mentionne le h) de l'article L. 311-5 2° ne peuvent pas couvrir le « secret de la défense nationale » déjà visé préalablement par son b). Le secret de défense n'est pas un « autre » secret protégé mais celui qui est invoqué expressément dès le début de cet article. Il est donc erroné de vouloir fonder le refus de communiquer un document classifié sur ce fondement alternatif. Ensuite, et surtout, l'exclusion du secret de la défense nationale ne peut s'appliquer qu'en la présence d'un véritable secret de défense répondant à toutes les caractéristiques prévues à l'article 413-9 CP, à savoir un lien matériel avec la défense nationale (ou, désormais, la sécurité nationale, dans le nouveau vocabulaire du code de la défense) mais aussi l'existence formelle d'une classification par l'autorité concernée préalablement à la demande de communication.

Ceci est d'autant moins contestable que le Conseil d'État lui-même a reconnu en 2005 que « ne peuvent être réputés présenter un caractère de secret de la défense nationale que les renseignements, procédés, objets, documents, données informatisées ou fichiers intéressant la défense nationale qui ont fait spécialement l'objet d'une classification par l'autorité compétente dans les conditions prévues par le code de la défense » [27].

L'enjeu de cette clarification des motivations justifiant le refus de communication n'est donc pas simplement formel. L'interprétation extensive des dispositions de l'article L. 311-5 CRPA conduit actuellement la CADA à pouvoir de sa propre initiative écarter de la communication publique des documents ou informations non classifiés dès lors qu'elle estime souverainement que leur divulgation pourrait conduire à la découverte indirecte d'un secret de défense. Or si une telle préoccupation peut se justifier, il faut reconnaître que la rédaction actuelle des textes ne le permet pas et qu'il faudrait au minimum qu'une modification de l'article L. 311-5 CRPA vienne la consacrer et que le Conseil d'État en valide ensuite les critères d'appréciation.

Mais une autre difficulté d'application des exceptions posées par l'article L. 311-5 CRPA réside dans sa conciliation avec les règles de transparence prévues par la loi en matière d'environnement, et particulièrement en matière nucléaire.

FORTE RESTRICTION DE L'INFORMATION EN MATIÈRE NUCLÉAIRE

L'article 19 de la loi n° 2006-686 du 13 juin 2006 relative à la transparence et à la sécurité en matière nucléaire, désormais codifié à l'article L. 125-10 du code de l'environnement (CEnv), a prévu que toute personne a le droit d'obtenir, auprès de l'exploitant d'une installation nucléaire, les informations détenues sur les risques liés à l'exposition aux rayonnements ionisants pouvant résulter de cette activité et sur les mesures de sûreté et

27. CE 25 mai 2005, *Assoc. Reporters sans frontières et a.*, n° 260926, *Rec.* Lebon T. 707.

Document téléchargé depuis www.cairn.info - Université Paris 8 - - 193.54.174.3 - 14/02/2019 22h55. © Ecole nationale d'administration

de radioprotection prises pour prévenir ou réduire ces risques, dans les conditions définies aux articles L. 124-1 à L. 124-6 du code de l'environnement.

Or, si l'article L. 124-4 I CEnv permet à l'autorité publique de refuser la communication de certaines informations relatives en l'environnement lorsqu'elles contreviendraient en particulier à l'article L. 311-5 CRPA, il prévoit expressément que cette possibilité de refus n'existe pas s'agissant des exceptions visés au e (et relatives « à la monnaie et au crédit public ») et au h du 2° de l'article L. 311-5° (qui concerne – nous l'avons vu – les autres secrets protégés par la loi « sous réserve de l'article L. 124-4 du code de l'environnement »).

Si cette exception empêche donc que des secrets économiques puissent contrarier la diffusion d'informations concernant les risques nucléaires [28] ou plus généralement celle des informations relatives à l'environnement, elle impose cependant que la transparence en matière nucléaire et environnementale cède le pas aux exigences régaliennes, qu'il s'agisse des exceptions de sécurité nationale (politique extérieure, secret de défense) ou de sécurité publique.

