



CONTRE-MESURES JURIDIQUES ET INGERENCES ÉCONOMIQUES

RAPPORT FINAL PRÉSENTÉ PAR LA PROMOTION 01
DES FORMATIONS SIJ / MSIJ 2024-2025

SIJ/MSIJ 01

Octobre 2025



Contre-mesures juridiques et ingérences économiques.

RAPPORT FINAL PRESENTE PAR LA PROMOTION OLIVIER MARLEIX

“Le monde a changé, et la naïveté est censée ne plus avoir cours.”

Olivier Marleix

SOMMAIRE

| | |
|---|-----------|
| SOMMAIRE | 3 |
| INTRODUCTION | 4 |
| I. COERCITION ECONOMIQUE : EMBARGOS, RESTRICTION EXPORT, ACCES MARCHES, SANCTIONS EXTRATERRITORIALES | 5 |
| II. FACE AUX POLITIQUES ETRANGERES DE CAPTATION, DES INSTRUMENTS DE CONTROLE DES INVESTISSEMENTS ET UN CONTRE-RENSEIGNEMENT ECONOMIQUE ET INDUSTRIEL A AMELIORER | 14 |
| III. DEPENDANCE STRUCTURELLE : CHAINES APPRO, ENERGIE, STANDARDISATION US | 25 |
| CONCLUSION ET OUVERTURE | 33 |
| ANNEXES | 35 |
| GLOSSAIRE | 45 |
| BIBLIOGRAPHIE | 50 |
| TABLE DES MATIERES | 58 |
| DROITS D'AUTEURS | 61 |

INTRODUCTION

La souveraineté juridique pourrait s'analyser comme étant la capacité d'un État à défendre son indépendance et son autorité en exerçant pleinement ses pouvoirs exécutif, législatif économique et social sur l'ensemble de son territoire.

Depuis plusieurs années, force est de constater que la souveraineté juridique de la France est régulièrement mise à mal. Attaquée, directement ou indirectement par différentes actions diligentées par voie directe ou non par d'autres nations en utilisant des moyens juridiques, informationnels technologiques et, plus globalement, et, surtout par des moyens économiques qui peuvent être assimilées des ingérences.

L'article L562-1 du code monétaire et financier présente l'acte d'ingérence comme étant un agissement commis directement ou indirectement à la demande ou pour le compte d'une puissance étrangère et ayant pour objet ou pour effet, par tout moyen, y compris la communication d'informations fausses ou inexactes, de porter atteinte aux intérêts fondamentaux de la Nation, au fonctionnement ou à l'intégrité de ses infrastructures essentielles ou au fonctionnement régulier de ses institutions démocratiques.

Cette ingérence économique se manifeste, se déploie ou prend la forme notamment de massifs investissements étrangers, souvent inamicaux dans les secteurs stratégiques, de campagnes de déstabilisation économique ou encore de pressions juridiques et politiques.

Au cours de cette année de formation, il nous a été donné d'étudier plusieurs cas d'ingérences économiques, de plus en plus importants et déstabilisateurs nonobstant les mesures prises pour y faire face.

Face à cette situation qui ne semble vouloir s'estomper, il apparaît plus qu'opportun de faire un état des lieux des mesures ou du dispositif mis en place par la France, à l'effet, après analyse, de faire ressortir les lacunes ou insuffisances et, faire des propositions ou recommandations pouvant contrecarrer ces ingérences économiques étrangères ou à minima, réduire leurs impacts sur la souveraineté juridique de la France.

Pour ce faire, la première partie de la démarche a consisté en une étude des exemples les plus caractéristiques d'ingérences économiques dont a été victime la France et quels étaient les textes de droit interne ou de droit européen qui pouvaient être appliqués pour contrer ou, à tout au moins, amoindrir les conséquences dommageables. Il en ressort que trois grandes catégories d'ingérences peuvent être distinguées ; en premier lieu, les actions de coercition économique (I), en second lieu les actions qui entrent dans le champ de la captation (II) et enfin des actions rendues possible par notre dépendance structurelle (III)

I. Coercition économique : embargos, restriction export, accès marchés, sanctions extraterritoriales

Dans un contexte de rivalités économiques croissantes, les États utilisent de plus en plus les instruments juridiques et commerciaux comme leviers de puissance. Embargos, contrôles des exportations, sanctions extraterritoriales ou surtaxes douanières ne visent plus seulement à réguler le commerce, mais à infléchir le comportement d'autres États et à protéger des secteurs stratégiques.

A. Entre pression américaine et souveraineté française : le poids de l'extraterritorialité du droit dans la compétition économique

Bien que l'idée d'extraterritorialité du droit trouve des origines historiques en Europe et en Asie, ce sont les États-Unis qui en ont été les véritables pionniers, en l'érigeant en instrument d'influence et d'ingérence économique. Au fil des années, sous l'impulsion des législations et actions américaines, la France, comme l'Union européenne, a progressivement intégré des mécanismes juridiques extraterritoriaux afin de protéger ses intérêts stratégiques.

Au niveau législatif américain, le Foreign Corrupt Practices Act (FCPA) interdit à toute entreprise ou tout individu relevant de la juridiction des États-Unis de verser un pot-de-vin ou un avantage indu à un responsable public étranger dans le but d'obtenir ou de conserver un marché ou un avantage commercial¹. Cette législation s'applique dès lors qu'une entreprise cotée aux États-Unis est impliquée dans un acte de corruption visant un agent public, indépendamment de la nationalité des personnes en cause ou du lieu où l'infraction est commise.

Le Public Company Accounting Reform and Investor Protection Act (plus connu sous le nom de Sarbanes-Oxley Act) complète cette approche en renforçant les obligations de conformité et en étendant la portée des règles américaines aux sociétés américaines cotées et à l'ensemble de leurs filiales, y compris celles implantées à l'étranger².

L'ensemble de ces dispositifs illustre la portée large de l'extraterritorialité du droit américain, fondée notamment sur l'utilisation du dollar et le statut boursier des entreprises concernées.

