PREMIÈRE
MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

GUIDE DE BONNES PRATIQUES

EN MATIERE DE COMMUNICATION, D'USAGE ET DE STOCKAGE D'INFORMATIONS, SANS MOUVEMENT D'UN SUPPORT PHYSIQUE, SUSCEPTIBLES DE RELEVER DU CONTROLE DES EXPORTATIONS DE MATERIELS DE GUERRE

(CONTROLE DIT DES « INTANGIBLES »)

SOMMAIRE

INTRODUCTION

Contexte d'élaboration du guide

Le système français de contrôle des exportations de matériels de guerre et matériels assimilés est fondé sur le principe général de prohibition, sauf autorisation de l'Etat, appelée licence d'exportation ou de transfert. Ce principe, justifié par la nature particulière du commerce des armes, est inscrit dans la loi (Partie 2, Livre III, Titre III du code de la défense).

Le transfert de certaines technologies, savoir-faire et informations peut être contrôlé au même titre que les matériels physiques : une licence d'exportation ou de transfert est alors nécessaire avant de pouvoir les exporter ou transférer, au sens du code de la défense et ce, quel qu'en soit le support. Il peut s'agir, par exemple, d'informations communiquées dans le cadre d'un prospect et qui seraient de nature à permettre ou à faciliter la fabrication ou la reproduction de matériels de guerre et matériels assimilés ou à compromettre leur efficacité. La pratique professionnelle, inspirée de la terminologie anglaise, désigne parfois cette thématique comme celle des « intangibles » ou des transferts « par voie [d']intangible ».

Ces types particuliers de flux peuvent soulever différentes questions d'application des règles en matière de contrôle des exportations de matériels de guerre, *a fortiori* dans un contexte où leur volume va croissant, en particulier s'agissant de l'absence de passage en douanes, de l'appréhension plus délicate de la notion même de franchissement de frontière ou encore, des difficultés liées à la localisation physique (par exemple : serveurs) des données elles-mêmes. De même, la forme numérique des transferts est multiple et regroupe un panel de moyens très étendus et diversifiés qui peuvent ne pas être toujours visibles par les personnes qui les utilisent au quotidien (réseaux, notamment).

Objectifs poursuivis

Dans ce contexte, le présent guide se présente comme un cadre d'interprétation partagé à l'intention des exportateurs d'informations, de nature à réduire les incertitudes et les risques de manquement. Il vise en particulier à éclairer :

- les situations dans lesquelles une licence de transfert ou d'exportation est requise et de préciser les implications de ce contrôle à l'attention de l'ensemble des opérateurs économiques amenés à produire, détenir ou manipuler ce type d'informations ;

- les conditions que la commission interministérielle pour l'étude des exportations de matériels de guerre (CIEEMG) peut imposer au stade de l'octroi de la licence, par exemple, le plan d'assurance de sécurité des informations ;

- les mesures de contrôle interne que l'administration peut être amenée à prescrire dans le cadre du contrôle *a posteriori*.

Périmètre et articulation avec des régimes connexes

Ce document regroupe des recommandations méthodologiques et de bonnes pratiques liées au seul contrôle des exportations depuis le territoire national.

Il ne traite pas de l'importation ni de la réexportation d'informations soumises à des exigences issues de règlementations de contrôle étrangères.

Il n'a pas non plus vocation à prévenir la compromission d'informations couvertes par le secret de la défense nationale (PSDN) ou de la sécurité des activités d'importance vitale (SAIV), ou les manquements à d'autres secrets ou régimes restrictifs (par exemple, les mentions « diffusion restreinte » et « spécial France », ou encore la protection du potentiel scientifique et technique de la Nation (PPST), au respect d'accords intergouvernementaux spécifiques limitant aux seuls ressortissants du pays de destination la transmission d'informations protégées) ni à se substituer aux réglementations relatives à la protection des systèmes d'informations sensibles[1].

En ce qui concerne les transferts et exportations par voie numérique, les recommandations formulées dans le présent guide s'appuient autant que possible sur les instructions ou guides existants de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) dont les références sont rappelées. Les exportateurs appliquant d'ores et déjà ces guides pourront donc utilement s'appuyer sur les outils et procédures déjà en vigueur sur ces questions.

Les recommandations organisationnelles et techniques formulées dans ce guide n'ont pas pour objectif de protéger les exportateurs contre des tentatives frauduleuses d'accès à leurs données numériques, même si elles peuvent y contribuer. Cette problématique, qui dépasse le seul contrôle des exportations et concerne en réalité l'ensemble des données numériques de l'entreprise, relève de sa politique de sécurité des systèmes d'information, qui a vocation à s'appuyer sur les instructions et documents édités par l'ANSSI.

Caractère non contraignant

Le présent guide ne revêt aucun caractère contraignant et ne crée pas d'obligation juridique pour ceux auxquels il s'adresse. Ses recommandations ne sauraient se substituer aux exigences légales et réglementaires issues, en particulier, du code de la défense.

Chaque exportateur a vocation à adopter les moyens qu'il juge pertinents pour se conformer à la réglementation, en fonction de son organisation, de ses spécificités (par exemple : taille d'entreprise, volume et format des informations manipulées) et des risques identifiés dans son activité, notamment au regard des technologies qu'il utilise.

Actualisation

Un retour d'expérience d'ici 18 mois permettra une mise à jour du présent guide, au regard des éventuelles difficultés rencontrées ou bonnes pratiques complémentaires identifiées.

[1] Ce guide prend en compte le principe d'indépendance des législations qui sera rappelé dans les cas d'études détaillés dans le présent guide.

PARTIE 1

-

DANS QUELS CAS LE CONTRÔLE DES EXPORTATIONS DE MATÉRIELS DE GUERRE A-T-IL VOCATION À S'APPLIQUER ?

1.1. Critères généraux

Les opérations concernées sont, pour l'essentiel, celles qui relèveraient du régime de contrôle des exportations (ou « transferts », au sein de l'espace européen[2]) de matériels de guerre et matériels assimilés[3], si elles donnaient lieu à un transfert physique d'un support matériel (comme l'envoi d'une documentation papier, d'un disque dur externe ou d'une clé USB) au destinataire final.