À titre d'exemple de cette prévalence de l'impératif sécuritaire sur la transparence citoyenne en matière environnementale, citons notamment cette délibération de 2009 par laquelle la CADA se prononce défavorablement sur la communication de documents relatifs à l'étude d'impact de la chute d'un avion sur un site nucléaire, estimant que bien que l'étude concernée entre dans les informations relatives à l'environnement objet du droit d'accès prévu à l'article L. 124-1 CEnv et suivants (puisqu'elle se rapporte aux retombées radiologiques d'un éventuel sinistre aérien), elle comporte des détails qui pourraient faciliter une attaque terroriste [29]. Elle s'est également déterminée dans le même sens concernant certaines informations relatives au transport de marchandises radioactives [30].

Or, cette priorité donnée aux impératifs sécuritaires sur la nécessaire transparence due aux citoyens dans les domaines touchant l'environnement peut déboucher sur des tensions et sur une incitation à restreindre excessivement la communication dans ces domaines, et donc à vider partiellement de son sens la politique d'information du citoyen.

Un exemple datant de 2003-2004 paraît emblématique de cette confrontation nécessairement délicate. Il concerne l'adoption puis la modification d'un arrêté « relatif à la protection du secret de la défense nationale dans le domaine de la protection et du contrôle des matières nucléaires » [31].

Dans sa rédaction du 24 juillet 2003, l'arrêté pris par le haut fonctionnaire de défense du Ministère de l'industrie soumettait l'ensemble des informations concernant les « matières nucléaires », leur transport, ainsi que « la préparation des exercices de crise relatifs à la protection des matières nucléaires » au régime du secret de la défense nationale.

Son article 1er disposait donc que toutes ces informations « présentent un caractère de secret de la défense nationale et à ce titre doivent faire l'objet d'une classification et de mesures de protection destinées à restreindre leur diffusion ». Mais cette automaticité de la classification fut fortement contestée par les défenseurs de l'environnement qui accusèrent l'État de profiter des réels besoins de sécurité dans le domaine (en particulier, pour ne pas faciliter la commission d'un acte de terrorisme à l'encontre des installations ou des convois

28. Ainsi, le secret en matière commerciale et industrielle ne saurait faire obstacle à la communication de telles informations (CADA, avis n° 20173363 du 11 janvier 2018).

29. Conseil n° 20093470, 8 octobre 2009.

30. CADA, conseil n° 20114256, 3 novembre 2011.

31. Arrêté du 24 juillet 2003 relatif à la protection du secret de la défense nationale dans le domaine de la protection et du contrôle des matières nucléaires abrogé et remplacé par l'arrêté du 26 janvier 2004 (*JORF* n° 24 du 29 janvier 2004).

Document téléchargé depuis www.cairn.info - Université Paris 8 - - 193.54.174.3 - 14/02/2019 22h55. © Ecole nationale d'administration

de matières nucléaires) pour assurer un secret absolu sur les programmes et les installations nucléaires, vidant ainsi de son sens les obligations de transparence imposées par la loi (voir sur cette polémique, et la relation entre environnement et le secret de défense : Prieur, 2006 ; et plus largement : Boutelet, 2012).

Avant même que le Conseil d'État ne statue sur un recours en annulation introduit à l'encontre de cet arrêté de 2003, l'administration fit marche arrière et l'abrogea au profit d'un nouvel arrêté du 26 janvier 2004 dont l'article 1er dispose que présentent un caractère de secret de défense les éléments relatifs à la protection et au contrôle des matières nucléaires « lorsque leur divulgation est de nature à nuire ou à nuire gravement à la protection physique de ces matières nucléaires dans les domaines de la prévention de la malveillance et de la prolifération ».

Cette rédaction respecte désormais les dispositions réglementaires de l'article R. 2311-3 Cdef qui réserve le niveau Confidentiel-Défense aux informations et supports dont la divulgation est de nature à nuire à la défense nationale et le niveau Secret-Défense aux informations et supports dont la divulgation est de nature à nuire gravement à la défense nationale. Tout au plus, l'arrêté de janvier 2004 a-t-il procédé à une sorte d'équivalence entre atteinte à la défense nationale et atteinte à la protection des matières nucléaires contre la malveillance ou la prolifération. Ce qui aurait pu surprendre à l'époque mais qui s'inscrit bien désormais dans le périmètre élargi de la nouvelle notion de sécurité nationale.

