



Rapport sur le secret de la défense nationale en France / II

Janvier 2018



Secrétariat général
de la défense
et de la sécurité nationale

Rapport sur le secret
de la défense
nationale en France / II



Trois ans après la parution d'un premier rapport sur la protection du secret de la défense nationale, le secrétariat général de la défense et de la sécurité nationale (SGDSN) renouvelle l'exercice, dans un souci de pédagogie et de bonne information des citoyens.

Objet de bien des fantasmes, qui l'assimilent encore parfois aux excès d'une raison d'État oublieuse des droits et libertés, le secret est pourtant un outil essentiel de défense de nos intérêts diplomatiques, économiques, stratégiques et sécuritaires. Il permet de garantir la confidentialité de près de cinq millions de documents sensibles, relatifs aussi bien à la conduite de nos interventions extérieures qu'à la lutte contre le terrorisme ou à la sécurité de nos infrastructures vitales.

Comme le met en valeur ce rapport, la protection du secret n'est d'ailleurs pas l'apanage d'un cercle restreint d'initiés. Elle relève de la responsabilité individuelle des quelques 400 000 personnes habilitées en France, dans les administrations comme dans les entreprises qui opèrent dans des secteurs sensibles, celui de l'énergie notamment. Elle est, de plus en plus, un objet de coopération avec nos alliés, dans le cadre de l'Union européenne et de l'OTAN en particulier.

Eclairer les enjeux concrets pour notre pays de la protection du secret, mieux faire connaître les règles de droit qui la régissent et les acteurs chargés de leur mise en œuvre, telle est la vocation de ce document de référence.

M. Louis GAUTIER,
Secrétaire général de la défense et de la sécurité nationale



Sommaire

1. La protection du secret, une œuvre collective	5
1.1 Le Premier ministre, responsable de la défense nationale, définit le cadre de la politique de protection du secret	7
1.2 Les ministères mettent en œuvre la protection du secret dans leur domaine de compétence	8
1.3 Le réseau des officiers de sécurité veille à la protection du secret dans les administrations et les entreprises	8
1.4 Les personnes habilitées : 400 000 acteurs quotidiens de la protection du secret	9
2. Vers une réforme de la protection du secret de la défense nationale	11
3. Lever le secret, la déclassification des documents	15
3.1 La déclassification	17
3.2 La communication	17
3.3 Une volonté d'ouverture et de transparence	19
4. Les entreprises et le secret de la défense nationale	21
4.1 L'accès au secret, une nécessité pour les entreprises engagées dans des secteurs stratégiques	23
4.2 L'accès au secret soumis au respect d'exigences de sécurité	23
4.3 La fin de l'habilitation	24
5. La protection du secret au cœur de nos alliances internationales	27
5.1 Les accords généraux de sécurité, instruments de la coopération bilatérale en matière de secret	29
5.2 L'OTAN et l'Union européenne, cadres de protection en commun du secret	30
5.3 Le rôle central du SGDSN, autorité nationale de sécurité, dans les négociations internationales relatives au secret	30
Annexes	31
Annexe 1 : Comment une demande d'habilitation est-elle remplie ?	33
Annexe 2 : Comment une information est-elle classifiée ?	37
Annexe 3 : Comment les informations et supports classifiés sont-ils gérés ?	41
Le secret en bref	43
Glossaire	44
Pour aller plus loin	46



1. La protection du secret, une œuvre collective



1.

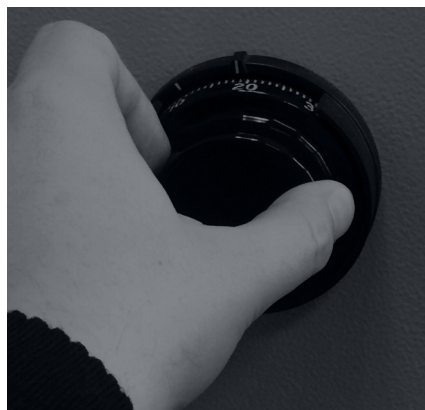
La protection du secret, une œuvre collective

La protection du secret de la défense nationale implique une grande diversité d'acteurs, détenteurs de la puissance publique ou opérateurs économiques dans des secteurs sensibles. Le Premier ministre, assisté par le secrétariat général de la défense et la sécurité nationale (SGDSN), et les ministres dans leur champ de compétence définissent les règles relatives à la protection des supports classifiés et à la délivrance des habilitations (cf. glossaire). La préservation du secret repose également, au sein des administrations et des entreprises concernées, sur l'action d'un réseau de 4 000 officiers de sécurité et sur la responsabilité des 400 000 personnes habilitées en France.

1.1 Le Premier ministre, responsable de la défense nationale, définit le cadre de la politique de protection du secret

Le Premier ministre assure un rôle primordial en matière de protection du secret de la défense nationale. Il prend l'ensemble des décisions relatives au niveau de classification le plus élevé (« Très Secret Défense »), qu'il s'agisse de déterminer les informations qu'il y a lieu de classer, de définir les modalités de protection de celles-ci, ou d'accorder les habilitations. Il fixe en outre le cadre dans lequel les ministres exercent leurs pouvoirs pour les niveaux de classification inférieurs.

Le Premier ministre est assisté dans l'exercice de ces responsabilités par le SGDSN, organe interministériel chargé d'étudier, de proposer, de coordonner et de contrôler la mise en œuvre des mesures propres à assurer la protection du secret. En tant qu'autorité nationale de sécurité (ANS), le SGDSN est aussi l'interlocuteur des États étrangers et des organisations internationales dans la négociation d'accords généraux de sécurité (AGS) permettant l'échange d'informations classifiées avec des partenaires étrangers (cf. *infra*).





1.2 Les ministères mettent en œuvre la protection du secret dans leur domaine de compétence

Les ministres sont responsables de la sécurité des informations et supports classifiés dans toute entité publique ou privée relevant de leur champ de compétence. Ils prennent les décisions d'habilitation de niveau « *Confidentiel défense* » et « *Secret défense* » et définissent les modalités de protection des informations relevant de ces niveaux de classification.

Pour remplir ses missions, chaque ministre s'appuie sur un haut fonctionnaire de défense et de sécurité (HFDS). Placé à la tête d'un service spécialisé, généralement assisté par un fonctionnaire de sécurité et de défense et par un fonctionnaire de sécurité des systèmes d'information, le HFDS :

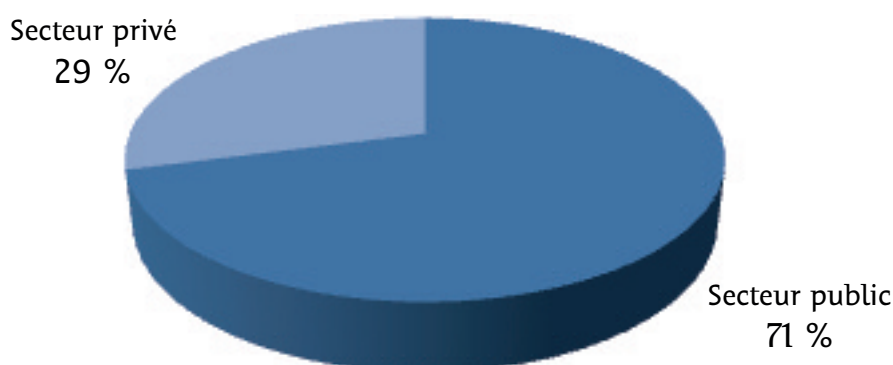
- veille au bon fonctionnement des services chargés de gérer des informations et supports classifiés ;
- effectue les contrôles et inspections nécessaires ;
- propose des mesures destinées à renforcer la protection des informations classifiées ;
- prend des décisions d'habilitation par délégation du ministre.