Cependant, ces pratiques ont eu des impacts négatifs, suscitant des réactions de la part des alliés, notamment la France, et fragilisant parfois le dollar sur la scène financière internationale. Par exemple, en 2023, l'Iran a signé un accord de libre-échange avec l'Union économique eurasiatique, comprenant la Russie, le Kazakhstan et d'autres pays, visant à réduire sa dépendance au dollar américain dans les échanges commerciaux³. De plus, en mai 2025, le Brésil a annoncé un accord de swap de devises avec la Banque populaire de Chine d'une valeur

¹ *Foreign Corrupt Practices Act (FCPA)*, « Dispositions sur la lutte contre la corruption et sur les livres comptables et les archives », traduction française, 22 juillet 2004, version consolidée, U.S. Department of Justice

² *Sarbanes-Oxley Act of 2002 [Public Law 107-204, approuvée le 30 juillet 2002; version consolidée « As Amended Through P.L. 117-328, en-fin 29 déc. 2022 »]*, 116 Stat. 745

³ "Russian-backed union signs free trade pact with Iran," Reuters, 25 décembre 2023.

maximale de 157 milliards de reais (environ 27,7 milliards de dollars), dans le but de renforcer la liquidité et de soutenir les marchés financiers en période de stress, réduisant ainsi sa dépendance au dollar américain⁴.

Toutefois, le droit américain est clairement utilisé comme instrument au service des entreprises américaines, constituant une véritable stratégie de domination économique. Par exemple, en 2024, sur 11 actions en justice intentées contre des entreprises, 5 concernaient des sociétés étrangères, soit environ 45 %, illustrant ainsi la portée extraterritoriale et sélective de l'application du FCPA⁵. Le cas d'Alstom en 2014 illustre parfaitement cette dynamique⁶ : dans le cadre d'une enquête américaine portant sur des actes de corruption liés à des contrats en Indonésie, l'enquête a coïncidé avec la mise en vente de la branche énergie d'Alstom à General Electric, société américaine. Cette procédure a largement influencé la transaction, qui a entraîné le transfert des activités stratégiques françaises à une entreprise américaine, perçu comme un affaiblissement de la souveraineté industrielle de la France. La valeur de la branche énergie vendue s'élevait à plusieurs milliards d'euros, et le contrôle de contrats clés a renforcé la position de General Electric sur le marché mondial de l'énergie.

Face à l'application extraterritoriale du droit américain, la France, particulièrement exposée à cette stratégie, a réagi dès 1968 en adoptant la loi dite de blocage⁷, interdisant la transmission d'informations économiques, commerciales ou techniques à des autorités étrangères sans autorisation préalable.

Ce dispositif a ensuite été complété au niveau européen par le règlement de blocage, qui vise à protéger les entreprises de l'Union européenne contre les effets de l'application extraterritoriale de législations étrangères, notamment américaines.⁸ Cette législation a été renforcée par la loi Sapin II en 2016, qui prévoit des sanctions pénales en cas de violation, notamment pour la protection des secrets d'affaires⁹. La loi Sapin II a également introduit le CJIP (Convention Judiciaire d'Intérêt Public), équivalent français du DPA anglo-saxon, permettant à une entreprise reconnue coupable de corruption ou de fraude de négocier un accord avec le PNF (Parquet National Financier). L'entreprise s'engage ainsi à payer une amende et à mettre en place des mesures de conformité, évitant un procès pénal complet tout en réduisant son exposition aux pressions extraterritoriales, comme celles issues du FCPA américain. Parallèlement, les entreprises françaises ont renforcé leurs procédures de due diligence, vérifiant systématiquement la conformité de leurs partenaires et opérations internationales afin de prévenir l'ingérence économique américaine et de protéger leurs intérêts stratégiques. Cependant, ces dispositifs ont montré leurs limites, en raison notamment de la prééminence du dollar dans les transactions internationales et de l'absence de réciprocité dans l'application du droit.

⁴ *Brazil central bank to sign currency swap deal with China's PBOC,* Reuters, 12 mai 2025.

⁵ *Brad Weil, "FCPA Enforcement Actions Against Foreign Companies from OECD Convention Peer Countries," FCPA Professor, 10 janv. 2025.*

⁶ *Alstom SA, "Alstom Pleads Guilty and Agrees to Pay \$772 Million Criminal Penalty to Resolve Foreign Bribery Charges," United States Department of Justice Office of Public Affairs, 22 déc. 2014.*

⁷ *Loi n° 68-678 du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères.*

⁸ *Règlement (CE) n° 2271/96 du Conseil du 22 novembre 1996 portant protection contre les effets de l'application extraterritoriale d'une législation adoptée par un pays tiers.*

⁹ *Loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique.*

En février 2025, le président américain Donald Trump a signé un décret exécutif suspendant temporairement l'application du FCPA, afin de réévaluer son impact sur la compétitivité économique des États-Unis¹⁰. Ce décret visait à limiter ce que l'administration considérait comme une application excessive et imprévisible de la loi, susceptible de nuire aux intérêts économiques et à la sécurité nationale du pays.

Cette suspension a été accompagnée de nouvelles directives du Département de la Justice, établissant des critères plus stricts pour l'ouverture de nouvelles enquêtes FCPA. Ces mesures ont été perçues comme un moyen de recentrer l'application de la loi sur les intérêts stratégiques américains, tout en réduisant les risques pour les entreprises opérant à l'international.

Avec un retrait relatif des États-Unis dans la lutte anticorruption mondiale, le PNF est appelé à jouer un rôle plus actif. Grâce aux CJIP, le Parquet peut intensifier les poursuites, y compris contre des entreprises américaines opérant en France.

RECOMMANDATIONS

Promouvoir, au sein du Conseil de l'UE, une révision du règlement de 1996 afin d'y inclure une clause de réciprocité : toute mesure américaine à portée extraterritoriale entraînerait des contre-mesures équivalentes en Europe (gel d'actifs, amende, ou restriction d'accès au marché européen).

Coordonner la reconnaissance mutuelle des dispositifs de conformité : création d'un protocole bilatéral de consultation préalable pour réduire les risques de double sanction. Création d'un groupe de travail permanent réunissant le PNF, l'Agence française anticorruption, le DOJ, et la SEC (Securities and Exchange Commission) pour harmoniser les programmes de conformité transnationaux.