Statuant une année plus tard sur le recours pour excès de pouvoir intenté contre l'arrêté de 2003 entre-temps abrogé, le Conseil d'État ne se contenta pas de rejeter les requêtes des associations plaignantes mais en profita pour critiquer la manière dont le texte initial avait voulu imposer une classification automatique sans prise en compte des risques réellement encourus par la sécurité nationale : « en se bornant à énumérer des catégories d'informations relatives aux transports et aux mesures de protection et de contrôle en matière nucléaire qui devront être classifiées, l'arrêté attaqué a eu pour seul objet d'encadrer les décisions ultérieures de classification ; que si cet arrêté lie les autorités chargées de classifier les informations et supports mentionnés à l'article 413-9 du code pénal qui entrent dans le champ de compétence du Ministère de l'économie, des finances et de l'industrie, il ne saurait par lui-même, en l'absence de classification relative à chaque information ou support, produire des effets juridiques vis à vis des tiers » [32].

Mais quel que soit le recadrage effectué à cette occasion, l'épisode a bien mis en lumière le risque permanent qu'une interprétation extensive des pratiques sécuritaires puisse freiner l'ouverture des données dans des domaines sensibles et intéressant le débat public. Plus de quinze années après son 10e rapport annuel, l'avertissement de la CADA en 2001 résonne encore comme une alerte : « L'administration jouit donc en pratique d'une très grande latitude pour fixer le régime d'accès aux documents touchant de près ou de loin au domaine de la défense. Il est à craindre qu'elle ait parfois la tentation de recourir à la classification dans des cas où celle-ci ne se justifie pas au regard des critères fixés par l'article 413-9 du nouveau code pénal pour faire échec à des demandes de communication qu'elle n'entend pas satisfaire » (CADA, 10e rapport, 2001, 41).

32. CE, 25 mai 2005, précité.

Document téléchargé depuis www.cairn.info - Université Paris 8 - - 193.54.174.3 - 14/02/2019 22h55. © Ecole nationale d'administration

CONCILIER SÉCURITÉ ET OUVERTURE, UN ENJEU DE L'*OPEN DATA* DANS LES SECTEURS SENSIBLES

Comme l'a voulu le législateur (lui-même poussé par le droit de l'Union européenne et par la Charte du G8 en la matière), le mouvement actuel d'ouverture et de réutilisation des données s'inscrit dans la continuité juridique du droit de la communication des documents administratifs initié par la loi du 17 juillet 1978.

La loi Lemaire sur « la République numérique » impose maintenant aux collectivités publiques soumises aux nouvelles obligations d'ouverture de leurs données de toujours respecter à cette occasion les exceptions posées par les articles L. 311-5 ou L. 311-6 CRPA [33]. C'est donc bien toute la doctrine et la pratique de la CADA et des juridictions administratives constituées au fil de ces quarante dernières années qui se retrouvent, *ipso facto*, applicables dans le nouveau contexte de l'*open data* public. Ce que résume bien le président Dandelot lorsqu'il écrit que « les règles traditionnelles relatives à la publication des documents administratifs ont été tout naturellement appliquées à la mise en ligne de données publiques par l'administration » (CADA, rapport 2017, 5).

Mais pour autant, le passage d'un mode ancien de type « réactif » (où la communication était demandée par une personne) à celui d'une publication « pro-active » (où l'administration met directement les données à la disposition de tous) va changer les choses, et ce y compris en ce qui concerne l'impact des exceptions sécuritaires de l'article L. 311-5 CRPA.

Le premier risque est sans doute d'origine exogène mais n'en est pas moins sérieux. Comme le soulevait Carolina Cerda-Guzman, les priorités contemporaines de la lutte contre le terrorisme pourraient constituer un frein potentiel au développement des logiques de « gouvernement ouvert » et d'*open data* (Cerda-Guzman, 2014, 47). Il est vrai que cette menace protéiforme, qui relève à la fois de la criminalité et de la violence politique, vient solliciter indifféremment les deux catégories d'exceptions sécuritaires que nous avons identifiées : celles touchant à la sécurité publique et aux procédures judiciaires et celles visant la protection de la sécurité nationale. On a déjà vu comment cette volonté légitime de prévenir le terrorisme pouvait justifier un refus de communiquer des informations qui seraient pourtant utiles aux citoyens pour apprécier les risques sanitaires ou environnementaux (Curtin, 2003, 101).