1.3 Le réseau des officiers de sécurité veille à la protection du secret dans les administrations et les entreprises

8

Les officiers de sécurité constituent un réseau de 4 000 personnes, présentes dans les administrations et les entreprises qui traitent et détiennent des informations et supports classifiés. Près d'un tiers exercent leurs fonctions dans le secteur privé (cf. graphique).

Répartition des 4 000 officiers de sécurité



Nommés par le chef de leur service employeur, ces officiers prennent en charge la sécurité au sein de leur organisation et veillent à la bonne application des règles de protection du secret. Ils sont les correspondants du haut fonctionnaire de défense et de sécurité du ministère auquel ils sont rattachés, ainsi que des services enquêteurs.



Leurs missions sont définies par l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale. Ils doivent notamment :

- ▶ gérer les habilitations ;
- ▶ sensibiliser les personnels concernés ;
- ▶ contrôler l'accès aux zones réglementées et le respect des dispositions réglementaires en matière d'accès, de manipulation, de conservation, de reproduction et de destruction des informations classifiées.



Dès 2018, l'Institut national des hautes études de la sécurité et de la justice (INHESJ) dispensera, en partenariat avec le SGDSN, une formation spécifique aux fonctions d'officier de sécurité.

1.4 Les personnes habilitées : 400 000 acteurs quotidiens de la protection du secret

La protection du secret de la défense nationale relève enfin et surtout de la responsabilité des 400 000 personnes habilitées que compte notre pays. Face au risque que ferait courir à la Nation une diffusion non maîtrisée des informations classifiées, il apparaît vital que tous les personnels concernés s'approprient pleinement les règles qui régissent l'usage de celles-ci. La protection du secret est, in fine, une œuvre collective.



Pour mieux connaître les règles de sécurité, il est désormais possible de s'entraîner sur :

<http://tcs.sgdsn.gouv.fr>



La longue histoire de la protection du secret

La fonction de gardien du secret de la défense nationale s'inscrit dans une longue tradition historique, que l'on peut faire remonter aux temps de la monarchie capétienne.

Les chambellans se voyaient ainsi confier la garde du sceau secret du roi. La première trace officielle de cette mission apparaît à l'article 4 de l'ordonnance de Bourges du 16 novembre 1318 : « *Et deffendons à nostre chambellain qui nostre scel secret portera, qui il ne scelle, ne encloe austres lettres, fors ou cas, et en la manière dessus diz* ».

Après la Révolution, Napoléon réorganise cette fonction, d'abord au cabinet de l'Empereur, puis dans les bureaux des ministères de la Guerre, de la Marine et des Affaires étrangères.

Confondue avec les activités de contre-espionnage, cette activité est redéfinie en 1945, sous l'impulsion directe du Général de Gaulle. Quelques semaines après la fin du conflit, il procède à la création d'un service de protection du secret à l'État-major général de la défense nationale, devancier de l'actuel SGDSN.

Son retour au pouvoir en 1958 consolide la protection du secret, avec la création par un décret du 11 mars 1963 d'un *service de sécurité de défense (SSD) au sein du secrétariat général de la défense nationale (SGDN)*.

Cet intérêt pour le secret traduit une ambition stratégique pour la France : il va de pair avec le développement de grands programmes, dans le domaine nucléaire et spatial par exemple, qui nécessitent un respect rigoureux du secret.

En 2009, le SGDN devient SGDSN et le SSD devient une sous-direction chargée de la protection du secret.

*

Ainsi, depuis le XIV^{ème} siècle, malgré les vicissitudes de l'Histoire, la fonction est demeurée au plus près du pouvoir : le chambellan, le secrétaire du cabinet de l'Empereur et le secrétaire général de la défense et de la sécurité nationale. Cette continuité historique témoigne de l'attention constante portée par les autorités françaises à la protection du secret de l'État, clef de voûte des politiques de protection et de sécurité de la Nation.



Un chambellan issu d'un extrait d'une miniature représentant un hommage (1369)

Gallica / Bibliothèque nationale de France



2. Vers une réforme de la protection du secret de la défense nationale



2.

Vers une réforme de la protection du secret de la défense nationale

Pour assurer sa protection, la pratique du secret est très règlementée. L'instruction générale interministérielle n° 1300 (IGI n° 1300) sur la protection du secret de la défense nationale définit les règles de gestion et d'utilisation des informations et supports classifiés. Elle articule les dispositions législatives et réglementaires issues du code pénal, du code de procédure pénale, du code de la défense et du code du patrimoine.

Une importante concertation interministérielle est actuellement en cours pour faire évoluer cette réglementation en profondeur.

Les objectifs visés sont les suivants :

- faciliter les échanges internationaux qui augmentent de manière exponentielle et aligner avec nos principaux alliés nos niveaux de classification ;
- améliorer la prise en compte de l'information classifiée dématérialisée et la protection des systèmes d'information contenant de telles informations de façon à s'adapter à la menace cyber. L'information doit être protégée tout au long de son cycle de vie, de sa conception à la fin de son exploitation ;
- changer la dénomination des niveaux de classification afin de mettre en évidence la nature interministérielle du secret avec, à l'avenir, deux nouvelles appellations *Secret* et *Très secret* ;
- réviser la procédure d'habilitation pour réduire les délais d'enquêtes ;
- simplifier la procédure de déclassification des documents :
 - la mention de l'échéance de la classification devra être indiquée sur le document ;
 - 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.

13

Ainsi, un document classifié devra comporter non seulement le timbre de classification, mais devra aussi préciser la dénomination de l'entité émettrice, le lieu, la date, le numéro d'enregistrement, mais surtout la date de déclassification du document, comme le montre le document ci-dessous.

DÉFENSE ET SÉCURITÉ NATIONALE SECRET	Dénomination de l'entité émettrice	SPÉCIAL FRANCE
Service émetteur		Lieu, date N° Déclassifié le :
<u>Objet</u>	: Intitulé	



3.

Lever le secret, la déclassification des documents



3.

Lever le secret, la déclassification des documents

Le secret de la défense nationale protège les intérêts fondamentaux de la Nation. Lorsque ces derniers ne sont plus en jeu, il est normal que le secret soit levé et que les règles ordinaires de conservation et de communication des documents soient appliquées. Ce processus intervient de différentes manières.

3.1 La déclassification

À tout instant, l'autorité qui a classifié une information peut la déclassifier si celle-ci n'est plus sensible.

En France, la déclassification n'est jamais automatique, ni obligatoire. Elle intervient après décision formelle de l'autorité émettrice.

17

3.2 La communication

Un document classifié ne peut jamais être communiqué au public sans déclassification préalable.