Les condamnations sur le fondement du FCPA ont été l'illustration de l'extraterritorialité du droit américain les plus marquantes pour l'économie mondiale. La réglementation export control est un outil de contrevenance tout aussi impactant à l'encontre de la souveraineté juridique de la France.

B. Le contrôle des exportations, un outil juridique face aux dépendances étrangères

La vente de matériel de guerre et la culture du secret en ce domaine représentent un enjeu stratégique pour tous les États. En ce sens, chacun a adopté une législation lui permettant de contrôler les technologies qui entrent et sortent de son territoire afin de garantir sa souveraineté et de se préserver de tout vol de technologies.

¹⁰ Executive Order No. 14209, Pausing Foreign Corrupt Practices Act Enforcement to Further American Economic and National Security, (Feb. 10 2025).

La France se place comme le deuxième pays exportateur en matière d'armement sur la période de 2020 à 2024 avec 9,6% des exportations mondiales¹¹. Cette donnée témoigne du savoir-faire de la BITD mais aussi de la nécessité de protéger cela. De ce fait, la France a mis en place par le biais de sa législation un contrôle des exportations de sa technologie. Ce contrôle répond à une triple nécessité, d'une part veiller à la sécurité nationale en garantissant la protection de nos forces et alliés engagés en opération, une sécurité économique et industrielle visant à assurer la maîtrise et le suivi du transfert de technologies sensibles. Et enfin une sécurité politique et juridique se traduisant par la garantie du respect des engagements internationaux souscrits par la France.

En France, ce contrôle est fondé sur les principes de prohibition, sauf dérogation de l'Etat au regard des articles L.2335-1 à L.2335-9¹² du code de défense. Cette dérogation passe par une demande d'autorisation d'exportation à l'administration, la licence, mise depuis le 4 juin 2014. Cette demande faite par les industriels de défense est ensuite analysée par les opérateurs de la Direction Générale de l'Armement qui rendent un avis. Si besoin d'approfondissement, la demande passera en commission interministérielle pour l'étude des exportations de matériels de guerre (CIEEMG).

Ce contrôle des exportations se présente de deux manières, d'une part celui pour le matériel de guerre et assimilé, et d'autre part celui pour les biens à double usage. Pour ce faire, la France s'est fondée sur l'arrangement de Wassenaar, conclu en juillet 1996 et regroupant actuellement 42 États, complété par un règlement communautaire européen¹³. Cette uniformisation du droit européen permet d'obtenir une harmonie et une mesure de protection globale du savoir-faire, que chaque État peut ensuite moduler.

Si le droit français en matière de contrôle des exportations n'apporte que peu de contraintes pour les pays importateurs, clause de End User Certificat et de Non Retransfert, d'autres pays comme les USA se sont dotés d'un droit en la matière beaucoup plus contraignant. Par le biais de sa réglementation ITAR (International Traffic in Arms Regulations) et EAR (Export Administration Regulations), les USA imposent un contrôle strict des exportations, transfert et utilisation de leurs technologies. Toute entreprise, qu'elle soit étrangère ou bien américaine, manipulant des composants ou données d'origine américaine doit obtenir des autorisations de l'administration américaine pour son utilisation ou sont retransfert, sous peine de lourdes sanctions. Ces procédures sont extrêmement lourdes pour les entreprises et leur imposent un fort devoir de vigilance. De nombreuses technologies sont donc soumises à une dépendance américaine et viennent fortement compromettre la souveraineté industrielle des pays partenaires comme en témoigne l'avion de combat F-35.

Si les USA ont pendant longtemps été le seul pays avec une législation très contraignante, récemment, la Chine avec sa nouvelle politique export control sur ses terres rares suit le même chemin. Une liste de métaux présents dans ses sols a été éditée, avec un seuil de minimis très bas, forçant ainsi une demande d'autorisation d'exportation à l'administration chinoise à toute entité souhaitant exporter un bien en comportant. La Chine passe ainsi d'une simple politique de contrôle, à une politique stratégique de contrôle visant à verrouiller sa position dominante sur le marché et la traçabilité.

¹¹ SIPRI Arms Transfer Data Base - Pays exportateur d'arme dans le monde entre 2020 et 2024

¹² Code de la défense, Article L2335-1 à L2335-9, version du 29 octobre 2025

¹³ Règlement CE n°428/2009, 5 mai 2009, instituant un régime communautaire de contrôle des exportations, des transferts, du courtage et du transit de biens à double usage

Pour se protéger et conformer face à des législations toujours plus restrictives et face à un contexte mondiale mouvant, les entreprises ont décidé de se doter de nouvelles fonction support, des chargés export control, qui auront pour rôle d'assurer la conformité de leurs entreprises, à la fois à leur réglementation nationale, mais également étrangères. Ces postes sont clés, tant pour la protection du savoir-faire de l'entreprise, que pour sa bonne conformité lui évitant des poursuites pénales ou la perte de partenaires / clients spécifiques.

La France va devoir continuer, par le biais de son administration et référent contrôles export des entreprises de la BITD, de rester informée et prête à pouvoir anticiper et adapter sa législation à ces nouvelles problématiques. La volonté d'une dés-ITAR-risation est également une solution à cette extraterritorialité américaine pour garantir la souveraineté française et à plus grande échelle, européenne.

RECOMMANDATIONS

Il est important pour la France de continuer ses efforts dans sa mise en œuvre du contrôle des exportations. Que ce soit pour son savoir-faire industriel en actualisant sa législation et en conservant la rigueur et la performance des processus de contrôles actuellement mises en place.

Il est également important que les acteurs de la BITD française poursuivent leurs efforts d'information et de mise en conformité vis-à-vis des législations étrangères contraignantes, US et chinoise, afin d'éviter le risque de lourdes sanctions économiques, mais également une profonde ingérence étrangères.

Après ces deux cas emblématiques d'ingérence économique et sectorielle, il convient d'observer le rapport de force plus diffus qui s'exerce dans le commerce international.