Un exemple indirect mais plus extrême de cette contamination possible de l'*open data* par la crainte du terrorisme se trouve déjà dans le code du patrimoine qui régit les délais de communication des archives publiques (lesquelles s'articulent avec les dispositions relatives aux données publiques). Depuis l'entrée en vigueur de la loi du 15 juillet 2008, son article L. 213-2 CPatr dispose, *in fine*, que « ne peuvent être consultées les archives publiques dont la communication est susceptible d'entraîner la diffusion d'informations permettant de concevoir, fabriquer, utiliser ou localiser des armes nucléaires, biologiques, chimiques ou toutes autres armes ayant des effets directs ou indirects de destruction d'un niveau analogue ». Là encore, c'est avant tout la crainte légitime de formes d'hyper-terrorisme qui motive cette prohibition, mais on perçoit en même temps jusqu'à quelle extrémité intrinsèquement absurde cette fixation exacerbée sur la prévention du terrorisme pousse notre droit. Créer des archives publiques indéfiniment incommunicables est une forme d'oxymore juridique qui mérite d'être relevée. De notre côté nous avons illustré

33. Voir les nouveaux articles L. 312-1-2 et L. 312-1-3 CRPA (créés par l'article 6 de la loi nº 2016-1321 du 7 octobre 2016) qui font référence aux articles L. 311-5 et L. 311-6 CRPA.

Document téléchargé depuis www.cairn.info - Université Paris 8 - - 193.54.174.3 - 14/02/2019 22h55. © Ecole nationale d'administration

d'autres effets pervers de la priorisation extrême de l'antiterrorisme sur les pratiques de renseignement public (Warusfel, 2017, 151-160).

Sans aller nécessairement jusqu'à de telles extrémités, C. Cerda-Guzman soulève une autre difficulté que peut induire le passage réactif de la communication à la demande à l'ouverture pro-active des données publiques en ligne (pour reprendre le distinguo de M. Dandelot). Elle fait justement remarquer que, dans certains cas (et notamment s'agissant des demandes d'accès dérogatoires à des archives classifiées), la CADA prenait aussi en compte la « nature du lecteur » (privilégiant, par exemple, les chercheurs justifiant d'une réelle démarche scientifique [34]) mais que « cet examen subjectif de la dangerosité ne peut être effectué dans le cadre de l'*open data*. Dans la mesure où cette politique suppose la communication de données à tous les internautes, quel que soit leur statut, elle conduit à exclure des documents à partir du moment où ils se rattachent à certains domaines de la sécurité et sont perçus comme objectivement dangereux, *erga omnes*. On voit donc que dès son origine la transparence prônée par l'*open data* se cantonne à un groupe limité de données » (Cerda-Guzman, 2014, 58).

Au-delà même du risque de survalorisation des impératifs antiterroristes induisant une forme d'autocensure administrative, cette remarque met bien l'accent sur l'un des aspects nouveaux de la politique d'ouverture des données par rapport à celle de communication des documents administratifs voulue à l'origine par la loi pionnière de 1978. Le rôle de la CADA (et, par-delà, de la juridiction administrative appelée à arbitrer les recours) s'en trouve changé. D'une approche au cas par cas où l'individualisation de la norme en fonction des circonstances de communication lui laissait une certaine souplesse (au risque – nous l'avons vu – de se mélanger dans les bases légales de sa motivation), elle doit en venir à la définition préalable de critères objectifs permettant à toutes les collectivités publiques – l'État mais aussi les collectivités territoriales, dont la majorité sont aujourd'hui entraînées dans l'*open data* tout en étant détentrices de données de sécurité (Warusfel, 2016) – de pouvoir trier assez finement les catégories de données qui seraient susceptibles de tomber sous le coup d'une des exceptions prévues à l'article L. 311-5 CRPA.

Deux modifications introduites par la loi Lemaire pourraient y contribuer. D'une part, le nouvel article L. 312-1-2 CRPA prévoit la possibilité de rendre publics des documents et données qui « comportent des mentions entrant dans le champ d'application des articles L. 311-5 ou L. 311-6 » lorsqu'ils ont « fait l'objet d'un traitement permettant d'occulter ces mentions ». Cela transpose dans le nouveau contexte de la publication en ligne le mécanisme des occultations de documents que la CADA recommandait lorsque cela lui apparaissait possible afin de concilier communication et sécurité ou vie privée.