Le délai légal de communication d'un document couvert par le secret de la défense nationale, après déclassification préalable, est de 50 ans, voire de 100 ans si sa communication est de nature à porter atteinte à la sécurité des personnes nommément désignées ou facilement identifiables. Certains documents restent par ailleurs incommunicables de façon permanente, conformément à nos engagements internationaux, lorsqu'ils entraînent la diffusion d'informations permettant de concevoir, d'utiliser ou de localiser des armes nucléaires, biologiques ou chimiques.

Des dérogations à ces délais sont possibles. Un accès anticipé, toujours après déclassification préalable, peut notamment être autorisé à la suite d'une demande formulée dans le cadre de recherches scientifiques, par exemple historiques. C'est à l'autorité émettrice qu'il revient d'accéder ou non à cette demande.

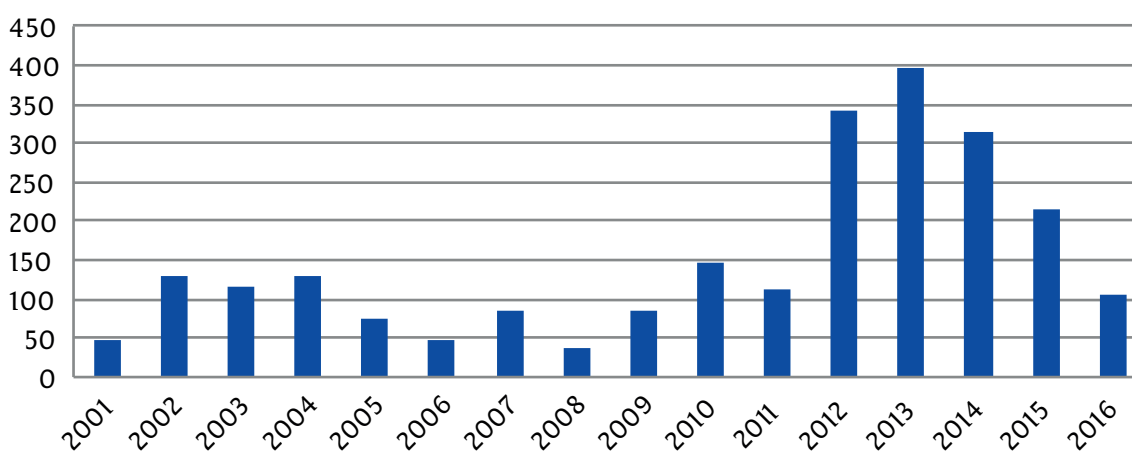
Concrètement, l'autorité qui a procédé à la classification, va relire le document et s'assurer qu'il ne contient plus d'information sensible. Elle va aussi vérifier le respect des différents délais imposés par le code du patrimoine.

Dans tous les cas, les services détenteurs d'archives procèdent à la vérification du délai de communicabilité auquel le document se rattache.



Au SGDSN, une commission d'accès aux archives est chargée d'examiner ces demandes depuis 2005. Elle évalue la sensibilité des documents classifiés concernés et rend un avis sur leur éventuelle déclassification, ainsi que, le cas échéant, sur l'opportunité de les communiquer de manière anticipée. Une centaine de cartons d'archives ont été demandés en 2016. Un carton peut contenir plusieurs dossiers qui eux-mêmes renferment plusieurs documents. Ainsi, cette même année, 135 dossiers ont été déclassifiés.

Nombre de demandes par année aux archives du SGDSN



Au cours des cinq dernières années, le taux d'avis favorables rendus par la commission d'accès aux archives du SGDSN se stabilise autour de 80 %. Les rares refus furent motivés par la protection des données intéressant la défense nationale ou la sécurité du pays et, en ce qui concerne la communication anticipée des pièces, par les exigences de la protection de la vie privée.

Année	Nombre de commissions	Nombre de dossiers demandés	% d'avis favorables à la communication
2016	11	104	80
2015	13	211	89
2014	19	315	85
2013	14	396	84
2012	10	343	81



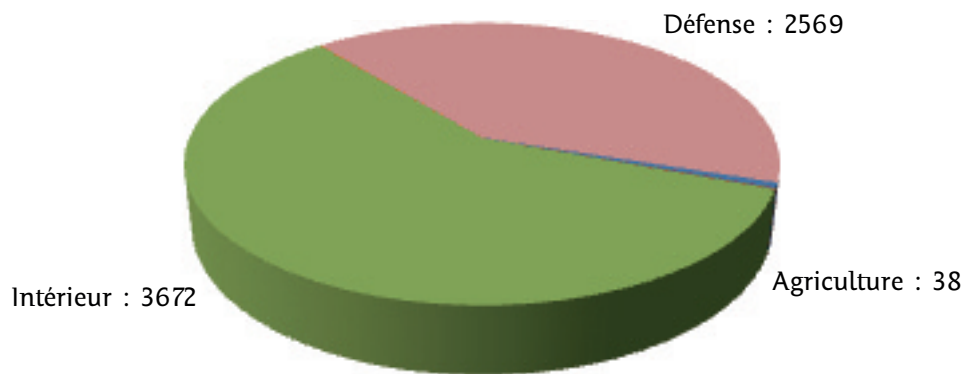
3.3 Une volonté d'ouverture et de transparence

Le travail effectué par la commission d'accès aux archives du SGDSN s'inscrit plus largement dans le cadre d'une politique d'ouverture des archives aux historiens et aux chercheurs.

À plusieurs reprises, le Président de la République s'est prononcé en faveur de la déclassification d'archives. En 2015, le Président François Hollande a souhaité que soient ouvertes celles de la Seconde Guerre mondiale. Dans une perspective similaire, le SGDSN s'est vu confier la mission de travailler à la déclassification des archives relatives à l'engagement de la France au Rwanda entre 1990 et 1994. Plus récemment encore, en déplacement au Burkina Faso, l'actuel Président de la République s'est engagé à déclassifier les archives relatives à l'affaire Thomas Sankara.

Ainsi, les ministères ont mené d'intenses activités de déclassification. Le ministère de l'intérieur a déclassifié, en 2016, plus de 3 500 documents. Le ministère des armées en a déclassifié plus de 2 500.

Nombre de documents déclassifiés par les ministères en 2016



Cependant, force est de constater 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.

Ces différents chantiers témoignent d'une volonté de concilier au mieux le secret de la défense nationale avec les exigences de transparence d'une société démocratique, tout en consolidant les règles et les modalités d'application pour assurer la plus grande sécurité de notre pays et la meilleure protection de ses intérêts fondamentaux.



4.

Les entreprises et le secret de la défense nationale



4.

Les entreprises et le secret de la défense nationale

Les entreprises peuvent avoir besoin d'accéder au secret de la défense nationale pour effectuer des travaux qui leur sont confiés par l'État dans des domaines sensibles. Il s'agit notamment de l'armement, de l'énergie ou des télécommunications.

