LIE n°14 de la DRSD

Le *lawfare* ou l'usage du droit à des fins stratégiques

La lettre d'information économique
Novembre 2023

Sommaire

Éditorial du Directeur du Renseignement et de la Sécurité de la Défense

Mesdames, Messieurs,

Le 9 novembre 2022, le président de la République présentait la nouvelle Revue nationale stratégique (RNS), document cadre de la doctrine stratégique française qui fixe les enjeux auxquels la France doit répondre dans les prochaines années en matière de défense et de sécurité. Parmi les menaces qui pèsent sur nos intérêts, la RNS 2022 identifie l'usage stratégique de la norme (ou *lawfare*) comme l'un des instruments mobilisés par nos compétiteurs pour prendre l'ascendant en matière économique.

Depuis 2017, la Direction du renseignement et de la sécurité de la Défense (DRSD) travaille et alerte sur cette nouvelle menace, exacerbée dans le contexte de durcissement continu de la compétition internationale. En effet, les entreprises et établissements de recherche constituant notre Base industrielle et technologique de défense (BITD) peuvent se révéler particulièrement vulnérables à ce vecteur potentiel d'ingérences économiques.

Dans le cadre des stratégies hybrides, l'instrumentalisation par certains États de leur droit national, à travers sa portée extraterritoriale, et les manœuvres d'influence conduites auprès des instances de normalisation sont employées comme levier de puissance.

Pleinement consciente de cette nouvelle donne, la DRSD souhaite à travers cette LIE partager avec vous l'état de la connaissance sur la menace *lawfare*, en matière de captation d'informations sensibles et de savoir-faire stratégiques, voire de déstabilisation d'entreprises. Notre engagement s'inscrit plus largement dans l'effort piloté au niveau interministériel par le Secrétariat général de la défense et de la sécurité nationale (SGDSN).

Notre souveraineté nationale et notre autonomie stratégique étant directement menacées par les pratiques en matière de *lawfare*, je renouvelle mon souhait de maintenir notre dynamique d'échanges afin d'apporter la meilleure réponse possible aux ingérences normatives auxquelles vous pouvez être confrontés.

Soyez une fois encore assurés de la disponibilité de nos agents à vos côtés pour vous accompagner dans votre volonté de protection face à cette menace protéiforme.

Général de corps d'armée Philippe Susnjara
Directeur du Renseignement et de la Sécurité de la Défense

Introduction : qu'est-ce que le *lawfare* ?

Le *lawfare*, contraction des termes anglo-saxons « *law* » (droit) et « *warfare* » (guerre), désigne **l'usage coercitif de normes juridiques** à l'encontre d'un adversaire à des fins politico-stratégiques. Parfois utilisé comme un instrument complémentaire au sein de stratégies hybrides, il peut être utilisé pour déstabiliser un adversaire ou concurrent et favoriser les intérêts d'un État.

L'usage stratégique du droit (*lawfare*) tel qu'identifié dans la Revue nationale stratégique de 2022 se décline selon trois axes :

- l'instrumentalisation par certains États de leur propre droit, à travers l'extraterritorialité[1] ;
- le détournement de la norme internationale ;
- l'exploitation des vulnérabilités juridiques de notre droit interne.

Les entreprises de la Base industrielle et technologique de défense (BITD) sont particulièrement vulnérables à **l'utilisation extraterritoriale du droit** par des pays étrangers. Certains États peuvent ainsi utiliser leur propre droit national comme **outil de protectionnisme** afin de protéger leurs entreprises et technologies stratégiques. Le droit peut également être utilisé comme **outil de coercition économique.** Les États peuvent ainsi cibler des entreprises pour les contraindre à adopter certains comportements. Enfin, le droit peut être utilisé comme **outil de politique étrangère** pour restreindre l'activité économique d'un pays adverse. À titre d'exemple, l'adoption d'embargos ou de sanctions économiques peut ainsi interdire aux entreprises d'exporter des biens vers certaines destinations.