D'autre part, la loi d'octobre 2016 a prévu que la CADA et la CNIL peuvent désormais se réunir « dans un collège unique, sur l'initiative conjointe de leurs présidents, lorsqu'un sujet d'intérêt commun le justifie » [35]. Cette nouvelle possibilité qui commence à se mettre en place va bien évidemment servir au premier chef pour régler les questions de conciliation entre l'ouverture des données et la protection des données personnelles et de la vie privée. Mais, compte tenu de l'expérience et de l'expertise propre à la CNIL dans toutes

34. Elle cite en particulier son avis n° 20132689 du 12 septembre 2013. On peut relever également ses avis n° 20050916-LV du 17 mars 2005 et n° 20051366-LV du 31 mars 2005, dans lequel la CADA indique que « vous aviez déjà formulé de nombreuses demandes d'accès à des archives par dérogation en faisant état de travaux de recherche dont les thèmes ont varié selon les demandes, sans que, à sa connaissance, vous ayez à ce jour publié d'ouvrage, de thèse ou d'article sur l'un ou l'autre de ces sujets… Dans ces conditions, la Commission a estimé que votre projet de recherche ne revêtait pas les assurances scientifiques qui permettent de déroger aux dispositions du code du patrimoine susmentionnées »).

35. Nouvel article L. 341-2 CRPA.

Document téléchargé depuis www.cairn.info - Université Paris 8 - - 193.54.174.3 - 14/02/2019 22h55. © Ecole nationale d'administration

les dimensions de l'usage du numérique, on peut penser que les discussions communes pourront aussi aider la CADA à définir à quel niveau de « granularité » il faut descendre dans le tri des données sensibles pour à la fois maximiser les possibilités de transparence tout en évitant qu'un traitement numérique tiers ne puisse venir *a posteriori* ré-identifier et extraire des informations secrètes, voire classifiées, du volume de données mises en ligne.

C'est là en effet l'une des autres conséquences du changement de paradigme qu'induit la mise en ligne de jeux de données massives. Elle permet la mise en œuvre par les tiers (citoyens, entreprises, journalistes, scientifiques, mais aussi tout autre intervenant légitime ou non) de pratiques de *big data*. Or, comme l'explique la direction de la sécurité du CEA, « les progrès du traitement des données imposent de passer d'une logique séquentielle à une vision globale de la sécurité. C'est moins la sensibilité individuelle de l'information scientifique ou technologique que la connaissance qui peut être déduite de l'analyse d'une somme d'informations, en apparence anodines, qui doit être pris en considération » (Mariotte *et alii*, 2014, 20). Une même prudence anime les archivistes qui soulignent que le développement de pratiques de *big data* pourrait accroître certains risques de divulgation de données sensibles : « Le *data lake* n'ayant *a priori* aucune idée de la nature des données qu'il stocke, le risque est élevé de voir des données personnelles y subsister au-delà de la durée légale, ou de voir des données sensibles être accessibles à tous. Ce risque est d'autant plus élevé que, à la différence des *data warehouses* historiques, le *data lake* contient une majorité de contenus non structurés » (Charaudeau *et alii*, 2015, 383).

Est-ce à dire que les grands services de l'État et leurs ministères régaliens impliqués prioritairement dans les missions de défense et de sécurité vont rester, par prudence ou par invocation abusive du secret, hors du champ de l'ouverture des données ? Ce n'est pas certain. D'ores et déjà, et même si cela demeure très limité, les ministères des Armées ou de l'Intérieur proposent sur leurs sites quelques jeux de données. C'est ainsi que le Ministère de l'intérieur fournit par exemple déjà les données des crimes et délits enregistrés par les services de police et de gendarmerie depuis 2012 et annonce « 555 jeux de données » [36] (même s'ils sont prioritairement consacrés aux fonctions non purement sécuritaires de ce ministère). Du côté de celui des Armées, sa plate-forme d'*open data* donne accès libre aux « principales données relatives à l'économie de la défense, à la condition des effectifs militaires, et au poids du budget de la défense dans l'économie nationale », à l'exception de toute autre donnée touchant les dimensions plus opérationnelles des Armées et des différents services relevant de ce ministère.