4.1 L'accès au secret, une nécessité pour les entreprises engagées dans des secteurs stratégiques



L'accès au secret des entreprises demeure limité à l'objet de leurs activités. Comme les personnes physiques, les personnes morales doivent être habilitées pour accéder à un secret de la défense nationale. Leur accès au secret est limité à l'objet des travaux confiés. L'entreprise ne classe que les documents qui s'y rapportent. Elle ne peut pas avoir accès à des documents, ni en classer, dans d'autres domaines.

23

Les entreprises sont habilitées dans le cadre d'un contrat conclu avec l'autorité publique pour l'exécution de travaux classifiés. Ce

contrat comporte une clause de protection du secret et une annexe de sécurité qui énumère les exigences de sécurité et détermine le besoin d'en connaître (cf. *glossaire*).

Pour être habilitée, l'entreprise transmet un dossier à l'autorité publique contractante qui, après vérification, le soumet à l'autorité d'habilitation qui prendra sa décision.

Ce n'est qu'une fois la personne morale habilitée que les personnes physiques travaillant pour son compte pourront l'être à leur tour.



4.2 L'accès au secret soumis au respect d'exigences de sécurité

La responsabilité pénale et contractuelle de la personne morale est engagée en cas de non-respect des mesures de sécurité.

Le représentant légal établit une politique de sécurité de l'entreprise pour la protection des informations et supports classifiés ainsi que, le cas échéant, la sécurité des systèmes d'informations classifiés.

Il désigne un officier de sécurité et, si nécessaire, un officier de sécurité des systèmes d'information.

Lorsque l'exécution du contrat implique la détention d'informations classifiées, la personne morale doit déposer un dossier d'aptitude physique à détenir de telles informations. Si à l'occasion d'un précédent contrat, elle a déjà bénéficié d'une telle évaluation, elle doit fournir l'avis technique d'aptitude physique délivré par le service enquêteur. Des contrôles sont diligentés périodiquement dans les locaux.

En cas d'utilisation d'un système d'information pour traiter d'informations classifiées, elle doit s'engager dans une démarche d'homologation de ces systèmes.

La personne morale de droit privé, comme toute personne physique, ne peut se prévaloir publiquement de son habilitation.

4.3 La fin de l'habilitation

L'habilitation en cours de validité peut être retirée si son titulaire ne remplit plus les conditions nécessaires à sa délivrance, ce qui est le cas lorsque des éléments de vulnérabilité apparaissent.

Lorsque les travaux classifiés sont terminés, l'autorité contractante informe le titulaire du contrat de la destination à donner aux informations et supports classifiés. Une fiche de clôture du plan contractuel de sécurité détermine les modalités d'archivage et de démantèlement.



La première affaire judiciaire de compromission



Nicolas IV de Neufville, marquis de Villeroy, secrétaire particulier de Charles IX, conseiller d'Henri III, ministre d'Henri IV et de la régente Marie de Médicis.

Une affaire d'espionnage à la cour d'Henri IV

Nicolas l'Hôte est au cœur de la première affaire judiciaire de compromission en 1604. Alors qu'il est en poste à l'ambassade de France en Espagne, il se lie d'intelligence avec des secrétaires d'État espagnols et leur fournit des informations secrètes.

De retour en France, il entre, en qualité de commis, au déchiffrement des dépêches au service du marquis de Villeroy, qui cumule alors les fonctions de secrétaire d'État à la guerre et des affaires étrangères sous Henri IV. Il continue à renseigner la couronne espagnole en lui communiquant les délibérations confidentielles du Conseil du Roi.

Or, dès le règne de Louis IX, les membres du conseil s'engagent à respecter le secret des délibérations. Ce principe vient tout juste d'être réaffirmé par le règlement du Conseil du 11 août 1578.

Les fuites sont connues. Des intrigues permettent de découvrir la « taupe ».

Interceptant le message qui le dénonce, Nicolas l'Hôte s'enfuit. Poursuivi par les archers du prévôt, il traverse la Marne à Fay le Bac et s'y noie.

Certains courtisans remettent en cause cette version officielle. Selon eux, Nicolas l'Hôte aurait été assassiné par le marquis de Villeroy qui craignait d'être dénoncé par son commis. Le marquis de Villeroy a poursuivi sa carrière sans être inquiété.

Un procès post-mortem

En revanche, le cadavre de Nicolas l'Hôte est repêché et embaumé au Châtelet de Paris. On lui fera son procès.

Le principe de la pénalisation de la compromission a été posé par François 1^{er} à l'article 34 de l'édit du 24 juillet 1534. Sous peine de crime de lèse-majesté, il était défendu de parlementer avec les ennemis. L'incrimination était très générale. Un édit de Charles IX du 16 août 1563 vient préciser l'objet des conversations « pour chose concernant nostre estat ».

Ainsi, Nicolas l'Hôte est condamné, par arrêt du 15 mai 1604, à « être traîné sur une claie, la face contre terre, ensuite tiré à quatre chevaux, et enfin à ce que les quartiers soient exposés sur quatre roues aux quatre principales avenues de la ville ».

La protection du secret consolidée

À l'issue de cette affaire, plusieurs ambassadeurs étrangers à Paris font part de leur crainte quant au traitement de leurs dépêches qui ne pourront plus contenir d'éléments importants. Pour prévenir la réitération de tels faits, le chiffre est changé et le recrutement des commis plus rigoureux.



5.

La protection du secret au cœur de nos alliances internationales



5.

La protection du secret au cœur de nos alliances internationales

5.1 Les accords généraux de sécurité, instruments de la coopération bilatérale en matière de secret

Dans le cadre de ses coopérations civiles ou militaires, la France a besoin d'échanger des informations classifiées avec des États ou des ressortissants étrangers. Ces échanges s'effectuent dans le cadre d'accords généraux de sécurité (AGS) conclus avec les autorités du pays concerné.

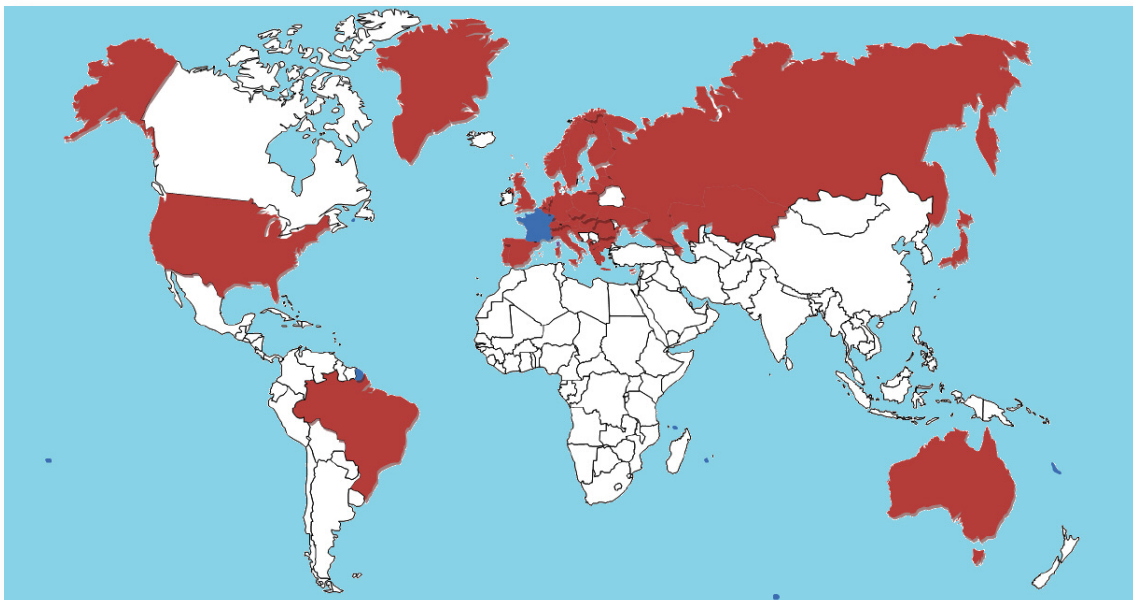
L'objet de l'accord est de permettre la transmission et la protection d'informations classifiées et d'organiser les conditions de cet échange. Il précise les modalités d'échange et de conservation des informations, permet la reconnaissance réciproque des habilitations de sécurité des personnes physiques et morales. Il établit aussi des équivalences entre les niveaux de classification fondée sur un niveau de protection comparable. Malgré une dénomination commune, certains niveaux de classification peuvent faire l'objet de procédures de sécurité différenciées entre les États partenaires et donc être plus complexes à recevoir, manipuler ou à transmettre.