Les entreprises doivent donc être conscientes de leur degré d'exposition aux contraintes issues de ces réglementations. En effet, en cas de non-conformité, les États concernés peuvent leur infliger des **sanctions économiques** ou encore des **contrôles de mise en conformité.**

Le lien de rattachement de l'entreprise à la norme étrangère peut être basé sur **l'activité commerciale** de l'entreprise sur le territoire étranger, ses **partenariats** avec des entreprises étrangères, son **actionnariat** étranger ou encore ses **filiales** à l'étranger.

De manière plus générale, l'usage d'une monnaie spécifique dans les transactions réalisées ou l'utilisation de moyens de communication particuliers peuvent créer un lien de rattachement avec un pays étranger, justifiant ainsi l'application de ses règles juridiques.

[1] Définition de *Dalloz* : L'extraterritorialité concerne les normes juridiques dont le champ d'application excède la compétence territoriale de l'État.

Stéphane BOUILLON,
Secrétaire général de la défense et de la sécurité nationale

QU'EST-CE QUE LE *LAWFARE* ?

Initialement issu du monde militaire, le concept de *lawfare* désigne aujourd'hui plus largement l'utilisation du droit à des fins stratégiques, dans les champs militaire mais aussi économique, diplomatique, etc.

Non dépourvu d'ambiguïtés, le terme de *lawfare* doit donc être abordé avec prudence car il recouvre une grande variété d'acteurs et une grande diversité de pratiques.

Il n'en reste pas moins que l'usage stratégique du droit par différents acteurs, étatiques ou non, s'est intensifié dans des proportions inédites sur la période récente. Cela s'explique notamment par la place croissante qu'occupent le droit et la justice dans nos sociétés, la mondialisation d'un nombre toujours plus important d'activités favorisant les phénomènes de *law shopping*[2], ou encore la rapidité des évolutions technologiques, qui appellent à construire de nouvelles régulations.

Ainsi, la norme est désormais conçue autant **comme un levier de puissance et de confrontation que comme un outil de régulation.**

QUELLES SONT LES PRINCIPALES MENACES ?

On peut identifier trois grandes menaces autour desquelles nous avons concentré notre attention.

Le *lawfare* normatif, tout d'abord : chaque État dispose bien sûr d'une capacité souveraine à réguler les activités de son ressort en produisant des normes et en faisant en sorte qu'elles soient respectées. Mais ce qui est préoccupant aujourd'hui, c'est que cette capacité est de plus en plus employée comme un outil de puissance et de compétition. L'exemple le plus significatif est bien sûr l'extraterritorialité, qui désigne l'application unilatérale de normes par un État en dehors de son territoire. Ce n'est pas forcément toujours illicite du point de vue du droit international et cela peut être légitime. Mais l'extraterritorialité peut devenir un puissant outil d'ingérence et de prédation lorsqu'elle s'applique sur la base de critères flous ou encore lorsqu'elle conduit un État à imposer ses normes directement à un autre État sans le consentement de ce dernier.

Le *lawfare* contentieux, ensuite : cela désigne l'instrumentalisation de nos juridictions par l'introduction d'actions en justice. Celles-ci sont rarement fructueuses, mais le but n'est pas tant d'obtenir un succès contentieux que de créer un effet d'intimidation ou de discrédit.

Le *lawfare* d'influence, enfin : il s'agit de démarches d'influence afin, par exemple, de faire prévaloir une interprétation de certaines normes internationales existantes (ce qui peut conduire à dévoyer ces normes) ou encore d'influencer l'élaboration de normes dans des domaines encore peu régulés. Il peut également s'agir de manœuvres étatiques visant à peser sur l'élaboration de nos propres normes par des actions d'influence auprès de ceux qui les fabriquent.

[2] Phénomène consistant, pour un individu ou une entreprise, à profiter de la diversité des systèmes juridiques pour choisir le plus profitable, par exemple dans le cadre d'un contentieux.

QUELLES RÉPONSES L'ÉTAT PEUT-IL APPORTER ?

Si, de notre point de vue, le droit doit rester un outil d'apaisement et de pacification des rapports sociaux et internationaux, cela ne nous empêche pas de répondre, dans le respect de nos principes et de nos valeurs, aux usages abusifs ou malveillants qui en sont faits et de promouvoir nos propres normes.