Des exemples étrangers montrent d'ailleurs que le mouvement va toucher progressivement les domaines les plus sensibles de l'activité gouvernementale, y compris en matière sécuritaire. À titre au moins symbolique, il est intéressant de souligner l'adoption en 2015 aux États-Unis des principes de transparence pour la communauté du renseignement (*Principles of Intelligence Transparency for the Intelligence Community*) [37]. Il ne s'agit que de l'affirmation de quatre principes sommairement détaillés mais ils indiquent à la fois une forme de *political correctness* très anglo-saxonne mais aussi le début d'une évolution des esprits en vue de la conciliation entre sécurité nationale et société ouverte et numérisée.

L'un de ces principes concerne logiquement la nécessité de protéger les informations relatives aux sources, méthodes et activités des services de renseignement mais il y est affirmé aussi que la classification nécessaire à cette fin doit toujours considérer « au maximum »

36. Sur la page Ministère de l'intérieur sur le site data.gouv.fr.

37. Accessibles sur le site https://www.dni.gov/index.php/ic-legal-reference-book/the-principles-of-intelligence-transparency-for-the-ic.

Document téléchargé depuis www.cairn.info - Université Paris 8 - - 193.54.174.3 - 14/02/2019 22h55. © Ecole nationale d'administration

l'intérêt public. Quant au second principe, il recommande une approche « pro-active » de la mise à disposition de données par tout moyen, notamment numériques.

S'il est sans doute prématuré d'envisager en France une véritable politique d'*open data* dans tous les secteurs touchant la sécurité nationale (et notamment le renseignement), on peut souhaiter que les ministères et les services concernés prennent en compte l'intérêt collectif qu'il y a à ce que, d'une manière ou d'une autre, le dialogue avec la société civile (nécessaire pour que la légitimité de l'action publique soit reconnue, y compris dans ses aspects sécuritaires potentiellement attentatoires aux libertés publiques) puisse profiter d'un partage plus large des données publiques. C'est d'ailleurs un exercice de même nature qu'Herbert Maisl appelait déjà de ses vœux en souhaitant « un nouveau débat sur les cloisonnements indispensables et les décloisonnements utiles » entre transparence et protection de la vie privée (Maisl, 1997, 85).

La publication d'un rapport sur le secret de la défense nationale (en 2015 et 2018) a été un premier signal adressé par le Secrétariat général de la défense et de la sécurité nationale (SGDSN). Sa seconde édition présente les efforts de déclassification réalisés par les principaux ministères (3 500 documents au Ministère de l'intérieur en 2016 et 2 500 par le Ministère des armées pendant la même année) mais reconnaît que « malgré les efforts entrepris, l'actuelle procédure de déclassification ne permet pas aux administrations de déclassifier autant de documents classifiés qu'elles en produisent. C'est pourquoi, dans le cadre des concertations interministérielles menées par le SGDSN, il est envisagé de faire évoluer cette procédure pour faciliter le travail des administrations mais surtout l'accès des chercheurs et des citoyens aux archives publiques » (SGDSN, 2018, 23). Notamment, il propose une réforme relative aux archives par laquelle « la classification ne pourra dépasser cinquante ans, sauf dispositions particulières prévues par le code du patrimoine et destinées notamment à lutter contre la prolifération des armes nucléaire, radiologique, biologique, chimique » (SGDSN, 2018, 17).

Bien qu'il faille rester très prudent lorsqu'il s'agit d'évolution dans ces domaines sensibles, on peut penser que, malgré les réelles inquiétudes qu'une application trop précautionneuse des textes pourrait entraîner, la logique politique du partage de l'information publique avec les citoyens, les entreprises et les chercheurs trouvera progressivement une conciliation utile avec les impératifs légitimes de sécurité. Nous sommes là, en tout état de cause, devant l'une des limites structurelles de l'*open data* que Lucie Cluzel-Métayer nous a invité à ne pas sous-estimer (Cluzel-Métayer, 2016, 102). Il est certain en particulier que le principe d'ouverture par défaut dont elle a souligné la « fragilité » reste lettre morte (malgré la loi Lemaire) dans les domaines régaliens de la sécurité [38]. Mais dans le nouveau droit de la défense et de la sécurité nationale en train de se construire par ailleurs [39], la prise en compte d'une transparence raisonnée et régulée dans ces secteurs devrait pouvoir progresser, notamment en favorisant un dialogue constructif entre les différentes autorités administratives indépendantes qui – parallèlement à la CADA – sont actives dans les différents champs de la sécurité nationale ou de la sécurité publique, comme la CNIL, mais aussi la CSDN, la Commission nationale de contrôle des techniques de renseignement – CNCTR – ou encore le Défenseur des droits. Sur ce terrain particulier, l'enjeu de l'ouverture

38. Un contentieux est d'ores et déjà engagé devant le Conseil d'État s'agissant du refus du Ministère de l'intérieur de mettre en ligne le rapport d'évaluation sur l'usage des caméras-piétons par les policiers (voir https://www.nextinpact.com/news/106989-face-a-justice-ministere-linterieur-refuse-dappliquer-lopen-data-par-defaut.htm).