En l'absence d'accord de sécurité, la transmission d'informations classifiées françaises constitue une compromission du secret de la défense nationale.

29

En sa qualité d'autorité nationale de sécurité, le SGDSN est l'interlocuteur des autorités de sécurité étrangères. Il négocie les accords généraux de sécurité avec les États, les organisations internationales, les institutions et les organes de l'Union européenne. Dans ce cadre, il étudie de manière approfondie les règles de protection du secret dans ces États ou institutions et vérifie qu'elles sont homogènes afin de garantir la sécurité des échanges d'informations.

États avec lesquels la France a conclu des accords généraux de sécurité





En 2017, la France est partie à 41 accords généraux de sécurité avec des États étrangers. Elle échange aussi des informations dans les cadres multilatéraux de l'Union européenne et de l'Organisation du traité de l'Atlantique Nord (OTAN).

5.2 L'OTAN et l'Union européenne, cadres de protection en commun du secret

L'OTAN a mis en place un cadre réglementaire pour la protection et la sauvegarde de ses informations classifiées, ou qui lui sont soumises par un État. Un accord pour la sécurité des informations a été signé à Bruxelles le 6 mars 1997, aux termes duquel les États s'engagent mutuellement à protéger les informations classifiées produites ou reçues. La protection des informations classifiées de l'Organisation est régie par une politique de sécurité, comprenant l'accord de sécurité et des directives complémentaires, elles-mêmes déclinées en recommandations et obligations. Ses standards sont transposés en droit interne français par l'instruction interministérielle n° 2100 pour l'application en France du système de sécurité de l'OTAN.

Les États membres de l'Union européenne se sont également non seulement engagés à échanger des informations classifiées nationales dans l'intérêt de l'Union, mais aussi à produire des informations classifiées dites de l'Union européenne (ICUE). Afin d'assurer la protection des ICUE, les États doivent respecter les règles de sécurité posées par une décision du Conseil européen. Ces règles sont transcrites en droit français dans l'instruction générale interministérielle n° 2102 relative à la protection en France des informations classifiées de l'Union européenne, approuvée en juillet 2013.

30

5.3 Le rôle central du SGDSN, autorité nationale de sécurité, dans les négociations internationales relatives au secret

Le SGDSN, qui conduit pour la France la négociation des accords généraux de sécurité (*cf. supra*), assure également les fonctions d'autorité nationale de sécurité (ANS) prévues notamment par la réglementation de l'Union européenne.

À ce titre, il veille à la sécurité des ICUE et des informations classifiées OTAN, et représente la France dans les enceintes multilatérales où sont élaborées de nouvelles réglementations en matière de protection du secret, comme les institutions et organes de l'Union européenne (Conseil, Commission, Service européen pour l'action extérieure, Europol) ou le Comité de sécurité de l'OTAN.



Annexes



Annexe 1 : Comment une demande d'habilitation est-elle remplie ?

1. À quel moment ?

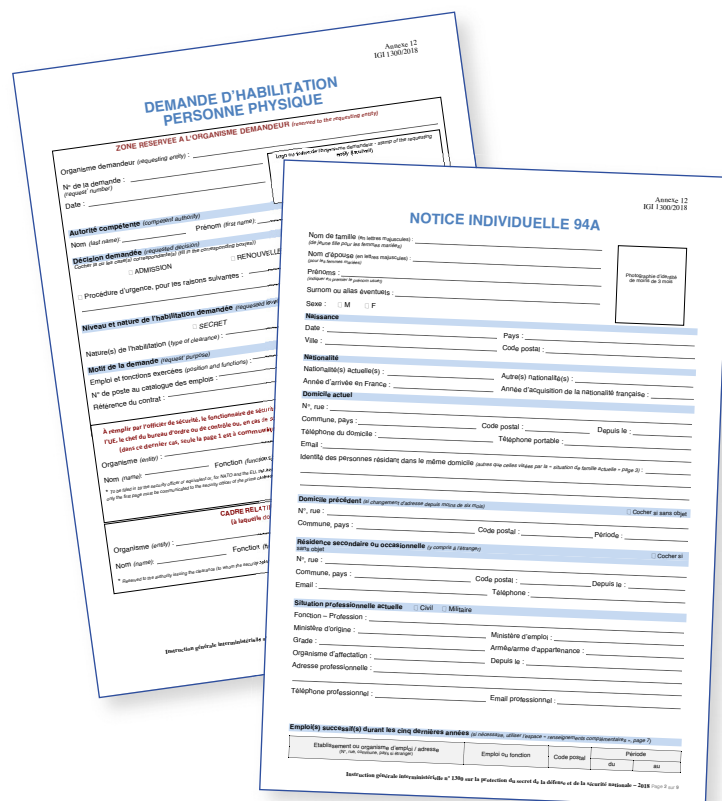
Sur demande de l'officier de sécurité, les demandes d'habilitation doivent être remplies en cas de :

- ▶ nomination dans un nouvel emploi ;
- ▶ changement de situation personnelle ;
- ▶ changement de poste ;
- ▶ renouvellement de l'habilitation qui va arriver à échéance.

2. Qu'est-ce qu'un dossier d'habilitation ?

Le dossier d'habilitation a pour objet de réunir les éléments qui seront vérifiés lors de l'enquête de sécurité. Il est constitué de :

- ▶ la demande d'habilitation formulée par l'employeur attestant le besoin de connaître des informations et supports classifiés à un niveau donné ;
- ▶ la notice individuelle de sécurité, renseignée intégralement par le candidat et vérifiée par l'officier de sécurité de l'entité dont il relève.





Le dossier est transmis par l'autorité d'habilitation au service enquêteur compétent (direction générale de la sécurité intérieure ou direction du renseignement et de la sécurité de défense) afin qu'il diligente une enquête administrative.