C'est dans cette perspective que le SGDSN travaille, avec l'ensemble des ministères et services, dont la DRSD, à identifier et mettre en œuvre les moyens de faire face à cette menace. Plusieurs pistes se dessinent d'ores et déjà.

Premièrement, il est impératif **d'améliorer notre connaissance et notre anticipation de la menace,** qui est protéiforme et évolutive. Le rôle des services est évidemment clé pour ce faire. Mais c'est aussi l'affaire de tous ceux qui peuvent faire l'objet d'attaques de type *lawfare* : entreprises, praticiens du droit notamment. Il est important que ces acteurs soient sensibilisés, voire dessillés, face à la réalité de ce phénomène. Enfin, une veille constante doit être menée sur les champs normatifs en friche ou en voie de régulation, comme par exemple le cyber ou le spatial : nous ne pouvons pas permettre que ces domaines cruciaux pour notre autonomie stratégique soient régulés demain selon les standards de nos compétiteurs.

Un deuxième axe d'effort consiste **à réduire nos vulnérabilités juridiques qui peuvent être exploitées à notre détriment.**

Cela passe d'abord par un meilleur encadrement de l'influence étrangère qui peut s'exercer sur l'élaboration de nos normes, en la rendant plus transparente voire en l'écartant lorsque cela est nécessaire.

Il faut également s'assurer que notre droit ne soit pas instrumentalisé par nos compétiteurs : pour ce faire, il importe de défendre nos intérêts devant les juridictions, de dissuader les recours abusifs et de communiquer fermement en vue de déconstruire le narratif bâti par l'adversaire.

En troisième lieu, il convient **de se doter d'outils de riposte adaptés.** Nous avons déjà des outils (loi de blocage, règlement de blocage par exemple) qui permettent en partie d'endiguer les effets négatifs qui peuvent nous être infligés par des normes étrangères. Mais cela n'est pas suffisant : il faut aussi pouvoir riposter lorsque cela est nécessaire De ce point de vue, il faut souligner les progrès considérables réalisés par l'Union européenne qui, avec l'engagement de la France, est en train de se doter d'un véritable arsenal pour lutter contre la coercition économique, notamment lorsque celle-ci passe par le droit.