1.1.1. Conditions tenant aux informations

→ L'information doit être classée au titre des matériels de guerre et matériels assimilés

L'information doit ainsi relever de l'une des catégories suivantes :

- technologies de la catégorie ML 22 figurant dans l'annexe de l'arrêté du 27 juin 2012 modifié relatif à la liste des matériels de guerre et matériels assimilés soumis à une autorisation préalable d'exportation et des produits liés à la défense soumis à une autorisation préalable de transfert ;

- technologies et formations figurant en deuxième partie de l'annexe du même arrêté, ainsi que les connaissances mentionnées au I de l'article L. 2335-18 du code de la défense ;

- informations, mentionnées aux 1° du I des articles R. 2335-9 et R. 2335-21 du code de la défense, de nature à permettre ou à faciliter la fabrication ou la reproduction de tout matériel de guerre ou matériel assimilé sous régime de contrôle, ou à en compromettre l'efficacité ;

- présentations, essais, documentations, études, résultats d'étude, résultats d'essai (à l'exception des prototypes) et technologies de conception ou de fabrication de matériels de guerre ou produits liés à la défense mentionnés aux 2°, 3° et 4° du I des articles R. 2335-9 et R. 2335-21 du code de la défense.

Il convient dans chaque cas de s'assurer du classement des informations concernées, en s'appuyant notamment sur le guide de classement édité par la DGA. **Les recommandations du présent guide ne sont applicables qu'aux informations classées comme matériels de guerre et matériels assimilés.**

→ L'information ne doit pas avoir subi un traitement emportant la levée du contrôle

L'anonymisation des informations désigne un procédé consistant à supprimer, dans un fichier ou document, toute information contrôlée, sans qu'il soit possible pour son destinataire de les reconstituer. Dans ce cas, le contenu n'est plus contrôlé.

Le chiffrement n'empêche pas quant à la lui la reconstitution. Il n'exonère pas du besoin de licence d'exportation. Il reste néanmoins très opportun en lui-même. Ainsi, même lorsque le niveau de confidentialité des informations concernées n'oblige pas juridiquement à un tel chiffrement, il est fortement recommandé pour limiter les risques d'exportation non autorisée.

[2] Par souci de simplification, le terme « exportation » désignera dans ce guide aussi bien les exportations, au sens de l'article L. 2335-2 du code de la défense, que les transferts au sens de l'article L. 2335-9 du même code, dans la mesure où les recommandations formulées s'appliquent indifféremment aux échanges hors ou au sein de l'Union européenne.
[3] Arrêté du 27 juin 2012 relatif à la liste des matériels de guerre et matériels assimilés soumis à une autorisation préalable d'exportation et des produits liés à la défense soumis à une autorisation préalable de transfert.

1.1.2. Conditions tenant au flux

→ Flux ne donnant pas lieu à un mouvement de support physique

Les informations recouvrent deux formes principales de communication :

- des échanges oraux, par exemple : conversation, présentation orale, formation ;

- des échanges numériques, par exemple : l'envoi de messages électroniques, le stockage sur certains serveurs et l'informatique en nuage.

→ Flux volontaire ou involontaire

La fourniture volontaire d'accès à des informations contrôlées a pour objet même la consultation et/ou le téléchargement par un destinataire final et peut, le plus souvent, être tracée. Elle nécessite une licence d'exportation vers ce destinataire si l'exportation *via* un support physique de ces mêmes informations vers cette même personne aurait nécessité une licence.

La fourniture involontaire d'accès relève de situations qui, sans induire automatiquement une exportation d'informations contrôlées, donnent néanmoins la possibilité à un tiers non autorisé d'en prendre connaissance (lecture, captation orale, visualisation/capture de données, mise à disposition sur un serveur), souvent plus difficiles à tracer. Elle expose l'entité ayant involontairement fourni l'accès au risque d'exportation non autorisée.

1.2. Eléments d'appréciation concernant le franchissement de la frontière

1.2.1. Cas généraux

La notion de frontière, qui soulève peu de questions dans le cas de biens physiques, est plus complexe à appréhender dans le cadre d'un flux d'information.

→ Nécessité d'une prise en compte globale de la qualité du destinataire

Une exportation est réalisée lorsqu'il y a transmission, par quelque moyen que ce soit, d'une information contrôlée à un destinataire situé hors du territoire douanier national[4], qu'il s'agisse d'une personne physique ou morale, et indépendamment de sa nationalité.

Mais certaines opérations consistant à présenter ou à transmettre, sur le territoire douanier national, des informations contrôlées à un tiers constituent également une exportation ou un transfert au sens du code de la défense, même en l'absence de franchissement de frontières, en fonction de la qualité du tiers auquel cette information est présentée ou transférée.

Dans cette hypothèse, il peut en particulier être tenu compte des éléments d'appréciation suivants qui, sans être exhaustifs, impliqueront en général un besoin de licence sauf exception[5] :

- tiers employé par une entité non établie en France, et qui n'est donc ni une personne morale de droit français, ni un établissement régulièrement immatriculé au RCS ;

- particulier (et non un salarié d'une personne morale), s'il est un étranger temporairement présent sur le territoire douanier national ou un Français résident permanent dans un pays étranger.

[4] En matière d'exportation de matériels de guerres, les dispositions applicables en métropole s'appliquent également aux exportations depuis l'outre-mer et la principauté de Monaco.
[5] De telles exceptions existent notamment dans le cadre de dérogations (par exemple : certains programmes en coopération, régime douanier du perfectionnement actif).

→ *Limites du seul critère de la nationalité du destinataire (physique ou moral)*

Dans les cas les plus fréquents où le destinataire est une personne morale, la notion de nationalité de l'employé du destinataire à qui sera adressé une information n'est pas un critère pertinent pour déterminer si la transmission d'une telle information est soumise à licence.

De même, la nationalité de la maison mère d'une filiale établie en France ne permet pas de déterminer si une licence est requise. En effet, le code de la défense ne mobilise pas ce critère pour caractériser les destinataires vers lesquels une exportation est soumise à licence[6].

	Thème	Cas d'étude	Besoin en licence	Eléments de réponse complémentaires
N1.	**Nationalité des salariés** d'une entreprise établie en France	Salarié étranger	Aucune licence n'est requise pour un salarié du seul fait de sa ou de ses nationalités.	Il convient de prendre en compte le contrat de travail, plus particulièrement la notion de lien de subordination pour déterminer la qualité de salarié[7]. La transmission peut toutefois faire l'objet de restrictions particulières, au titre d'autres réglementations (ex. : PSDN, PPST…).
N2.		Salarié binational		
N3.	**Statut des personnels non-salariés** d'une entreprise établie en France	Stagiaire/ doctorant dépendant d'une université étrangère	Une licence est requise pour l'accès car l'établissement de rattachement est étranger.	Le stagiaire est «placé sous l'autorité fonctionnelle de l'entreprise d'accueil»[8] mais il reste rattaché à son établissement d'enseignement.
N4.		Doctorant étranger dépendant d'une université ou une entreprise française	Aucune licence n'est requise s'il existe un lien de subordination entre le doctorant et l'université ou l'entreprise française. Une licence est, en revanche, requise, si le doctorant, bien qu'effectuant sa thèse en France, ne dispose pas d'un contrat de travail (ex. : boursier d'un gouvernement étranger).	Il existe toutefois plusieurs statuts de doctorants : (1) étudiant salarié de droit public (contrat doctoral, rattaché à une université) ou étudiant salarié de droit privé (rattaché à une entreprise) ; (2) étudiants boursiers (d'un gouvernement étranger, par exemple). Le cas (2) nécessite une licence.
N5.		Transfert par un industriel français de données à un laboratoire de recherche étranger ou une université étrangère	Une licence est requise pour l'accès car l'établissement est étranger.	
N6.	Statut des personnels non-salariés d'une entreprise **non établie en France**	Intérimaire étranger dépendant d'une société d'intérim étrangère	Une licence est requise.	
N7.		Prestataires extérieurs étrangers	Une licence est requise.	