C. Mesures de rétorsion agressives : droits de douane US, coordination UE-US et règlement de blocage

Face aux ingérences économiques et à l'extension extraterritoriale de certaines législations étrangères, l'Union européenne (UE) peut combiner des rétorsions tarifaires coordonnées avec les Etats-Unis lorsqu'il existe une convergence d'intérêts, et des outils autonomes visant à protéger ses opérateurs et à dissuader la coercition économique. Cette approche s'appuie sur le règlement de blocage (CE) n°2271/96¹⁴, qui neutralise dans l'ordre juridique de l'UE les effets de lois extraterritoriales désignées¹⁵, et sur des instruments offensifs de contre-coercition¹⁶ et renforcement commercial¹⁷. Dans la doctrine, Charlotte Beaucillon montre que les « *secondary sanctions* »¹⁸ visent des acteurs non soumis à la juridiction territoriale

¹⁴ Règlement (CE) n° 2271/96 (Blocking Statute), 22 novembre 1996, JO L 309, p. 1–6, EUR-Lex

¹⁵ Règlement délégué (UE) 2018/1100 du 6 juin 2018 modifiant l'annexe du 2271/96 (mise à jour liée au JCPOA), JO L 199 I, 7.8.2018.

¹⁶ Règlement (UE) 2023/2675 (Instrument anti-coercition), 22 novembre 2023, JO L du 7.12.2023 (EUR-Lex).

¹⁷ Règlement (UE) n° 654/2014 (exercice/renforcement des droits commerciaux) et COM(2022) 74 exposant l'extension 2021 (couverture services/DPI) et l'usage en contexte de paralysie de l'Organe d'appel (EUR-Lex/Commission)

¹⁸ Charlotte Beaucillon, « *Secondary Sanctions — What's in a Name?* », in *The Cambridge Handbook of Secondary Sanctions and International Law*, Cambridge University Press, 2024.

de l'Etat qui les édicte, leur effectivité reposant sur des effets de réseau et des comportements de sur-conformité privés, autant de dynamiques que l'UE doit intégrer pour calibrer sa réponse.

« Entériner » des rétorsions tarifaires par des accords UE-US (cadre, TRQ, SnapBack)

Deux précédents récents démontrent qu'un accord politique UE-US peut stabiliser des rétorsions tout en conservant un levier. D'abord, le dossier Airbus-Boeing a été « gelé » le 15 juin 2021 par un cadre coopératif qui suspend pour cinq ans les surtaxes réciproques et organise une coopération technique, avec possibilité de réactiver des mesures en cas de rechute¹⁹. Ensuite, le 31 octobre 2021, les parties ont réglé le différend acier/aluminium (section 232) en remplaçant les droits de 25% par des contingents tarifaires (TRQ) fondés sur des volumes historiques, assortis d'un suivi conjoint et d'un chantier vers un arrangement global (carbone/surcapacités)²⁰. Ce format ménage ménage un instrument de rétorsion calibré, réversible et ajustable, si l'une des parties dévie.

Sur cette base, l'UE peut proposer un mécanisme de rétorsion coordonnée avec les Etats-Unis : listes sectorielles pré-notifiées (métaux critiques, techniques sensibles, biens à double usage), TRQ modulables, et clause de swap-back avec déclenchement synchronisé contre un tiers coercitifs. L'objectif est double : crédibiliser la menace en amont pour dissuader l'ingérence et réduire le forum shopping, tout en abaissant le coût politique d'une activation unilatérale.

Protéger et riposter à l'échelle européenne : le règlement de blocage et les outils offensifs.

Le règlement de blocage (CE n°2271/96)²¹ interdit aux personnes et entreprises relevant de la juridiction de l'UE de se conformer aux lois extraterritoriales listées en annexe, écarte dans l'UE la reconnaissance et l'exécution de décisions fondées sur ces lois et ouvre un droit à la réparation (claw-back) des préjudices subis ; son annexe a été mise en jour en 2018 à la suite du retrait américain du JCPOA. Sur le plan contentieux, l'arrêt CJUE Bank Mellî²² (21 déc 2021) précise l'office du juge : une rupture contractuelle motivée par la crainte de sanctions « secondaires » doit être spécifiquement motivée et proportionnée ; la charge de la preuve et le contrôle juridictionnel s'apprécient in concreto, offrant un mode d'emploi. Aux juridictions nationales et aux entreprises. Cet arrêt souligne l'importance d'un contrôle rigoureux par les juridictions nationales, qui doivent vérifier la proportionnalité et la motivation spécifique d'une rupture de contrat invoquant la crainte de sanctions secondaires. Cela garantit un équilibre entre protection des entreprises européennes et respect des contraintes internationales, évitant ainsi des mesures disproportionnées au risque d'entraver la sécurité juridique.

¹⁹ USTR – 15 juin 2021, « Joint U.S.–EU Cooperative Framework for Large Civil Aircraft » : suspension cinq ans des contre-mesures et cadre de coopération.

²⁰ USTR – 31 octobre 2021, « Joint U.S.–EU Statement on Trade in Steel and Aluminum » (TRQ, suivi conjoint, « arrangement global »).

²¹ Mettre note bas page règlement de blocage

²² CJUE (grande chambre), 21 décembre 2021, Bank Mellî Iran c. Telekom Deutschland, C-124/20, ECLI:EU:C:2021:1035 (texte EUR-Lex)

Pour compléter ce bouclier, l'UE s'est dotée d'outils offensifs. D'abord, l'instrument anti-coercition (ACI) (règlement 2023/2675) autorise, après constat d'un acte de coercition par un état tiers, une palette graduée de réponses (droits additionnels, quotas, restrictions d'accès aux marchés publics/IDE, licences, mesure sur services/DPI) avec réversibilité destinée à obtenir la cessation de la coercition²³. Ensuite, le règlement « enforcement » n° 654/2014), interprété et étendu en 2021 pour couvrir notamment les services et certains aspects de la propriété intellectuelle, permet d'imposer des contre-mesures lorsqu'une partie n'exécute pas une décision issue d'un mécanisme de règlement des différends (OMC/accord bilatéral), point crucial dans un contexte de paralysie de l'organe d'appel²⁴. Malgré son cadre robuste, le règlement de blocage souffre d'une application inégale entre États membres, d'une faible mobilisation judiciaire et d'une diffusion limitée auprès des opérateurs économiques. Les mécanismes de *claw-back* restent peu engagés, en raison notamment des coûts et complexités des procédures contentieuses.