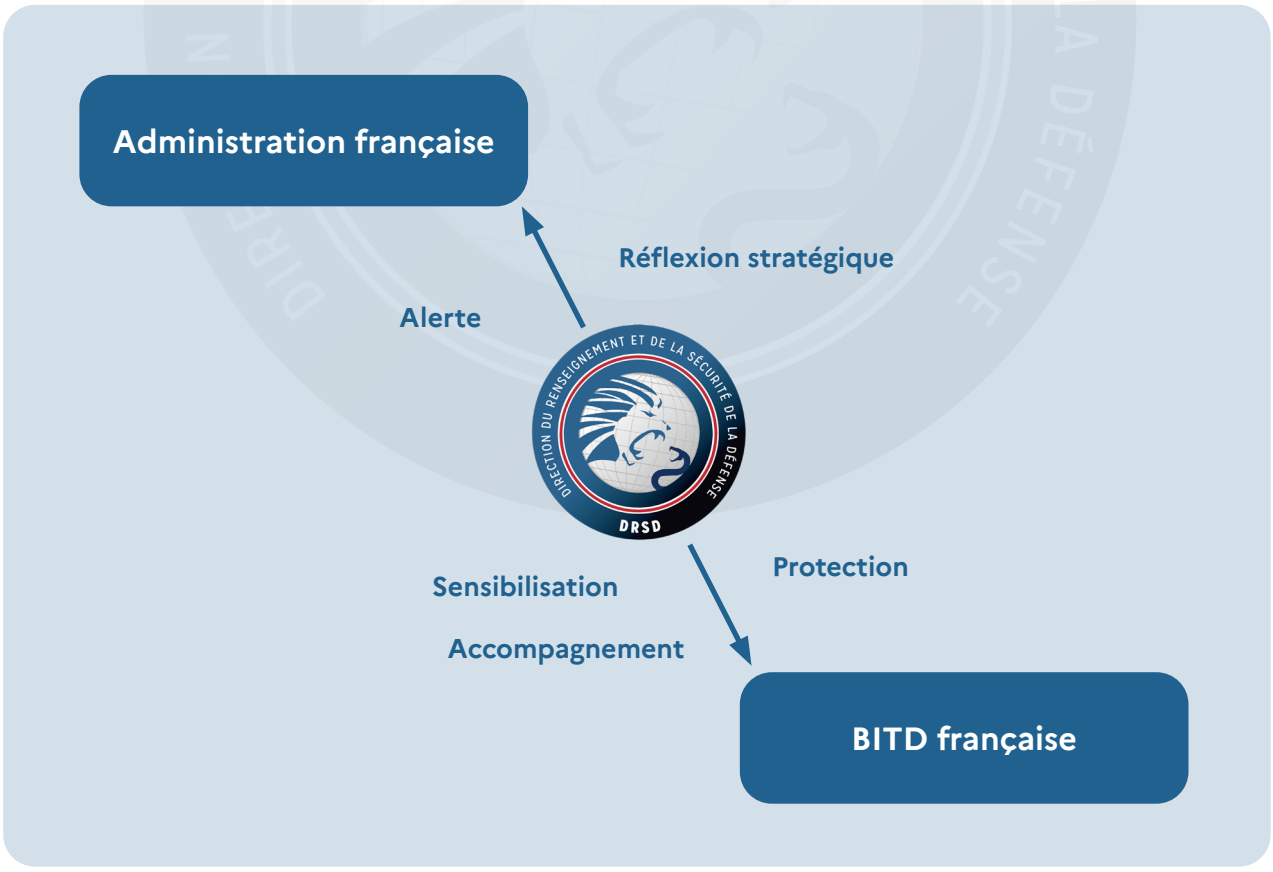
Enfin, si la France ne cherche pas à imposer brutalement une vision unilatérale du droit, elle a néanmoins pleinement son rôle à jouer pour **promouvoir largement à l'international des normes conformes à ses valeurs et à ses intérêts,** d'autant que dans de nombreux domaines les normes françaises et européennes offrent un cadre juridique parmi les plus complets et ambitieux du monde. La réglementation sur la protection des données ou en matière de normes sociales et environnementales en constituent autant d'exemples.

Rôle et mission de la DRSD en matière de *lawfare*

La DRSD s'attache à anticiper, détecter, caractériser et **entraver les tentatives d'ingérences étrangères** utilisant le droit comme un outil coercitif à l'encontre des intérêts économiques, industriels et scientifiques majeurs de la France.

Dans ce cadre, la DRSD a plusieurs missions :

- **veille juridique** sur les normes à portée extraterritoriale susceptibles d'être appliquées aux entreprises de la BITD et **anticipation des risques induits** ;
- **contribution à la réflexion stratégique** sur l'usage stratégique du droit et la protection des intérêts nationaux face aux ingérences normatives ;
- **sensibilisation des entreprises** de la BITD aux risques liés à l'application de normes à portée extraterritoriale ;
- **détection** à temps des premiers signaux de tentatives de contrainte ou de déstabilisation par le biais de juridictions étrangères ;
- **accompagnement des entreprises** de la BITD visées par des normes à portée extraterritoriale dans l'objectif de limiter les risques et la captation d'informations sensibles par des acteurs étrangers.