[6] Le code de la défense fait référence aux «destinataires situés», respectivement, dans un Etat non-membre de l'Union européenne ou dans un autre Etat-membre de l'Union européenne.

[7] La notion de «lien de subordination» a été définie par la jurisprudence de la Cour de cassation : «Le lien de subordination est caractérisé par l'exécution d'un travail sous l'autorité de l'employeur qui a le pouvoir de donner des ordres et des directives, d'en contrôler l'exécution et de sanctionner les manquements de son subordonné. Le travail au sein d'un service organisé peut constituer un indice du lien de subordination lorsque l'employeur détermine unilatéralement les conditions d'exécution du travail» (Cass. soc., 13 novembre 1996).

[8] La référence au «lien de subordination» renvoie à une réalité précise en droit du travail, qui correspond exclusivement au rapport salarial. Le lien de subordination permet de déduire qu'il y a relation salariale (voir à propos des services type Uber Eat Cass.Soc. 28 nov.2018, n° 17 - 20. 079). Sont exclus les stagiaires qui sont seulement «sous l'autorité fonctionnelle de l'entreprise d'accueil» (Cass.Soc.4 oct2007, n° 06 -44 .106).

1.2.2. Cas particulier des échanges avec des organismes étrangers (OTAN, ambassades, relations interétatiques, coopérations industrielles)

	Thème	Cas d'étude	Besoin en licence	Eléments de réponse complémentaires
N8.	Echanges dans le cadre de **coopérations européennes ou interalliées**	*Exemple 1 : dans le cadre de coopérations industrielles ou intergouvernementales* *Exemple 2 : dans le cadre OTAN : (i) coopération internationale / groupe de travail ; (ii) exercices OTAN ; (iii) forums OTAN ou AED (rapports techniques, présentations PowerPoint, mails, échanges oraux en réunion)* *Exemple 3 : dans le cadre de l'ESA*	Une licence est requise pour la transmission d'informations contrôlées.	Possibilité de recourir à des dérogations au titre de programmes en coopération
N9.	Echanges *via* **ambassades**	A l'étranger *Exemple : Envoi d'informations contrôlées à des organismes institutionnels étrangers en France (ambassade étrangère)*	Une licence est requise.	
N10.		*Via* le réseau diplomatique français *Exemple : Envoi d'informations contrôlées à une ambassade de France à l'étranger de manière sécurisée (ACID) pour une présentation à un tiers étranger*	Une licence est requise pour une présentation à un tiers étranger.	L'usage d'une clé ACID n'exonère pas du besoin de licence. Il permet simplement d'acheminer des informations protégées jusqu'au niveau « diffusion restreinte -Spécial France ».

1.3. Les particularismes liés aux procédés utilisés

1.3.1. Accès visuel ou auditif à l'information : démonstrations, présentations, séminaires, salons, visio/audioconférences

	Thème	Cas d'étude	Besoin en licence	Eléments de réponse complémentaires
N11.	Présentations verbales et démonstrations **en France (à une entité étrangère) ou à l'étranger**	Par un salarié de l'exportateur à un représentant d'une entité étrangère *Ex. 1 : à un représentant d'une société étrangère* via *un plateau d'étude commun* *Ex. 2 : à destination du monde académique/ de la recherche : séminaires, colloques* *Ex. 3: déplacement professionnel* *Ex. 4: à un Français résidant à l'étranger*	Une licence est requise car le destinataire n'est pas une société établie en France.	
N12.		Par un Français non-salarié de l'exportateur (ex. : sous-traitant) à des représentants d'une société étrangère		
N13.	**Visites de sites en France**	De délégations étrangères	Une licence est requise si la visite inclut la transmission d'informations contrôlées.	
N14.	**Téléconférences, tété-démonstrations, télé-présentations internationales**	Présentations verbales et démonstrations à une entité étrangère en France ou à l'étranger	Une licence est requise.	

1.3.2. Hébergement et accès sur des serveurs (en France et à l'étranger)

Le lieu d'hébergement de l'information contrôlée peut emporter une exportation si un franchissement de frontière est constaté. L'hébergement de ce type d'information sur un sol étranger nécessite ainsi en principe une licence d'exportation.

L'hébergement doit toutefois être distingué du simple transit qui ne nécessite pas de licence d'exportation. Le stockage momentané de données dans les mémoires tampons d'équipements (par exemple : les routeurs) de réseaux informatiques relève du transit.