Les rapports parlementaires (Assemblée nationale²⁵, Sénat) convergent pour recommander une montée en effectivité du blocage (usage du *claw-back* et non-reconnaissance), un meilleur soutien contentieux et l'activation coordonnée d'ACI/*Enforcement* pour passer de la protection à la dissuasion. Dans cette perspective, l'analyse de **Beaucillon** éclaire l'articulation entre droit et puissance : au-delà du texte, c'est en **réduisant l'over-compliance** et en **élevant le coût anticipé** de la coercition (via ACI/*Enforcement*) que l'UE accroît l'effectivité de sa riposte.

RECOMMANDATIONS

Malgré un cadre juridique robuste, l'application du blocage demeure inégale entre États membres, avec peu de notifications ou de recours au *claw-back*. Plusieurs rapports parlementaires et évaluations de la Commission appellent à :

- Standardiser les pratiques de motivation des entreprises (modèle *Bank Mellî*) ;
- Clarifier les critères de l'article 5§2 (autorisation en cas de préjudice grave) ;
- Soutenir des contentieux pilotes pour activer le *claw-back* ;
- Créer des indicateurs de suivi (KPI), publiés dans les rapports annuels (article 7(a)).

Dans cette perspective, la véritable dissuasion ne réside pas uniquement dans les textes, mais dans la capacité à élever le coût anticipé de la coercition pour l'État émetteur. La combinaison du blocage, du soutien contentieux, et des leviers de rétorsion calibrés permettrait ainsi à l'UE de réduire la sur-conformité privée et de rétablir un espace autonome de décision pour ses opérateurs. (voir la bibliographie contenant les rapports parlementaires et évaluations de la Commission).

²³ Règlement (UE) 2023/2675 (Instrument anti-coercition), 22 novembre 2023, JO L du 7.12.2023 (EUR-Lex).

²⁴ Règlement (UE) n° 654/2014 (exercice/enforcement des droits commerciaux) et COM(2022) 74 exposant l'extension 2021 (couverture services/DPI) et l'usage en contexte de paralysie de l'Organe d'appel (EUR-Lex/Commission).

²⁵ Assemblée nationale – Rapport Gauvain (26 juin 2019), Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et mesures à portée extraterritoriale (Vie-publique, PDF) ; voir aussi les travaux du Sénat (mission « Souveraineté économique », 2022–2023)

Les rétorsions douanières relèvent d'une logique de confrontation directe entre les États. À l'inverse, les mesures antidumping s'inscrivent dans une logique de correction économique, visant non pas à sanctionner un État, mais à rétablir des conditions de concurrence équitables sur le marché européen.

D. Dumping extra-européen

Lorsqu'un pays exporte des produits à un coût inférieur à celui des producteurs locaux, il gagne rapidement des parts de marché à l'étranger. Si ce phénomène se prolonge, l'industrie locale peut être évincée, entraînant une dépendance aux importations. Une fois la position dominante établie, l'exportateur est en mesure d'imposer ses standards et d'exercer des pressions économiques ou politiques. L'exemple de l'acier chinois, dont les prix ont longtemps été maintenus artificiellement bas, a conduit à la fermeture ou à la fragilisation de plusieurs aciéries européennes, illustrant comment l'inondation d'un marché étranger peut affaiblir durablement une filière et entraîner une perte de souveraineté.

Dans le cas du dumping, on observe un écart entre le prix intérieur et le prix d'exportation, pouvant aller jusqu'à une vente à perte. Une entreprise ne peut maintenir durablement de tels prix sans soutien financier. C'est pourquoi le dumping est généralement associé à des aides d'État, qui compensent les pertes et permettent de proposer des prix artificiellement bas. Ce soutien peut prendre la forme de subventions directes, de crédits publics, d'avantages fiscaux ou d'un accès facilité aux matières premières. Il en résulte une concurrence faussée au détriment des producteurs du pays importateur.

L'OMC autorise les États à adopter des mesures antidumping pour corriger ces distorsions et préserver la libre concurrence.²⁶ Le dumping n'est donc pas illégal en soi : ce sont ses effets sur le marché importateur qui sont visés. Les mesures antidumping n'ont pas pour objet de sanctionner un exportateur, mais de restaurer l'équilibre concurrentiel de l'importateur.

Au sein du marché intérieur européen, les pratiques permettant le dumping sont neutralisées. Les aides d'État peuvent soutenir l'innovation ou des secteurs stratégiques, mais ne peuvent pas servir à évincer des concurrents européens.²⁷ En revanche, vendre moins cher à l'exportation n'est pas interdit en soi, puisque l'OMC ne prohibe pas la pratique : elle permet simplement aux pays qui en sont la cible de se défendre. L'Union européenne a d'ailleurs déjà utilisé ce levier, notamment dans les années 1990 avec la PAC, lorsque des surplus agricoles subventionnés étaient écoulés à bas prix en Afrique. Les réformes successives ont cependant encadré ces pratiques, qui sont aujourd'hui exceptionnelles et sanctionnées. Contrairement à des puissances comme la Chine, la Russie ou l'Inde, l'UE n'emploie plus le dumping comme outil stratégique, ce qui la place désormais davantage en position de défense que d'initiative.

Dans ce contexte, l'Union européenne met en œuvre ses instruments antidumping conformément aux règles de l'OMC. Une enquête peut être ouverte lorsque l'industrie européenne ou les autorités d'un État membre démontrent à la fois un prix d'importation inférieur au prix domestique du pays exportateur et un préjudice

²⁶ OMC, *Agreement on Implementation of Article VI of the GATT 1994 (Anti-Dumping Agreement)*, 1994.

²⁷ *Article 107 TFUE, JO C 202, 7 juin 2016.*

pour le secteur européen concerné. La Commission peut alors imposer des droits provisoires, puis, si le dumping est confirmé, des mesures définitives pour une durée de cinq ans.