Exemple d'outils normatifs s'appliquant aux entreprises de la BITD française

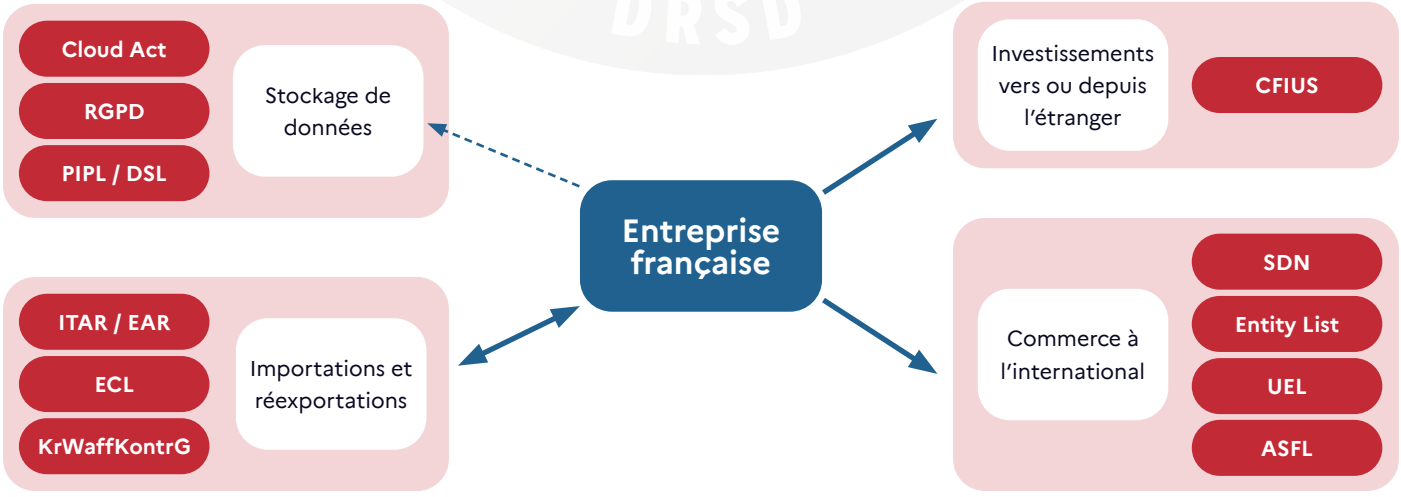
Domaine	Réglementation	État	Contexte	Risque(s)
Contrôle des exportations de technologies sensibles	*International Traffic in Arms Regulations* (ITAR) / *Export Administration Regulations* (EAR)	États-Unis	Les entreprises qui utilisent des composants d'origine américaine contrôlés par les réglementations ITAR et EAR doivent faire l'objet d'une autorisation officielle et se conformer à diverses obligations dans la gestion de ces composants.	Poursuites et sanctions
				Audits de conformité par les autorités américaines
				Restriction des exportations
	Export Control Law (ECL)	Chine	Les entreprises qui utilisent des composants d'origine chinoise contrôlés par la réglementation ECL doivent faire l'objet d'une autorisation officielle avant une exportation ou réexportation.	Poursuites et sanctions
				Restrictions des exportations
	Kriegswaffenkontrollgesetz (KrWaffKontrG)	Allemagne	Les entreprises qui intègrent des composants allemands dans des systèmes d'armes doivent obtenir une autorisation officielle avant une exportation ou réexportation.	Poursuites et sanctions
				Restriction des exportations

Exemple d'outils normatifs s'appliquant aux entreprises de la BITD française

Domaine	Réglementation	État	Contexte	Risque(s)
Sanctions économiques	*Entity List*	États-Unis	Le Département du commerce américain peut adopter des sanctions visant des entités étrangères spécifiques. Celles-ci doivent alors obtenir une autorisation de l'administration américaine pour exercer certaines activités commerciales en lien avec les États-Unis. L'objectif est de restreindre les flux de biens et technologies.	Restriction des activités commerciales dans certains pays Poursuites et sanctions
	Specially Designated Nationals and Blocked Persons List (SDN)	États-Unis	Cette liste diffusée par le Département du trésor recense les personnes physiques et morales susceptibles de représenter une menace à la sécurité nationale américaine ou à ses politiques économiques et étrangères. Les personnes exerçant une activité aux États-Unis ont interdiction de travailler avec les personnes désignées par la liste. L'objectif est de restreindre notamment les transactions financières.	
	Unreliable Entity List	Chine	Les autorités chinoises peuvent placer des entités étrangères sur une « liste noire » afin de restreindre leurs activités commerciales avec la Chine.	Sanctions
	Anti-Foreign Sanctions Law (AFSL)	Chine	Les entreprises qui se conforment à des sanctions internationales contre la Chine peuvent faire l'objet de mesures de rétorsion par les autorités chinoises.	Restriction des activités commerciales Poursuites et sanctions