Thème		Cas d'étude	Besoin en licence	Eléments de réponse complémentaires
N15.	**Hébergement** d'informations contrôlées **à l'étranger**	Par une entreprise établie en France *Exemple : Stockage d'informations contrôlées sur un serveur localisé à l'étranger*	Une licence est requise pour envoyer des informations contrôlées vers le site d'hébergement à l'étranger. Le lieu d'hébergement détermine une exportation, si un franchissement de frontière est constaté.	Si le chiffrement est fortement recommandé, il n'exonère cependant pas du besoin de licence d'exportation. L'anonymisation qui consiste à supprimer, dans un fichier ou document, toute information contrôlée, peut exonérer le besoin en licence d'exportation. *In fine*, le contenu n'est plus contrôlé. Elle peut éventuellement permettre l'intervention d'une société étrangère d'infogérance (toute information contrôlée étant *in fine* supprimée du fichier ou document). Dans le cas du nomadisme, il convient de respecter des mesures d'hygiène informatique, en s'appuyant notamment sur les guides de l'ANSSI. La revue des technologies proposée à la 3ème partie vise à donner un éclairage, non exhaustif, des référentiels pertinents en la matière.
N16.	**Accès à partir de la France ou de l'étranger** à des informations contrôlées hébergées sur un serveur localisé **à l'étranger**	Par un salarié (étranger ou français) d'une société étrangère *Exemple : Accès par une société étrangère d'infogérance informatique à des informations contrôlées de son client qui sont hébergées sur un serveur à l'étranger*	Si cet accès n'était pas envisagé au moment de l'exportation pour hébergement à l'étranger, une demande de levée de certificat de non-réexportation est requise. Ainsi, l'accès par une société étrangère doit autant que possible avoir été prévu lors de la demande de licence initiale.	
N17.		Par un salarié d'une entreprise établie en France *Exemple 1 : Accès par une entreprise d'infogérance informatique établie en France à des informations contrôlées de son client qui sont hébergées sur un serveur à l'étranger* *Exemple 2 : Accès par un salarié français ou étranger d'une entreprise établie en France mais accédant aux données, hébergées sur un serveur étranger, de son entreprise depuis l'étranger*	Aucune licence n'est requise pour l'accès car l'établissement de rattachement est l'entreprise établie en France.	
N18.		Par un salarié (étranger ou français) d'une société étrangère *Exemple 1: Accès par une société étrangère d'infogérance informatique à des informations contrôlées de son client qui sont hébergées sur un serveur en France.* *Exemple 2 : Mise à disposition d'information contrôlée à un stagiaire / thésard étranger dépendant d'une université étrangère*	Une licence est requise pour l'accès car l'établissement de rattachement est étranger (société ou université).	

N19.	**Accès à partir de la France ou de l'étranger** à des informations contrôlées hébergées sur un serveur localisé **en France**	Par un salarié (étranger ou français) d'une entreprise établie en France *Ex. 1: Accès par une entreprise d'infogérance établie en France à des informations contrôlées de son client qui sont hébergées sur un serveur en France* *Ex. 2 : Mise à disposition d'information contrôlée à un thésard étranger dépendant d'une université Française* *Ex. 3 : Accès à des données, hébergées sur un serveur en France de son entreprise depuis l'étranger* *Ex. 4 : Accès* via *un accès VPN proposé par une société étrangère* *Ex. 5: Accès lors de travail à distance (télétravail, par exemple)*	Aucune licence n'est requise pour l'accès, si l'accès est réalisé depuis la France. En revanche, l'accès depuis l'étranger peut nécessiter une licence d'exportation, s'il se traduit par un enregistrement de l'information contrôlée sur un support physique situé à l'étranger.	
N20.		Par la gestion de droits d'accès	Une licence peut être requise si l'accès distant à des informations contrôlées se traduit en pratique par un enregistrement de l'information contrôlée sur un support physique situé à l'étranger.	La mise en place d'une politique de gestion de droits d'accès peut être requise selon le niveau de sensibilité ou de confidentialité des informations manipulées. Cette ségrégation des informations constitue une mesure nécessaire de prévention des risques, mais n'exonère pas du besoin en licence.
N21.		Par l'anonymisation du document[9]	Aucune licence n'est requise, puisqu'aucune information contrôlée n'est transmise.	
N22.		Par le chiffrement	Une licence peut être requise si l'exploitation des informations contrôlées se traduit en pratique par un enregistrement de l'information contrôlée sur un support physique situé à l'étranger.	
N23.	**Sauvegarde** d'informations contrôlées	Stockage d'information contrôlée sur un serveur en France mais pour lequel une sauvegarde est réalisée à l'étranger	Une licence est requise pour la sauvegarde d'informations contrôlées à l'étranger au même titre que l'hébergement de ces informations à l'étranger.	
N24.	***Cloud***	Stockage sur un *cloud*	Aucune licence n'est requise, si le *cloud* est hébergé en France. En revanche, une licence est requise si le *cloud* est hébergé à l'étranger.	Le recours à une solution *Cloud* doit être le fruit d'une analyse de risques approfondie intégrant, entre autres, la nationalité du fournisseur de *Cloud* et des sociétés qui opèrent des services en sous-traitance, les mesures d'hygiène informatique pour maitriser les accès potentiels, la nature des destinataires ayant accès aux informations hébergées sur le *Cloud*. La revue des technologies proposée en 3ème partie vise à accompagner les entreprises dans leur choix d'outils, en matière d'hygiène informatique (certification SecNum Cloud, notamment).

[9] L'anonymisation des informations, au sens de la définition donnée dans le présent guide, peut éventuellement permettre l'intervention d'une société étrangère d'infogérance, toute information contrôlée étant *in fine* supprimée du fichier ou document.

1.3.3. Messageries électroniques

	Thème	Cas d'étude	Besoin en licence	Eléments de réponse complémentaires
N25.	Envoi d'un message électronique et **nationalité du destinataire**	Nationalité du destinataire *Exemple 1 : Personne physique* *Exemple 2 : Personne morale*	Une licence est requise si le serveur de messagerie de l'expéditeur est situé à l'étranger (analogue au cas N15). Lorsque ce serveur est situé en France (cas le plus fréquent *a priori*), une licence est requise si le message vise à acheminer des informations contrôlées vers un destinataire dont la qualité implique une exportation ou un transfert. *Exemple : client étranger, quelle que soit sa localisation au moment de l'envoi.*	Concernant les salariés étrangers de personnes morales établies en France, l'envoi peut toutefois faire l'objet de restrictions issues d'autres réglementations (ex. : PSDN) ou d'accords de sécurité.