Cette enquête administrative est fondée sur des critères objectifs permettant de déterminer si l'intéressé, par son comportement ou par son environnement proche, présente une vulnérabilité, soit parce qu'il constitue lui-même une menace pour le secret, soit parce qu'il se trouve exposé à un risque de chantage ou de pressions pouvant mettre en péril les intérêts de l'État, chantage ou pressions exercés notamment par un service étranger de renseignement, un groupe terroriste, une organisation ou une personne se livrant à des activités subversives.

3. Comment la notice est-elle remplie ?

Une notice mal remplie ne sera pas prise en compte et elle sera retournée à l'officier de sécurité par le service enquêteur. De la précision avec laquelle la notice est remplie dépendra la rapidité du traitement de la demande. En cas de doute, le candidat peut consulter l'officier de sécurité.

Le candidat s'engage sur l'exactitude des renseignements fournis et s'expose, en cas d'altération frauduleuse, à une peine de 3 ans d'emprisonnement et 45 000 euros d'amende.

34

Plusieurs renseignements concernent la famille du candidat. Demander directement ces renseignements peut être délicat. Le candidat est alors invité à expliquer à ses proches que cette procédure de sécurité est habituelle et nécessaire à l'exercice de ses fonctions. En revanche, le candidat ne doit jamais décrire les aspects sensibles de son activité. La discrétion est un gage de sécurité.

Par la suite, il sera tenu d'informer l'officier de sécurité de tout changement de situation qui affecte sa vie personnelle (changement d'adresse, mariage, naissance d'enfants).

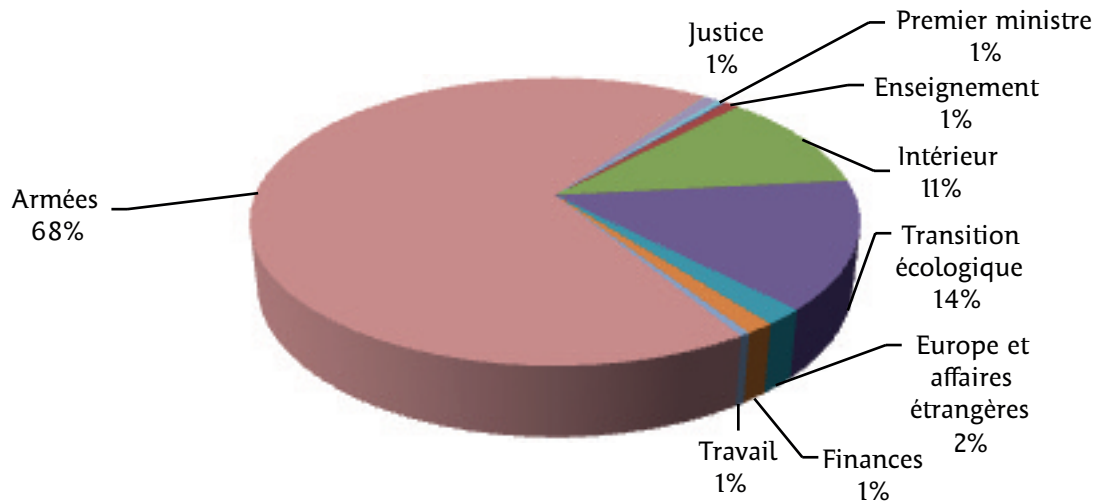
4. Et après ?

Sur demande de l'officier de sécurité, les demandes d'habilitation doivent être remplies en cas de :

- ▶ 1. Un avis de sécurité est rendu par le service enquêteur ;
 - ▶ 2. L'autorité d'habilitation prend la décision d'habilitation et en informe l'employeur ;
 - ▶ 3. L'officier de sécurité notifie la décision à l'intéressé ;
 - ▶ 4. L'intéressé signe un engagement de responsabilité.
-



Répartition des habilitations par ministère



Près de 400 000 personnes sont habilitées. Les deux tiers le sont par le ministère des armées, 14 % par le ministère chargé de la transition écologique et 11 % par le ministère de l'intérieur.

Près de 100 000 habilitations sont délivrées chaque année.



Annexe 2 : Comment une information est-elle classifiée ?

1. Qu'est-ce qui est classifié ?

La protection du secret de la défense nationale vise à maîtriser la diffusion d'informations stratégiques dont la compromission porterait atteinte aux intérêts fondamentaux du pays. Ces informations constituent une cible majeure pour les services étrangers comme pour des groupements hostiles cherchant à déstabiliser l'État ou la société. Aujourd'hui, plus de 5 millions de documents sont couverts par le secret de la défense nationale, essentiellement dans le domaine de la défense, mais aussi de la sécurité énergétique.

La décision de classifier résulte de l'analyse de l'importance de l'information au regard des textes applicables, des instructions du ministre compétent, mais surtout des risques et menaces.

En fonction de sa sensibilité, l'information est couverte, jusqu'à la mise en œuvre de la réforme de la protection du secret de la défense nationale, par l'un des trois niveaux de classification suivants :



- ▶ **Confidentiel Défense** : réservé aux informations et supports dont la divulgation est de nature à nuire à la défense et à la sécurité nationale ;
- ▶ **Secret Défense** : réservé aux informations et supports dont la divulgation est de nature à nuire gravement à la défense et à la sécurité nationale ;
- ▶ **Très Secret Défense** : réservé aux informations et supports qui concernent les priorités gouvernementales en matière de défense et de sécurité nationale et dont la divulgation est de nature à nuire très gravement à la défense et à la sécurité nationale.



2. Qui peut classifier ?

Marque de l'autorité publique, l'usage du secret est strictement réservé aux seules personnes habilitées et autorisées :

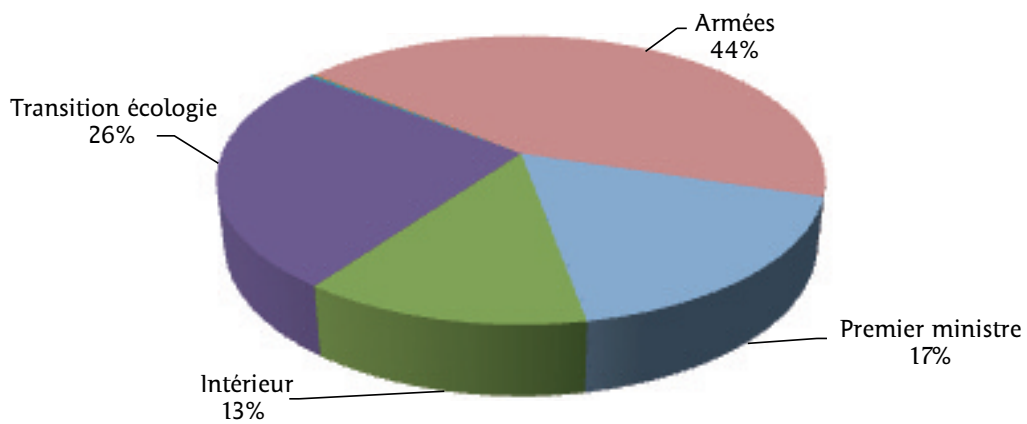
- relevant d'un ministère ou d'une entité placée sous l'autorité ou la tutelle de ce dernier ;
- agissant dans le cadre d'un contrat, conclu directement ou indirectement avec l'autorité publique ;
- relevant de la réglementation relative aux activités d'importance vitale.