Exemple d'outils normatifs s'appliquant aux entreprises de la BITD française

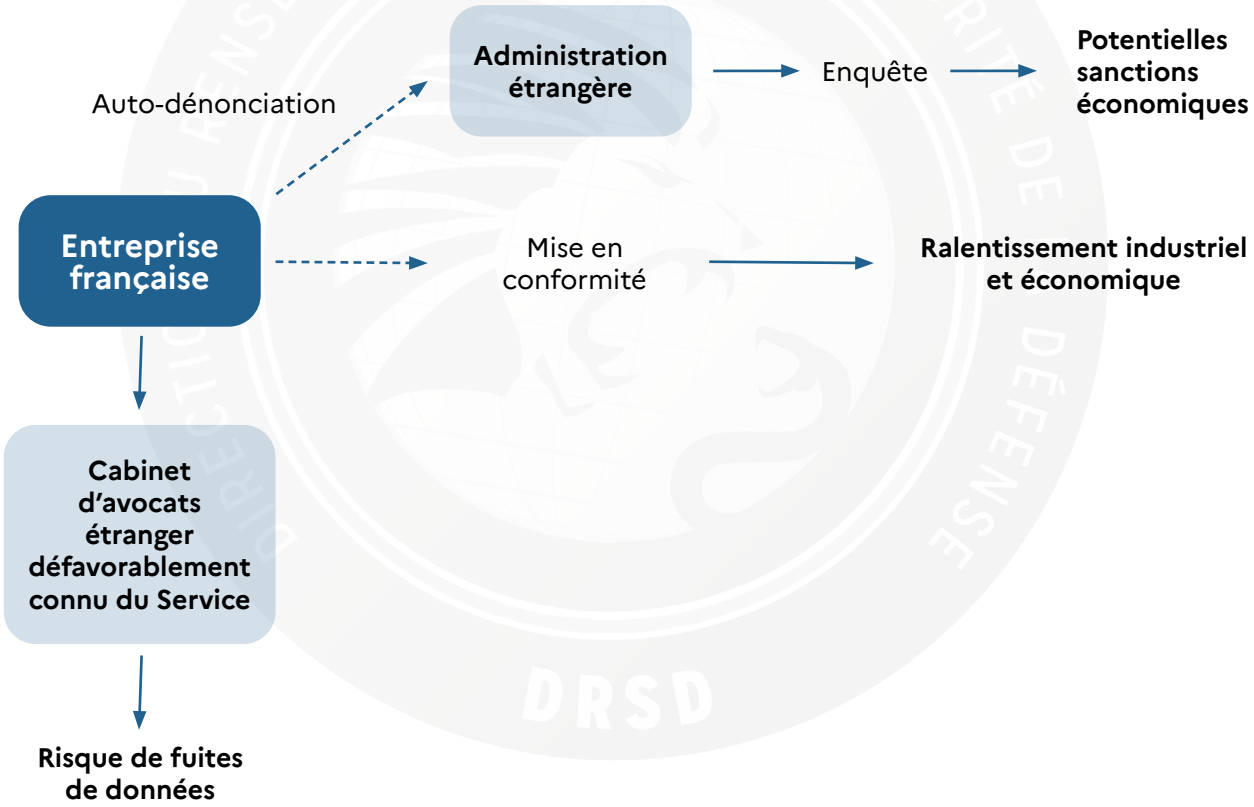
Domaine	Réglementation	État	Contexte	Risque(s)
Cyber	*CLOUD Act*	États-Unis	Les autorités américaines peuvent, dans certaines conditions, accéder aux données que les entreprises françaises confient à des fournisseurs Cloud américains.	Transmission non contrôlée de données
	Cybersecurity Maturity Model Certification (CMMC)	États-Unis	Les entreprises contractant directement ou indirectement avec le Département de la Défense américain (DoD) peuvent faire l'objet d'un audit de leurs systèmes d'information pour vérifier leur niveau de cybersécurité.	Audits informatiques
	Personal Information Protection Law (PIPL)	Chine	Les lois PIPL et DSL permettent à la Chine de contrôler les activités de traitement de données effectuées hors du territoire chinois lorsqu'elles concernent des personnes physiques chinoises ou les intérêts chinois.	Sanctions
	Data Security Law (DSL)			
Contrôle des investissements étrangers	Procédures du *Committee on Foreign Investment in the United States* (CFIUS)	États-Unis	Les entreprises souhaitant investir dans des entités américaines, ou ayant une activité commerciale aux États-Unis, doivent faire l'objet d'une procédure de contrôle intrusive par le CFIUS.	Audits Refus d'une partie de la transaction