1.3.4. Plateformes d'échange, outils collaboratifs, opérations à distance et partages d'écran

	Thème	Cas d'étude	Besoin en licence	Eléments de réponse complémentaires
N26.	Transfert d'information contrôlée **par une plateforme numérique**	Echange d'informations contrôlées au travers d'un document mis à disposition dans une communauté de partage au sein d'une plateforme numérique de gestion documentaire *Exemple 1 : Plateforme en France utilisée par des exportateurs français* *Exemple 2 : Plateforme à l'étranger utilisée par des exportateurs français*	Une licence est requise si l'accès se traduit en pratique par un enregistrement des informations contrôlées sur un support physique situé à l'étranger. Tel sera le cas dans l'exemple 2 qui se rapproche des cas N15 ou N24.	Le recours à une solution de plateforme numérique doit être le fruit d'une analyse de risques approfondie intégrant, entre autres, la nationalité du fournisseur et des sociétés qui opèrent des services en sous-traitance, les mesures d'hygiène informatique pour maitriser les accès potentiels, la nature des destinataires ayant accès aux informations hébergées sur la plateforme numérique, la localisation des serveurs de stockage. La revue des technologies proposée en 3ème partie vise à accompagner les entreprises dans leur choix d'outils, en matière d'hygiène informatique (certification SecNum Cloud, notamment)
N27.	Accès à des informations contrôlées *via* **des opérations transfrontalières exécutées à distance**	Opération de maintenance effectuée à l'étranger grâce à un accès distant à des informations contrôlées hébergées en France	Une licence d'exportation est requise pour réaliser la prestation de maintien en condition opérationnelle.	La télé-opération est une exportation d'assistance technique au sens de la ML 22. Elle doit être couverte par la licence relative à l'opération d'exportation concernée qui précisera que la documentation et l'assistance peuvent être fournies par voie tangible et/ou intangible.
N28.	Transfert d'information contrôlée **par visioconférence, téléconférence, télé-démonstrations, télé-présentations-internationales**	Partage d'une information contrôlée par visio-conférence avec une société étrangère	Une licence est requise.	L'infrastructure du système est une source de risques supplémentaires.
N29.	Transfert d'information contrôlée *via* **le partage d'écran d'un ordinateur situé en France**	Ordinateur localisé en France affichant une information contrôlée au profit d'utilisateurs étrangers localisés à l'étranger et relevant de sociétés étrangères	Une licence est requise.	
N30.		Ordinateur localisé en France affichant une information contrôlée au profit d'utilisateurs français ou étranger localisés à l'étranger et relevant d'une entreprise établie en France	Aucune licence n'est requise car l'établissement de rattachement est l'entreprise établie en France.	
N31.		Ordinateur localisé en France affichant une information contrôlée au profit d'utilisateurs français ou étrangers localisés en France et relevant de sociétés étrangères	Une licence est requise.	

PARTIE 2

-

COMMENT ORGANISER LA GESTION DES RISQUES EN CE DOMAINE ?

Compte tenu des risques que la communication, l'usage et le stockage d'informations relève du contrôle des exportations de matériels de guerre, il est utile, dans tous les cas, que les exportateurs élaborent une politique de prévention des risques (2.1).

Dans certains cas particuliers, un tel dispositif pourra être imposé dans le cadre des procédures de contrôle *a priori* ou *a posteriori* (2.2).

2.1. L'élaboration d'une politique de prévention des risques à l'initiative de l'exportateur

Les exportateurs sont invités à élaborer une politique de prévention des risques (2.1.1) qui peut prendre la forme d'un plan d'amélioration continue de la sécurité (2.1.2) soutenu dans l'un et l'autre cas par un « engagement de la direction ».

2.1.1. Fond de la démarche

→ Adaptation de la politique à chaque situation

Le contenu de la politique de protection ainsi que ses modalités d'application relèvent de chaque exportateur, selon son appréciation des risques et en fonction de la nature de ses activités et des spécificités de son organisation (taille, structure, type de systèmes d'information). A cette fin, les pratiques recommandées et documents de référence mentionnés dans le présent guide (*cf.* Partie 1), sont susceptibles de garantir aux exportateurs la qualité minimale de leur dispositif.

En outre, l'efficacité du dispositif repose sur son appropriation par l'ensemble des acteurs concernés qui devront donc être sensibilisés aux enjeux et risques propres aux informations concernées, dans l'objectif de diffuser et de faire progresser les bonnes pratiques mais aussi le retour d'expérience.

→ Responsabilité et gouvernance internes

L'exportateur est encouragé à identifier un ou des responsables de la politique de prévention et de protection des informations, à définir ses missions et à affecter les ressources nécessaires à leur exercice.

Il est fortement recommandé que la politique de prévention et de protection soit endossée par l'exportateur au moyen d'un « engagement de la direction ». Sa signature par une personne ayant le pouvoir d'engager l'exportateur atteste ainsi de sa prise de connaissance des dispositions légales et des présentes recommandations.

L'exportateur aura tout intérêt par ailleurs à définir l'ensemble des chaînes de responsabilité, notamment les responsabilités contractuelles des acteurs extérieurs avec lesquels il interagit dans le cadre de la gestion et de l'exportation des informations concernées. Ces acteurs extérieurs sont notamment les prestataires informatiques, fournisseurs de services de *cloud* et d'infogérance, pouvant être amenés à manipuler ces informations. Il peut s'agir également de personnels sans lien de subordination avec l'exportateur.

→ Gestion de la relation avec les acteurs externes

Il y a lieu de s'assurer que tout acteur extérieur qui est (ou peut potentiellement être) en contact avec les informations concernées, applique des règles au moins équivalentes à celles mises en œuvre par l'exportateur lui-même, dont le prestataire extérieur a pris connaissance et qu'il a acceptées explicitement.

Cette acceptation peut prendre la forme d'un engagement explicite de l'acteur extérieur, que l'exportateur conserve et peut tenir à disposition des autorités de contrôle *a posteriori* qui peuvent en tenir compte pour l'évaluation des responsabilités en cas de manquement à la réglementation en vigueur en matière de contrôle des exportations.

Plus généralement, il est utile que l'exportateur rassemble et soit à même de présenter à l'administration, si nécessaire, l'ensemble des mesures prises (par exemple : dispositions

contractuelles, accords de non divulgation) pour assurer que le niveau d'exigence qu'il s'est lui-même fixé ne soit pas dégradé lorsqu'il fait appel à des intervenants extérieurs.

2.1.2. Format de la démarche : documents préexistants ou « plan d'amélioration continue de la sécurité » (PACS) spécifique

Il appartient à chaque exportateur de définir le format qu'il jugera le plus approprié à son organisation. Ainsi, un exportateur disposant déjà d'un plan d'amélioration continue de la sécurité ou document analogue, dans le cadre de sa politique de gestion des risques et/ou ses pratiques de sécurité des systèmes d'information, pourra préférer amender un document existant plutôt que d'en créer un nouveau consacré aux seules informations susceptibles de relever du contrôle des exportations de matériel de guerre.

Lorsque le choix est fait d'élaborer un PACS spécifique, il a vocation à intégrer les éléments suivants :

→ *Appréciation des risques*

L'appréciation des risques vise l'identification des menaces et des vulnérabilités, l'analyse et l'évaluation du niveau de criticité des risques, en fonction de leur probabilité de réalisation et de leur niveau de gravité en cas de survenance. Les présentes recommandations précisent les risques principaux qui doivent être pris en compte par les exportateurs lorsqu'ils réalisent leur cartographie des risques. Cette appréciation par les exportateurs a vocation à englober aussi l'exposition aux risques inhérents aux relations avec des acteurs extérieurs et à être mise à jour régulièrement pour permettre l'amélioration continue de la mise en œuvre du PACS.