Au sein de chaque ministère, la décision de classifier une information est prise, sur proposition de son auteur, au niveau hiérarchique le plus apte à évaluer les enjeux.

Ainsi, au 1^{er} janvier 2017, sur plus de 5 millions de documents classifiés dénombrés, 586 914 informations ou supports classifiés au niveau « Secret Défense » ont été recensés par les ministères. Ce chiffre tient également compte des documents transmis par nos partenaires internationaux.

Le détail de ce nombre met en lumière les ministères les plus concernés par la question du secret de la défense nationale. Différents transferts de compétences, qui sont récemment intervenus, modifient la répartition ministérielle des documents classifiés.

Volume des documents classifiés au niveau Secret Défense





3. Comment une information est-elle marquée ?

Lorsqu'un support matériel est classifié, un marquage lui est apposé, qui comporte l'identification du document ainsi qu'un timbre de classification.

Ce timbre est appelé à évoluer dans le cadre de la réforme sur le secret de la défense nationale comme indiqué ci-dessous :



Des modalités particulières de marquage sont prévues pour les supports immatériels.



L'usage frauduleux ou indu :

L'usage frauduleux du marquage de classification est passible de 3 ans d'emprisonnement et de 45 000 euros d'amende (article 444.4 du code pénal).

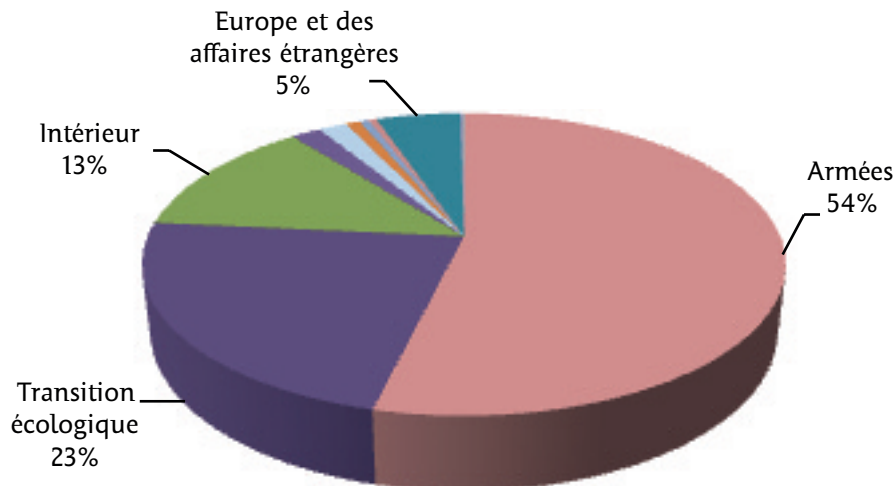
Le fait de faire indûment bénéficier de la protection attachée au secret de la défense nationale des informations ou documents non classifiés expose son auteur aux mêmes peines (en application du I de l'article 56.4 du code de procédure pénale et de l'article 434.4 du code pénal).



Annexe 3 : Comment les informations et supports classifiés sont-ils gérés ?

Les informations et supports classifiés ne peuvent par principe être entreposés ou exploités que dans des zones sécurisées déclarées en qualité de lieux abritant des éléments couverts par le secret de la défense nationale.

Répartition des lieux abritant des éléments couverts par le secret de la défense nationale par ministères



41

Au niveau *Confidentiel Défense*, il est recommandé de créer une zone protégée qui offre une protection pénale contre l'intrusion. L'ensemble des accès doit faire l'objet d'un contrôle permanent et la pénétration à l'intérieur de la zone est soumise à autorisation. Au sein d'une zone protégée, la zone réservée est obligatoire en cas de détention d'informations ou supports classifiés de niveau *Secret Défense*.



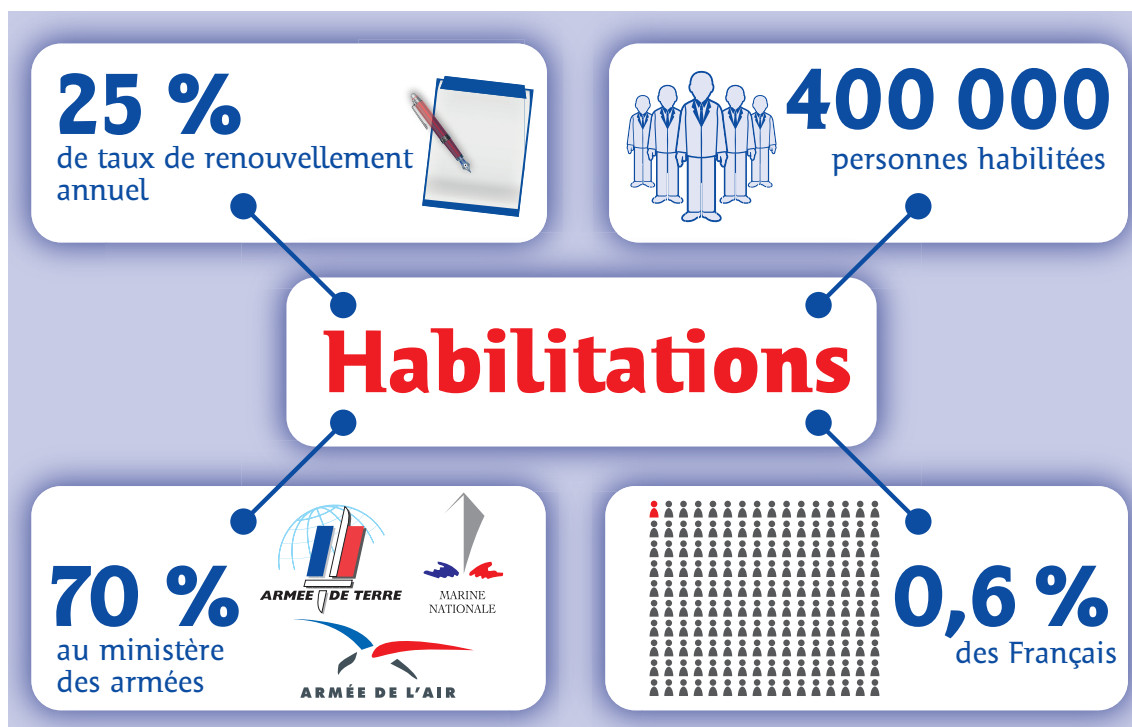


La gestion des informations et supports classifiés obéit à des règles précises destinées à assurer leur sécurité :