CAS CONCRETS d'ingérences normatives visant des entreprises de la BITD française

CAS CONCRET 1
Mise en conformité avec les réglementations de contrôle des exportations

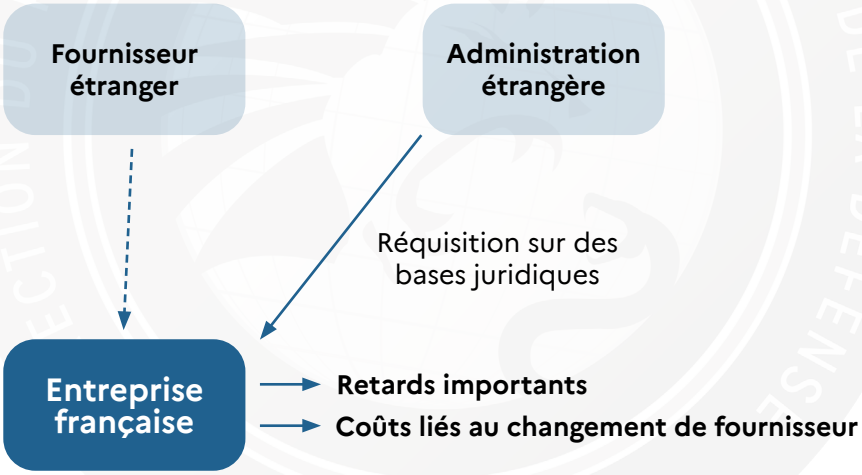
En 2020, une entreprise de la BITD a découvert dans l'historique de ses activités commerciales l'existence de plusieurs manquements aux réglementations de contrôle des exportations **d'un pays étranger.** En suivant les conseils de son cabinet d'avocats, l'entreprise a transmis aux autorités une auto-dénonciation reconnaissant les faits. Ainsi, elle s'expose à une **amende** de plusieurs millions de dollars ainsi qu'à un **potentiel monitorat étranger.** En attendant une décision officielle de l'administration, l'entreprise a adopté un programme de conformité pour mettre fin aux irrégularités constatées. Ce programme a entrainé un **ralentissement de l'activité** de l'entreprise ; la société risque également de perdre certains clients craignant des sanctions internationales par rebond.



CAS CONCRET 2
Réquisition de matériaux stratégiques

En 2022, une entreprise de la BITD s'approvisionnant en composants de semi-conducteurs auprès d'un distributeur étranger a vu ses **commandes réquisitionnées de façon arbitraire** par un État étranger. En effet, celui-ci a décidé d'allouer les ressources à son industrie nationale en priorité pour maintenir le niveau d'approvisionnement sur son marché.

Du fait de cette réquisition, l'entreprise française a subi des retards de production pouvant atteindre **36 semaines.** Pour limiter les retards auprès de ses clients, l'entreprise a dû identifier un **fournisseur de substitution** proposant des **tarifs cinq fois plus élevés.**



Recommandations

Comment prémunir son entreprise des risques liés au *lawfare* ?

Veiller à la conformité de ses activités

- **Anticiper** la mise en conformité de l'entreprise avant la découverte d'irrégularités ;
- **Obtenir un accompagnement** d'un cabinet de conseil ou d'avocats spécialisé, en privilégiant les cabinets français ;
- **Recruter** un collaborateur spécialisé en conformité ;
- **Former** un ou plusieurs collaborateurs aux questions de conformité.

Bonnes pratiques cyber

- Recourir à un **fournisseur de *cloud* français de préférence** ;
- **Chiffrer ses données** et conserver le contrôle des clés de chiffrement ;
- **Lire attentivement les contrats** passés avec les prestataires de services étrangers.