Ainsi, si l'Union européenne ne pratique plus le dumping, elle en est aujourd'hui l'une des principales cibles, et souhaite renforcer ses mécanismes de protection pour en limiter les effets.²⁸ La tendance se renforce. En 2024, l'UE a annoncé un niveau record de 199 mesures de défense commerciale et 33 nouvelles enquêtes, principalement dans l'acier, secteur devenu emblématique des tensions de concurrence mondiale.²⁹ Elle modernise également son dispositif, avec l'enregistrement automatique des importations, l'extension de la surveillance à d'autres secteurs et l'allègement des procédures pour réagir plus rapidement.³⁰

Ce type d'ingérence commerciale représente 86 % des mesures de défense commerciale adoptées par l'Union européenne en 2023, les autres instruments portant principalement sur les subventions étrangères, les mesures de sauvegarde et le contrôle des investissements.³¹ Cette politique s'inscrit dans une logique de protection préventive des filières vulnérables. Ses effets sont visibles : le nombre d'emplois protégés est passé d'environ 500 000 fin 2023 à plus de 625 000 en décembre 2024, dont plus de 115 000 dans le secteur des véhicules électriques.³²

Ces contre-mesures à l'importation ne sont pas sans conséquences sur l'économie et la politique en Europe. Elles s'inscrivent dans un mouvement global de durcissement du commerce international, où les grandes puissances cherchent à protéger leurs industries stratégiques. Aux États-Unis, par exemple, le Department of Commerce a renforcé en mars 2024 l'application des lois antidumping (ADD) et antisubventions (CVD), montrant que la défense commerciale n'est plus perçue comme une mesure exceptionnelle, mais comme un instrument structurel de politique industrielle.³³ Dans ce contexte, l'UE n'agit pas isolément : ses mesures entraînent des tensions géopolitiques croissantes, particulièrement avec la Chine. Lorsque l'UE impose des droits sur les véhicules électriques chinois, Pékin réplique en ouvrant des enquêtes anti-dumping sur des produits européens comme le cognac ou la viande porcine et adopte des mesures miroirs.³⁴

La préservation de secteurs stratégiques comme l'acier ou les véhicules électriques ne se fait donc pas sans contreparties. En protégeant certaines filières clés, l'UE expose indirectement d'autres secteurs plus dépendants des exportations, qui deviennent alors des cibles privilégiées de rétorsion. Il s'agit de vases communicants : renforcer la souveraineté industrielle implique d'accepter un durcissement du rapport de force commercial, reflet d'un commerce mondial devenu plus politique que strictement économique.

²⁸ DG TRADE, communication interne sur l'évolution de la Trade Defence Toolbox, 2024.

²⁹ Commission européenne, Commission launches record number of trade defence investigations in 2024, Communiqué de presse, Bruxelles, 28 juillet 2025.

³⁰ Décision d'exécution du 15 octobre 2024 (Journal officiel à paraître).

³¹ Commission européenne, EU trade defence measures in force – Annual Statistics 2023, Communiqué de presse IP/24/4829, Bruxelles, 17 juin 2024.

³² Commission européenne, Trade Defence: Measures and impact on employment, DG TRADE, Bruxelles, 2024.

³³ U.S. Department of Commerce, Strengthening Enforcement of Antidumping and Countervailing Duty Laws, Federal Register Notice, mars 2024.

³⁴ MOFCOM, Notice of Anti-Dumping Investigation on Brandy Imported from the European Union, Annonce officielle, Pékin, 5 janvier 2024.

RECOMMANDATIONS

Maintenir un dispositif de défense commerciale robuste et poursuivre les efforts engagés pour en perfectionner les modalités d'application (meilleur suivi des importations, réactivité accrue, transparence des aides étrangères).

Toutefois, ces mesures entraînent des rétorsions ciblées de la part des États tiers, il est essentiel de concentrer prioritairement la protection sur les secteurs où une souveraineté est nécessaire (acier, énergie, technologies de transition, véhicules électriques), plutôt que d'élargir le champ des enquêtes. Une stratégie trop extensive risquerait de diluer l'efficacité du dispositif et d'alimenter une escalade commerciale préjudiciable à d'autres filières exportatrices européennes.

L'enjeu est donc de protéger sans se disperser, en privilégiant une approche ciblée, proportionnée et stratégique.

La défense commerciale permet de répondre aux ingérences qui visent les flux de marchandises et les conditions de concurrence. Mais l'affaiblissement d'un acteur ne passe pas toujours par les prix ou l'accès au marché : il peut aussi viser **les capacités productives elles-mêmes**. Lorsque la pression se déplace vers l'entreprise, l'enjeu n'est plus la concurrence, mais **la captation**. D'où la nécessité d'examiner désormais **les dispositifs de protection des actifs stratégiques : investissements, contrôle des acquisitions et lutte contre l'espionnage industriel**.

II. Face aux politiques étrangères de captation, des instruments de contrôle des investissements et un contre-renseignement économique et industriel à améliorer

Face à la montée des stratégies de captation étrangères, qu'elles prennent la forme d'acquisitions ciblées, de prises de participation insidieuses, la France et l'Union européenne ont progressivement pris conscience de la nécessité de protéger leur patrimoine économique et technologique national. Loin d'être une question purement financière, le contrôle des investissements, la sécurisation des savoir-faire et la protection du renseignement économique constituent désormais des piliers essentiels de la souveraineté nationale, dans un contexte de rivalités économiques exacerbées notamment par les cyberattaques en hausse constante.

A. Un instrument en constante amélioration : le contrôle des investissements entrants et sortants

Au cœur des opérations agressives de captation du patrimoine économique national, le contrôle des investissements, entrants et sortants de France, constitue un instrument clé, à la main de la puissance publique. Remis sur le devant de la scène durant l'affaire Alstom et par l'activisme du Ministre de l'Economie,

Arnaud Montebourg, le dispositif de contrôle des investissements étrangers en France a depuis connu une consécration, par l'extension de son champ d'application.