39. Citons par exemple la conciliation entre impératifs de publicité et de concurrence et nécessités de la sécurité de l'information que réalise la directive 2009/81/CE du 13 juillet 2009 sur les marchés publics de défense et de sécurité.

Document téléchargé depuis www.cairn.info - Université Paris 8 - - 193.54.174.3 - 14/02/2019 22h55. © Ecole nationale d'administration

des données est aussi celui de la modernisation de notre droit public dans une société où la puissance publique doit assumer la légitimité de ses prérogatives sécuritaires tout en préservant les libertés fondamentales et l'accès le plus large aux ressources numériques.

Références bibliographiques

Boutelet, Marguerite (2009-2012), « Le droit à l'information du public à l'épreuve du secret défense », *in* SEMIPAR, *Secret militaire et participation en matière nucléaire*, Convention 6422, p. 95.

CADA (2001), 10e rapport, La documentation française.

CADA (2018), Rapport d'activité 2017, juin.

Cerda-Guzman, Carolina (2014), « L'*open data* à l'épreuve de la lutte contre le terrorisme », *in* Gilles J. Guglielmi et Élisabeth Zoller (dir.), *Transparence, démocratie et gouvernance citoyenne*, Éd. Panthéon-Assas, p. 47.

Charaudeau, Marie-Odile ; Fritel, Alexis ; Huot, Charles ; Martin, Philippe ; Prével, Laurent (2015), « Et demain ? Archivage et *big data* », *La Gazette des archives*, nº 240, 4, p. 383.

Cluzel-Métayer, Lucie (2016), « Les limites de l'*open data* », *AJDA*.

Curtin, Deirdre (2003), "Digital government in the European Union: freedom of information trumped by "internal security"", *in National security and open government: Striking the right balance*, Campbell Public Affairs Institute, Syracuse University, p. 101.

Livre blanc sur la défense et la sécurité nationale (2008), Éd. O. Jacob.

Maisl, Herbert (1997), « Le citoyen internaute entre liberté d'accès aux documents administratifs et protection des données personnelles », *Revue française d'administration publique*, nº 81, p. 77-85.

Mariotte, Frédéric ; Chican, Jean-Pierre et Profichel, Jean-François (2017), « *Big data* et intelligence économique : entre prudence et opportunité », *Clefs CEA* nº 64, p. 20.

Prieur, Michel (2006), « Nucléaire, information et secret défense », *Revue juridique de l'environnement*, nº 3, p. 289-301.

SGDSN (2018), *2e rapport sur le secret de la défense nationale en France.*

Warusfel, Bertrand (2000), *Contre-espionnage et protection du secret – Histoire, droit et organisation de la sécurité nationale en France*, Éditions Lavauzelle, 2000, p. 361-380.

Warusfel, Bertrand (2011), « La sécurité nationale, nouveau concept du droit français », *in Les différentes facettes du concept juridique de sécurité – Mélanges en l'honneur de Pierre-André Lecocq*, Lille2, décembre, p. 461-476.

Warusfel, Bertrand (2013), « Pour un véritable secret de sécurité nationale », *in Administration – Revue de l'administration territoriale de l'État*, nº 239, septembre-octobre, p. 76-78.

Warusfel, Bertrand (2016), « Loi Lemaire : les collectivités territoriales dans la République numérique », *Bulletin juridique des collectivités locales*, nº 12, décembre.

Warusfel, Bertrand (2017), « La (re)définition d'un droit du renseignement », *in* Julie Alix et Olivier Cahn, *L'hypothèse de la guerre contre le terrorisme – Implications juridiques*, Dalloz, p. 151-160.

Document téléchargé depuis www.cairn.info - Université Paris 8 - - 193.54.174.3 - 14/02/2019 22h55. © Ecole nationale d'administration