Contacts et ressources

Loi de blocage[3]
loi.deblocage@finances.gouv.fr

Conformité ITAR / EAR
dga-di.certificats-etrangers.fct@intradef.gouv.fr
09 88 67 26 86

Contact du ministère des Armées pour les PME-ETI
dga.pme.fct@intradef.gouv.fr
0 800 027 127

Contact DRSD
drsd-cie-sensibilisation.contact.fct@intradef.gouv.fr

En cas de demande d'inspection de l'administration américaine
controle-export@sgdsn.gouv.fr

« Les règlementations américaines du contrôle des exportations »
DGA Communications, février 2022

« Les règlementations américaines de contrôle à l'exportation des biens sensibles »
SGDSN, DSAF/SPDG, juin 2020

« Guide à usage des entreprises d'identification des données sensibles »
SISSE, AFEP, EF, décembre 2021

PME-ETI, LE MINISTÈRE DES ARMÉES EST À VOTRE ÉCOUTE

0 800 02 71 27
Appel gratuit

[3] Voir la LIE n°10 (mai 2022), p.7, « Évolution des modalités d'application de la loi dite ''de blocage'' »

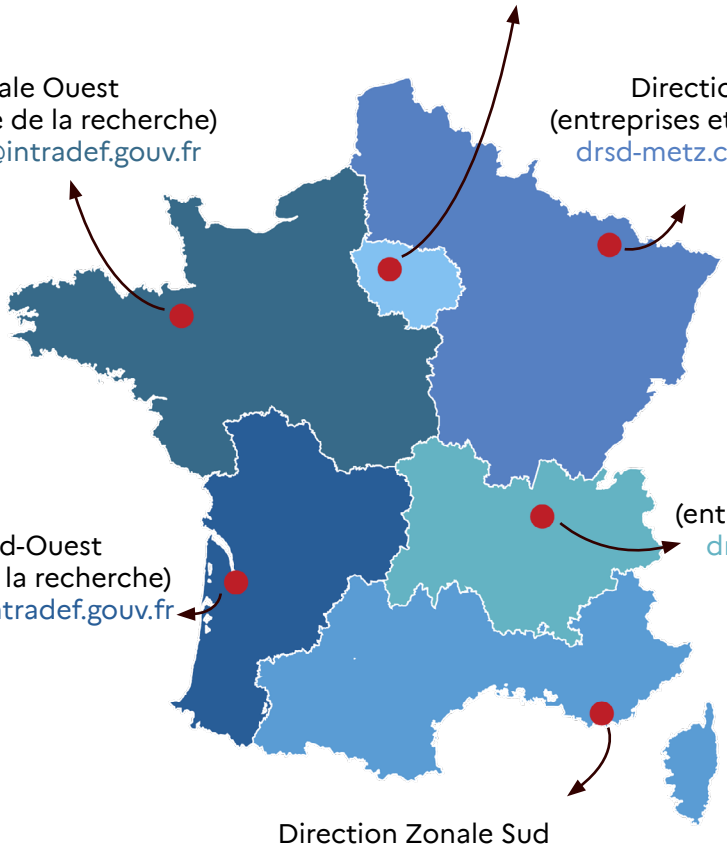
Gardons le contact

Direction Centrale
Section « Sensibilisation »
drsd-cie-sensibilisation.contact.fct@intradef.gouv.fr

Directions Zonales Ile-de-France
Entreprises : drsd-dsezp-4.cds.fct@intradef.gouv.fr
Écoles et instituts de recherche : prsd-villacoublay.cmi.fct@intradef.gouv.fr

Direction Zonale Ouest
(entreprises et monde de la recherche)
drsd-rennes.cmi.fct@intradef.gouv.fr

Direction Zonale Nord-Est
(entreprises et monde de la recherche)
drsd-metz.cmi.fct@intradef.gouv.fr



Direction Zonale Sud-Est
(entreprises et monde de la recherche)
drsd-lyon.cmi.fct@intradef.gouv.fr

Direction Zonale Sud-Ouest
(entreprises et monde de la recherche)
drsd-bordeaux.cmi.fct@intradef.gouv.fr

Direction Zonale Sud
(entreprises et monde de la recherche)
drsd-toulon.cmi.fct@intradef.gouv.fr