Pour cette phase d'analyse, les exportateurs pourront notamment s'appuyer sur la méthode EBIOS Risk Manager[10], éprouvée par l'ANSSI dans le domaine des risques numériques.

→ *Priorisation des risques à traiter*

Elle a vocation à reposer sur l'analyse du contexte de chaque exportateur et en particulier :

- les particularités d'infrastructure des sites industriels ou fonctionnels ;
- leur localisation, tout particulièrement pour les sites étrangers ;
- les principaux acteurs internes de l'entreprise impliqués et des organisations et dispositifs existants (pour assurer la sécurité des SI ou la PPST, par exemple) ;
- les principaux acteurs extérieurs à l'entreprise (infogérants, intermédiaires, sous-traitants impliqués, etc.).

Il s'agit de déterminer, sur la base de la cartographie réalisée, les niveaux de risque acceptables au regard de seuils limites afin d'identifier les risques pour lesquels un dépassement des seuils nécessite de mettre en place des mesures de réduction. Cette démarche permet de documenter les risques qui sont propres aux informations contrôlées et aux technologies de l'information (*cf.* Partie 3).

→ *Définition des mesures préventives*

Il s'agit de définir les mesures adéquates pour réduire la probabilité de réalisation des risques et la gravité des conséquences de cette réalisation.

A cet effet, il est possible d'exploiter les résultats de l'analyse de risque de manière échelonnée dans le temps, dans une démarche d'amélioration continue, en fonction des moyens et des contraintes (temps, budget, complexité). En pratique, l'ensemble des mesures de traitement est documenté en associant à chaque mesure le responsable, les principaux freins et difficultés de mise en œuvre, le coût et l'échéance.

[10] https://www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager/.

La mise en œuvre du PACS permet ainsi de réduire graduellement (par exemple tous les trimestres) les risques, jusqu'à atteindre les objectifs que l'exportateur s'est fixés.

→ Gestion des incidents et de la gestion de crise

Il s'agit de décrire et de mettre en place les procédures à suivre en cas de survenance d'un incident afin d'en limiter les conséquences.

En pratique, cela peut se traduire par des fiches reflexes qui sont actualisées et améliorées en fonction du retour d'expérience procuré par le traitement des incidents déjà rencontrés. Une de ces mesures de précaution peut consister à informer sans délai la DGA de tout incident identifié.

→ Suivi et mise à jour du plan

Ce suivi vise en particulier à :

- contrôler régulièrement l'efficacité des mesures mises en place pour réduire les risques dans le cadre du PACS afin, le cas échéant, d'adopter des mesures correctives ;

- mettre à jour le PACS lorsque de nouveaux risques sont identifiés (boucle itérative).

L'exportateur est invité à évaluer en permanence le niveau de sécurité des systèmes d'information et à suivre l'évolution des risques dans le temps. L'exportateur peut apprécier ainsi les événements liés à la sécurité de l'information et décider s'il y a lieu d'en qualifier certains en incident de sécurité. En cas de doute, l'exportateur peut utilement solliciter l'expertise technique des prestataires qualifiés de l'ANSSI[11]. Lorsqu'un incident de sécurité est avéré, il est vivement recommandé d'informer, sans délai, la DGA.

L'exportateur gagnera à effectuer régulièrement des vérifications et à réaliser des audits fonctionnels et techniques de sécurité des systèmes d'information. Cette évaluation permet, en effet, de réduire l'impact des incidents éventuels.

Les exportateurs sont invités à tenir à la disposition de l'administration leurs PACS et engagements de direction.

→ Sensibilisation de l'ensemble des acteurs

L'efficacité du PACS repose notamment sur son appropriation par l'ensemble des acteurs chargés de sa mise en œuvre, au travers par exemple de l'organisation régulière de formations et/ou séances de sensibilisation. Ces démarchent concourent au développement d'une culture de la sécurité dans l'entreprise.

2.2. Les exigences susceptibles de s'imposer dans le cadre du contrôle *a priori* ou *a posteriori*

2.2.1. Au stade du contrôle *a priori*

Dans le cadre du processus d'instruction des demandes de licence d'exportation, la CIEEMG peut considérer que le dispositif existant est insuffisant pour garantir le contrôle des informations contrôlées, ou qu'une opération implique des modalités d'échanges de données techniques qui appellent une vigilance particulière.

La CIEEMG précise alors, au cas par cas, sous forme de conditions, les mesures indispensables pour préserver les informations concernées de toute exportation non autorisée.

Les mesures complémentaires requises par la CIEEMG peuvent ainsi prendre la forme d'un plan d'assurance de sécurité des informations (PASI) spécifiquement adapté à l'opération dont il s'agit et exigé au titre des conditions de la licence d'exportation. La DGA définit les modèles qui servent de base aux exportateurs pour la rédaction spécifique de chacun de leur PASI. La DGA analyse et approuve les PASI dont la mise en œuvre est contrôlée dans le cadre du contrôle *a posteriori.*

[11] https://www.ssi.gouv.fr/entreprise/qualifications/prestataires-de-services-de-confiance-qualifies/.

2.2.2. Au stade du contrôle *a posteriori*

Dans le cadre de leur contrôle, la DGA et le comité ministériel du contrôle *a posteriori* (CMCAP) peuvent demander aux exportateurs qu'ils fournissent la description de leur dispositif de gestion des informations concernées, ce qui peut inclure :

- l'engagement de la direction ;
- le PACS, ou autre document formalisant de manière synthétique la politique de prévention et de protection pour les informations contrôlées intangibles ;
- et plus généralement, tout document relatif à la mise en place de la politique de prévention et de protection des informations contrôlées intangibles.

En application de l'article L. 2339-1-2 du code de la défense, le président du CMCAP peut mettre en demeure l'exportateur de mettre en place un PACS, si ses procédures de contrôle interne présentent un risque d'exportation non autorisée d'information.

Le dispositif mis en place par l'exportateur pourra constituer un élément d'appréciation de l'effort réalisé par celui-ci lors des évaluations du CMCAP.

PARTIE 3

-

QUELLES PRÉCAUTIONS PRENDRE DANS L'UTILISATION DES TECHNOLOGIES DE L'INFORMATION ?

3.1. Cadre général

3.1.1. Risques liés à l'emploi de technologie de l'information

L'utilisation croissante des technologies de l'information est susceptible d'accentuer les risques d'exportation non autorisée d'informations, en raison notamment de :

- la divulgation de données contrôlées par négligence ou absence de mise en œuvre de précautions élémentaires ;
- l'accès non désiré, par une autorité gouvernementale étrangère, à des données contrôlées sous couvert de réglementations étrangères.