Initialement institué par une loi de 1966 sous le gouvernement Pompidou, le dispositif de contrôle des investissements étrangers en France (IEF) visait à préserver les secteurs stratégiques de la mainmise d'intérêts extérieurs. Ce mécanisme fut cependant amoindri en 1996, avec l'introduction d'un principe d'autorisation quasi automatique, adopté au nom de la liberté de circulation des capitaux étrangers. Un tournant s'opère en 2005, sous le gouvernement de Dominique de Villepin, avec la création – par décret intégré au Code monétaire et financier – d'un dispositif ciblé de contrôle des investissements. Ce texte restreignait les participations étrangères dans des domaines jugés sensibles, tels que la sécurité privée, la lutte contre le terrorisme, les activités d'écoute et de sécurité des technologies de l'information, ou encore l'armement. Le décret du 14 mai 2014, dit « *décret Montebourg* »³⁵, est venu renforcer ce cadre, en élargissant le périmètre du contrôle des investissements étrangers par le Ministère de l'Economie aux activités de santé, de transports, de télécommunications mais aussi d'approvisionnement en eau et en énergie³⁶.

Deux dynamiques ont ensuite transformé en profondeur le champ d'application de ce précieux instrument dont dispose Bercy. D'une part, le Ministère de l'Economie n'aura de cesse, en 2019, puis 2020 et 2021, d'allonger la liste des secteurs d'activité listés à l'article L.151-3 du Code monétaire et financier, et concernés par les contrôles (cybersécurité, spatial, IA, robotique, stockage d'énergie, quantiques, presse en ligne). En parallèle, le Ministère a également augmenté le nombre de contrôles réalisés, en abaissant le seuil de participation contrôlée de 33,3% à 25 puis 10% pour les investissements non-européens, via la loi PACTE de 2019. En 2023, 255 décisions ont été rendues par le bureau de contrôle, autorisant seulement 135 prises de participation, dont 60 sont assorties de conditions.

Ainsi, la procédure de contrôle des investissements étrangers en France constitue un instrument, petit à petit, renforcé, efficace, dissuasif, s'inscrivant dans un renforcement européen de la législation.

Adopté en 2019, le règlement (UE) 2019/452³⁷ instaure un cadre européen commun de filtrage des investissements directs étrangers, face à des vulnérabilités identifiées, certains Etats étant protecteurs et d'autres permissifs. Il permet une coopération et un échange d'informations entre les Etats membres et la Commission européenne concernant les investissements dans des secteurs stratégiques (technologies critiques, infrastructures, défense, etc.). Chaque Etat conserve sa propre compétence pour filtrer les investissements, la Commission disposant d'un rôle consultatif. Ce dispositif vise à prévenir les prises de contrôle étrangères susceptibles de menacer la souveraineté économique européenne. La France, l'Italie et l'Allemagne se distinguent par leur activisme quant au contrôle de ces investissements, notamment en 2020-2021 au plus fort de la crise Covid. Depuis 2022, ce ne sont pas moins de 1 300 investissements qui furent contrôlés.

En miroir, l'Union européenne cherche à créer un cadre juridique lié aux investissements européens sortants. L'Union ne dispose pas d'une législation harmonisée en la matière, la France étant par exemple encore centrée

³⁵ Décret n° 2014-479 du 14 mai 2014 relatif aux investissements étrangers soumis à autorisation préalable.

³⁶ Portail de l'Intelligence économique, *Le décret Montebourg, entre héritage protectionniste et nouveau permanent*, Club Droit, 16/01/2025.

³⁷ Journal officiel de l'UE, Règlement (UE) 2019/452 du Parlement européen et du Conseil du 19 mars 2019 établissant un cadre pour le filtrage des investissements directs étrangers dans l'Union.

sur le contrôle des investissements sortants. Suite à la parution d'un livre blanc sur le sujet, l'Union a adopté la Recommandation (UE) 2025/63, non-contraignante, invitant les États membres à créer des mécanismes de filtrage des investissements sortants dans des secteurs sensibles tels que les semi-conducteurs, l'intelligence artificielle et les technologies quantiques. Les États ont jusqu'au 30 juin 2026 pour rendre compte des progrès réalisés en la matière, et d'émettre des propositions pour adopter un cadre européen ambitieux et harmonisé.

Par ailleurs, la loi SAPIN II, votée en 2016, renforça l'encadrement juridique des investissements étrangers en France, en imposant à toutes les entreprises françaises d'identifier et déclarer leurs bénéficiaires effectifs afin d'empêcher certains détenteurs de capitaux d'avancer masqués derrière des holdings ou sociétés écrans. De plus, la création de l'Agence Française Anticorruption (AFA) permet de renforcer le cadre légal dissuasif sur les risques de captations de patrimoine, de corruption ou blanchiment, en améliorant les moyens de vigilance financière de l'État. Par ailleurs, cette loi a permis de créer un cadre de coopération renforcé et salué entre le Ministère, l'AFA, la Direction générale du Trésor et Tracfin.

RECOMMANDATION

Dès lors, il convient de soutenir un règlement européen ambitieux sur les investissements sortants listant les pays et les secteurs stratégiques à risque, devant faire l'objet de contrôle renforcé. Par ailleurs, la France doit être précurseur, et ne pas attendre le règlement européen qui n'advient pas avant 2027 avec une application à l'horizon 2028. Cela passe par la création, par décret, d'un dispositif rattaché à la Direction Générale du Trésor. La difficulté résidera dans l'établissement d'un mécanisme de notification volontaire, prenant en compte les lourdeurs administratives et les risques pour leurs investissements.

Ainsi, si la prise de contrôle d'une partie ou de l'intégralité d'une entreprise stratégique constitue un élément de déstabilisation, au détriment de notre souveraineté, les vols d'informations ciblées et l'espionnage industriel constituent un risque réel.

Toutefois, la captation ne passe pas toujours par la prise de participation capitalistique : lorsqu'une information stratégique seule suffit, c'est la voie de l'espionnage industriel qui devient le principal vecteur d'ingérence.