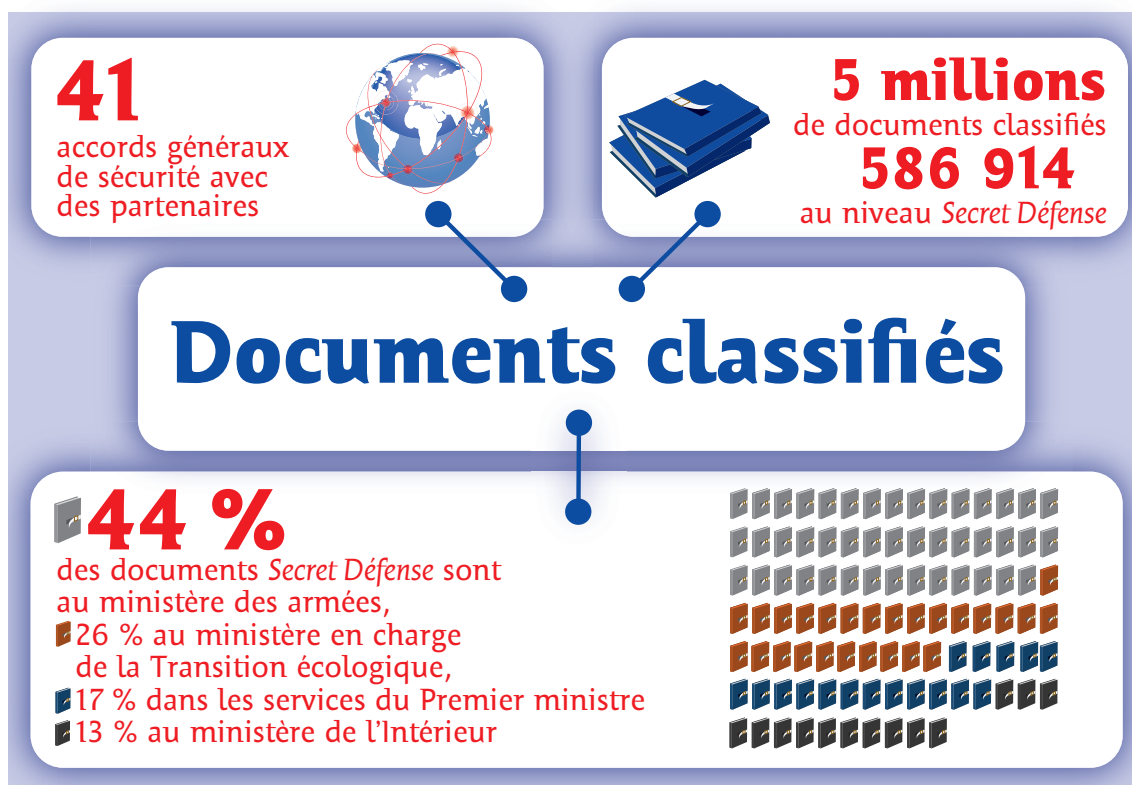
- ▶ création d'un bureau de protection du secret pour la gestion des documents de niveau « *Secret défense* », seul apte à élaborer, marquer, suivre, stocker et détruire des supports classifiés de ce niveau ;
- ▶ enregistrement obligatoire pour les documents de niveau « *Secret défense* » dans un système spécifique dont l'accès est restreint, voire classifié ;
- ▶ inventaire annuel, fortement recommandé pour les documents « *Confidentiel défense* », et obligatoire à partir du niveau « *Secret défense* » ;
- ▶ stockage sûr, dans des meubles de sécurité conformes aux normes en vigueur (coffres et armoires fortes) ou dans un système d'information homologué.



Le secret en bref



43





Glossaire

Accord de sécurité : accord intergouvernemental conclu entre au moins deux États ou au sein d'une alliance multinationale et ayant pour objet la protection d'informations ou de supports classifiés. Ces accords comprennent notamment l'identification et la reconnaissance mutuelle des autorités nationales de sécurité, la correspondance des niveaux de classification, la reconnaissance mutuelle des habilitations de personnes, les modalités de transmission et de protection des informations et supports classifiés.

Autorité nationale de sécurité (ANS) : organisme gouvernemental chargé des relations avec les autres États et les structures internationales en matière d'habilitation de personnes et de protection des informations ou supports classifiés. En France, l'autorité nationale de sécurité est le Secrétaire général de la défense et de la sécurité nationale.

Avis de sécurité : conclusion émise par un service enquêteur à l'issue d'investigations se rapportant à une personne et visant à détecter et à évaluer les vulnérabilités de cette personne. L'avis de sécurité est une aide à la décision d'habilitation, mais il ne lie pas l'autorité responsable de la décision.

Besoin d'en connaître : nécessité impérieuse de prendre connaissance d'une information dans le cadre d'une fonction déterminée, pour la bonne exécution d'une mission précise.

Catalogue des emplois : dans un organisme, liste des emplois qui peuvent nécessiter l'accès aux informations ou supports classifiés. Le catalogue est dressé sur le seul critère du besoin d'en connaître.

Compromission : prise de connaissance, certaine ou possible, d'une information ou d'un support classifié par une ou plusieurs personnes non qualifiées.

Décision d'habilitation : acte administratif autorisant, au terme de la procédure d'habilitation, le titulaire, en fonction de son besoin d'en connaître, à accéder aux informations ou aux supports classifiés d'un niveau déterminé. L'intéressé est informé de la décision d'habilitation, qui ne lui est jamais remise.

Haut fonctionnaire de défense et de sécurité (HFDS) : personne chargée d'assister le ministre dans l'exercice de ses attributions de sécurité, de défense et de protection du secret. Il est, dans certains ministères, appelé haut fonctionnaire correspondant de sécurité et de défense (HFCDS) ou haut fonctionnaire de défense (HFD).



Service enquêteur : service d'État chargé de procéder aux investigations sur les personnes préalablement à une décision d'habilitation ou dans le cadre d'un contrôle élémentaire, d'évaluer l'aptitude des locaux et de contrôler les mesures de sécurité. Ces services rendent leurs conclusions sous la forme d'avis de sécurité.

Vulnérabilité : fait relatif à la situation d'une personne et qui amoindrit les garanties qu'elle présente pour la protection des informations ou supports classifiés. Il s'agit d'une fragilité qui peut donner lieu à des pressions de diverses natures et qui doit être prise en compte pour accorder avec ou sans restriction, pour refuser ou pour retirer l'accès aux informations ou supports classifiés.



Pour aller plus loin

Dispositions juridiques

- Code pénal, notamment les articles 226-13, 413-7 à 413-12, 414-7 à 414-9, 434-4 et R. 413-1 à R. 413-5
- Code de procédure pénale, notamment l'article 56-4.
- Code de la défense, notamment les articles L. 1111-1, L. 2312-1 à L. 2312-8, R*. 1132-1 à R. 1132-3, R. 1143-1 à R. 1143-8, R. 2311-1 à D*. 2311-12, R. 2312-1 et R. 2312-2.
- Code du patrimoine, notamment ses articles L. 213-1 à L. 213-7 et R. 213-11.
- Arrêté du Premier ministre du 30 novembre 2011 portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale

Rapports publics

- Rapport sur le secret de la défense nationale en France, 2015, secrétariat général de la défense et de la sécurité nationale
- Rapport d'activité 2016, commission d'accès aux documents administratifs
- Dossier documentaire, décision n° 2011-192 QPC, Conseil constitutionnel
- Dossier documentaire, décision n° 2015-713 DC, Conseil constitutionnel

Rapport sur le secret de la défense nationale *en France* / II

Janvier 2018



51, boulevard de La Tour-Maubourg
75700 Paris SP 07
01 71 75 80 11
sgdsn.gouv.fr