3.1.2. Registre de suivi des projets

Il est fortement recommandé que l'exportateur tienne un registre des projets utilisant les technologies de l'information. Ce registre participe utilement du respect des exigences de conservation des registres des exportations imposées par le code de la défense, qui doivent en particulier rassembler les informations relatives aux flux d'informations contrôlées.

3.1.3. Marquage des données contrôlées à l'exportation

Un système de marquage[12] permet à l'exportateur d'assurer l'identification et la traçabilité des informations concernées. Le marquage contribue à prévenir les risques d'exportation non autorisée en permettant aux différents acteurs de l'entreprise de prendre conscience de la nature des informations qu'ils manipulent. Il permet également d'orienter le choix de technologies appropriées pour la gestion de ces informations.

La traçabilité des informations contrôlées vise notamment à démontrer qu'une exportation a été réalisée en conformité avec la licence l'ayant autorisée. Elle couvre les éléments suivants :

- les documents transmis (quoi ?) ;
- les destinataires (qui ?) ;
- la date de l'opération (quand ?) ;
- le moyen utilisé (comment ?).

Ces données ont vocation à être conservées dix ans, comme pour l'exportation de matériels.

3.2. Analyse par type de technologie

Le tableau ci-après identifie les principales technologies de l'information utilisées et pour chacune présente :

- les risques particuliers associés ;
- des recommandations qu'il convient de mettre prioritairement en œuvre ;
- des indications complémentaires au travers de référentiels techniques pertinents ;
- des produits ou services certifiés par l'ANSSI, le cas échéant.

Nota : *Lorsqu'une technologie (par exemple, l'utilisation d'un VPN) est associée à une autre (par exemple la messagerie), il convient alors de combiner l'ensemble des risques.*

[12] L'exportateur pourra utilement se reporter aux recommandations de l'ANSSI sur le marquage figurant dans son guide « Recommandations pour les architectures des systèmes d'information sensibles ou diffusion restreinte ».

3.2.1. Accès visuel ou auditif à l'information et messageries électroniques

Technologies	Risques	Recommandations techniques prioritaires	Référentiels techniques de l'ANSSI	Produits ou services recommandés par l'ANSSI (le cas échéant)
Messageries électroniques	• Récupération des informations contrôlées par des destinataires non autorisés • Exposition des informations contrôlées stockées ou en traitement (ex. authentification simple, faible qualité des mots de passe, mauvaise gestion des identités, défaut de traçabilité, faiblesse de sécurité du prestataire de service)	• Chiffrement hors ligne de l'information contrôlée avec des produits qualifiés par l'ANSSI (ex. Cryhod pour le chiffrement de disques ; Zed! pour le chiffrement de fichiers) • Définir les conditions d'utilisation (notamment, échanges, stockage de clés)	• Guide d'hygiène informatique • Recommandations pour une utilisation sécurisée de Cryhod • Recommandations pour une utilisation sécurisée de Zed !	Produits listés dans la catégorie «sécurité du poste de travail» sur le site de l'ANSSI[13]
Messagerie instantanée			NA	Produits listés dans la catégorie «sécurité du poste de travail» sur le site de l'ANSSI
Visio-conférence		• Chiffrement de bout en bout des conférences • Eviter l'utilisation des services de retranscription et de traduction si ces derniers ne sont pas complètement maîtrisés (ces services peuvent faire transiter les informations en dehors du réseau de confiance utilisé pour la visio-conférence)	NA	Produits listés dans la catégorie «Produits autres» sur le site de l'ANSSI *Nota : A la date de publication du présent guide, le produit qualifié par l'ANSSI ne permet pas de traiter des informations de type «diffusion restreinte» et ne peut donc être envisagé que pour échanger des informations qui, bien que contrôlées, ne présentent pas une forte sensibilité.*
Sécurisation des flux *Exemple : VPN*	• Récupération des d'informations contrôlées en traitement par requête administrative ou judicaire d'un Etat tiers	• Définir les règles et maîtriser la gestion des clés et des points de déchiffrement • Application des recommandations de l'ANSSI pour les protocoles TLS et IPSEC • Utilisation de produits VPN qualifiés par l'ANSSI	• Recommandations de sécurité relatives à TLS[14] • Recommandations de sécurité relatives à IPSEC[15] • Recommandations de sécurité concernant l'analyse des flux HTTPS[16]	Produits listés dans les catégories «Equipements de chiffrement IP, ethernet, etc» et «Protection réseau et télécom» sur le site de l'ANSSI[17]
Services de transfert/ d'échange de fichiers volumineux	• Récupération des informations contrôlées par des destinataires non autorisés • Exposition des informations contrôlées stockées ou en traitement (ex.: authentification simple, faible qualité des mots de passe, mauvaise gestion des identités, défaut de traçabilité, faiblesse de sécurité du prestataire de service)	• Chiffrement hors ligne de l'information contrôlée avec des produits qualifiés par l'ANSSI • Définir les conditions d'utilisation (notamment : échanges, stockage de clés)	NA	Produits listés dans la catégorie «stockage sécurisé en nuage» sur le site de l'ANSSI[18]

[13] https://www.ssi.gouv.fr/uploads/liste-produits-et-services-qualifies.pdf.
[14] https://www.ssi.gouv.fr/uploads/2017/07/anssi-guide-recommandations_de_securite_relatives_a_tls-v1.2.pdf.
[15] https://www.ssi.gouv.fr/uploads/2012/09/NT_IPsec.pdf.
[16] https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_TLS_NoteTech.pdf.
[17] https://www.ssi.gouv.fr/uploads/liste-produits-et-services-qualifies.pdf.
[18] https://www.ssi.gouv.fr/uploads/liste-produits-et-services-qualifies.pdf.

3.2.2. Plateformes d'échange, outils collaboratifs, opérations à distance et partages d'écran

Technologies	Risques	Recommandations techniques prioritaires	Référentiels techniques de l'ANSSI	Produits ou services recommandés par l'ANSSI (le cas échéant)
Informatique en nuage	• Exposition des informations contrôlées stockées ou en traitement suite à un défaut de configuration, l'application d'une politique de sécurité insuffisante (ex. authentification simple, faible qualité des mots de passe, mauvaise gestion de identités, défaut de traçabilité) ou une faiblesse de sécurité du prestataire de service • Récupération des informations contrôlées stockées par requête administrative ou judicaire de l'Etat dans lequel circule l'émetteur ou le détenteur de l'information contrôlée à des fins de renseignement ou d'atteinte à la réputation	• Utilisation d'un prestataire de confiance non soumis à de la réglementation extraterritoriale et ayant un niveau de sécurité satisfaisant • Création, modification et chiffrement hors ligne de l'information contrôlée avec des produits qualifiés par l'ANSSI • Définir les conditions d'utilisation (notamment : échanges, stockage des clés de chiffrement, chiffrement des flux) • Mise en place d'authentifications fortes (au moins deux facteurs d'authentification) • Activation et contrôle des options de traçabilité des données et usages (prêter attention aux options de sécurité prévues par le contrat avec le prestataire)	• Prestataires de services d'informatique en nuage (SecNumCloud) – Référentiel d'exigences • Maîtriser les risques de l'infogérance – Externalisation des systèmes d'information	Produits listés dans la catégorie « Informatique en nuage » sur le site de l'ANSSI.
Infogérance[19]		Utilisation d'un prestataire de confiance non soumis à de la réglementation extraterritoriale et ayant un niveau de sécurité satisfaisant	• Maîtriser les risques de l'infogérance – Externalisation des systèmes d'information • Référentiel PAMS (Prestataire d'administration et de maintenance sécurisées) – Référentiel d'exigences	NA

[19] Infogérance : Externalisation appliquée au domaine des systèmes d'information. Elle peut induire les mêmes risques que l'informatique en nuage, dès lors que l'acteur extérieur assurant cette infogérance est implanté à l'étranger.

3.2.3. Technologies de la mobilité, du nomadisme ou du télétravail des employés de l'exportateur

Technologies	Risques	Recommandations techniques prioritaires	Référentiels techniques de l'ANSSI	Produits ou services recommandés par l'ANSSI (le cas échéant)
Téléphones mobiles	• Récupération des informations contrôlées par des destinataires non autorisés • Exposition d'informations contrôlées non autorisées à l'export par une mauvaise gestion de la circulation de l'information (ex. perte du terminal, communication en clair d'informations sensibles)	Chiffrement du terminal, des fichiers et des communications (voix et data)	• Recommandations sur le nomadisme numérique – Guide ANSSI[20] • Recommandations de sécurité relatives aux ordiphones[21] • Bonnes pratiques à l'usage des professionnels en déplacement[22]	Solutions de mobilité dans la liste des produits et services qualifiés par l'ANSSI[23]
Ordinateurs portables ou tablettes		Chiffrement du terminal et des communications	• Recommandations sur le nomadisme numérique – Guide ANSSI • Bonnes pratiques à l'usage des professionnels en déplacement	Produits listés dans la catégorie «sécurité du poste de travail» sur le site de l'ANSSI[24]
Supports de stockage externes *Exemples : disques durs, clés USB*	• Récupération des informations contrôlées par des destinataires non autorisés • Exposition des informations contrôlées non autorisées à l'export par une mauvaise gestion de la circulation de l'information (ex. perte du support de stockage, accès en clair à des informations sensibles, défaut de vigilance ou absence de procédure concernant l'utilisation des supports USB)	Chiffrement du support de stockage	• Recommandations sur le nomadisme numérique – Guide ANSSI • Bonnes pratiques à l'usage des professionnels en déplacement	Solutions de mobilité dans la liste des produits et services qualifiés par l'ANSSI

[20] https://www.ssi.gouv.fr/entreprise/guide/recommandations-sur-le-nomadisme-numerique.
[21] https://www.ssi.gouv.fr/entreprise/guide/recommandations-de-securite-relatives-aux-ordiphones.
[22] https://www.ssi.gouv.fr/uploads/2014/09/anssi_passeport_2019_1.0.pdf.
[23] https://www.ssi.gouv.fr/uploads/liste-produits-et-services-qualifies.pdf.
[24] https://www.ssi.gouv.fr/uploads/liste-produits-et-services-qualifies.pdf.

PRINCIPAUX TEXTES JURIDIQUES ET INSTRUCTIONS

Exportation des matériels de guerre

Code de la défense : articles L. 2335-2, L. 2335-9, L. 2335-18, L. 2339-1, L. 2339-1-1, L. 2339-1-2, R. 2335-9 et R. 2335-21.

Arrêté du 30 novembre 2011 modifié fixant l'organisation du contrôle sur pièces et sur place effectué par le ministère de la défense en application de l'article L. 2339-1 du code de la défense.

Arrêté du 27 juin 2012 modifié relatif à la liste des matériels de guerre et matériels assimilés soumis à une autorisation préalable d'exportation et des produits liés à la défense soumis à une autorisation préalable de transfert.

Protection du secret de la défense nationale

Instruction générale interministérielle n° 1300/SGDSN/PSE/PSD sur la protection du secret de la défense nationale (IGI n° 1300), approuvée le 9 août 2021.

Instruction générale interministérielle n° 2100/SGDN/SSD du 1er décembre 1975 sur la protection en France des informations classifiées de l'Organisation du Traité de l'Atlantique Nord (IGI n° 2100).

Protection du potentiel scientifique et technique de la nation

Article 413-7 du code pénal.

Décret n° 2011-1425 du 2 novembre 2011 portant application de l'article 413-7 du code pénal et relatif à la protection du potentiel scientifique et technique de la nation.

Arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation.

Circulaire interministérielle de mise en œuvre du dispositif de protection du potentiel scientifique et technique de la nation du 7 novembre 2012.

Instruction interministérielle n° 901/SGDSN/ANSSI du 28 janvier 2015 relative à la protection des systèmes d'information sensibles.

GLOSSAIRE

ACID • ACID Cryptofiler – Logiciel de chiffrement conçu par la DGA

AED • Agence européenne de défense

ANSSI • Agence nationale de la sécurité des systèmes d'information

CIEEMG • Commission interministérielle pour l'étude des exportations de matériels de guerre

CMCAP • Comité ministériel du contrôle *a posteriori*

DGA • Direction générale de l'armement

ESA • Agence spatiale européenne

OTAN • Organisation du traité de l'Atlantique Nord

PACS • Plan d'amélioration continue de la sécurité

PASI • Plan d'assurance de sécurité des informations

PPST • Protection du potentiel scientifique et technique de la Nation

PSDN • Protection du secret de la défense nationale

SAIV • Sécurité des activités d'importance vitale

SGDSN • Secrétariat général de la défense et de la sécurité nationale

SIGALE • Système d'information, de gestion et d'administration des licences d'exportation

SSI • Sécurité des systèmes d'information

VPN • Réseau virtuel privé

PREMIÈRE
MINISTRE
Liberté
Égalité
Fraternité

Secrétariat général de la défense
et de la sécurité nationale

Affaires internationales, stratégiques et technologiques
51, boulevard de la Tour Maubourg, 75007 Paris
Version 1.0 - Avril 2023