B. La protection du patrimoine informationnel privé : une lutte contre l'espionnage économique

Face à la montée des menaces d'espionnage industriel et de sabotage orchestrées par des puissances étrangères, la France soucieuse, a progressivement pris conscience de la nécessité de défendre son patrimoine immatériel. Dans une logique de protection de sa souveraineté économique et juridique, elle a mis en place un arsenal législatif destiné à sécuriser ses données stratégiques et son savoir-faire national. Cette démarche s'est traduite par plusieurs jalons majeurs tels que la loi de blocage de 1968, la loi Hamon en 2014 et plus récemment, la loi sur le secret des affaires.

La genèse du lawfare défensif français : la loi de blocage de 1968

L'un des premiers dispositifs français de protection contre les ingérences juridiques étrangères a été la loi dite « de blocage »³⁸. Elle s'inscrit dans une réponse directe à l'ingérence croissante du droit extraterritorial américain, dont les effets se traduisent par une extension de la compétence des juridictions et autorités américaines. Toute entité recourant au dollar américain, exerçant une activité sur le sol des États-Unis ou disposant d'une filiale de droit américain est susceptible d'en être la cible.

Révisée à plusieurs reprises³⁹ dans un souci d'adaptation à l'ère de la compliance et du numérique, elle permet d'empêcher le transfert direct d'informations économiques stratégiques d'une entreprise française à des autorités étrangères, notamment dans le cadre de contentieux ou d'enquêtes et de répondre à des discovery orders étrangers sans passer par la Commission des sanctions économiques du ministère de l'Économie (SISSE/MEFSIN). La Direction générale du Trésor, le SGDSN et le SISSE assurent quant à eux la veille, la coordination et la diffusion de consignes de conformité. Entre les années 1980 et 2000, la France a redécouvert cette loi comme un instrument de contre-lawfare et de protection de sa souveraineté informationnelle ; suite à la montée en puissance d'ingérences économiques américaines sous couvert de droit⁴⁰. Ce phénomène a engendré plusieurs affaires emblématiques⁴¹ et surtout la consécration de la loi Sapin II⁴².

Si la loi de blocage reste un arsenal juridique pertinent pour préserver la compétence exclusive du droit français pour la transmission d'informations stratégiques, elle se heurte malgré tout à des limites : les entreprises, craignant davantage les sanctions américaines (amendes du DOJ) que les sanctions françaises (faibles et rarement appliquées à cette période), couplé au manque de coordination entre l'État, la justice et le secteur privé ainsi que la mondialisation des flux numériques (clouds américains, données délocalisées) ; empêchent de rendre son applicabilité dissuasive.

Pendant que la loi de blocage peine à s'affirmer, les entreprises françaises et européennes souhaitent, coûte que coûte, assurer leur place sur le marché concurrentiel. L'affaire Laguiole, entre autres, déclenche une conscientisation à l'échelle communautaire en matière de protection du savoir-faire.

Laguiole ou l'éveil d'un savoir-faire français menacé

La prise de conscience d'une énième forme de guerre par le droit s'est ancrée en matière de défense du savoir-faire national. Dans les années 1990-2000, le constat de détournement des marques ou de la non-protection des indications géographiques (IG) à des fins d'ingérence économique survient avec l'affaire Laguiole. Le dépôt abusif de la marque "Laguiole", fleuron du savoir-faire français, par Gilbert Szajner a permis la

³⁸ Loi n°68-678 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères

³⁹ Jusque-là jugée trop symbolique, le décret du 9 décembre 2019 et la loi du 22 décembre 2022 ont cherché à rendre la loi opérationnelle au travers notamment de la création d'un point de contact national (au MEFSIN), la clarification de la procédure de notification et la possibilité d'un dialogue stratégique avec le parquet national financier (PNF).

⁴⁰ Le Foreign Corrupt Practices Act (FCPA, 1977), le Patriot Act (2001), le Cloud Act (2018), et les sanctions économiques de l'OFAC.

⁴¹ Voir les affaires Alstom, BNP Paribas, Total...

⁴² Les apports conséquents de la loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, soit la mise en oeuvre d'obligations de démarches et procédures pour les entreprises ou encore la protection renforcée des lanceurs d'alerte place la France en tête de fil au niveau des standards internationaux.

commercialisation, en France comme à l'étranger, de divers types de produits sans lien avec le territoire ni la coutellerie artisanale locale.

Le gouffre juridique de l'époque, longtemps préjudiciable à la réputation territoriale, laissait le champ libre à l'exploitation commerciale abusive, au détournement de la réputation et à la dilution économique du tissu productif local. En invoquant une atteinte à son nom, son image et sa réputation, s'ensuit une bataille juridique houleuse autour de l'utilisation de l'appellation géographique "Laguiole" (patrimoine immatériel régional) et sa commercialisation (propriété industrielle). Dans le sillage de la stratégie française de *lawfare* défensive, cette affaire a joué un véritable rôle de catalyseur législatif, aussi bien en France qu'en Europe.

Après deux décennies de contentieux et de pressions médiatiques, la France, puis le droit communautaire, se sont dotés d'un faisceau de mécanismes coercitifs pour préserver le contrôle du nom, du savoir-faire des acteurs locaux et - *a fortiori* - l'image de qualité et de prestige de la France et de ses territoires à l'étranger. C'est alors en 2014 que la France s'est dotée d'un outil majeur de soft power français : la "loi Hamon", qui étend la protection d'indication géographique (IG) des produits agricoles et alimentaires (IGP et AOP) aux produits artisanaux et manufacturés ; créant la notion d'Indications Géographiques pour Produits Industriels et Artisanaux (IGPIA)⁴³.

A cela, s'ajoutent d'autres contre-mesures défensives comme le droit d'alerte pour les collectivités⁴⁴, la procédure d'opposition devant l'INPI et l'EUIPO ou encore le recours pour pratiques commerciales trompeuses⁴⁵. Ces outils permettent aux collectivités, syndicats et groupements d'artisans de défendre collectivement leurs intérêts immatériels et de neutraliser les tentatives de captation économique ou d'usurpation de réputation.

A l'échelle européenne, la CJUE a réaffirmé la protection stricte des IGP contre toute appropriation illicite. Cette stratégie d'inscription du patrimoine industriel dans les priorités de souveraineté juridique de la France a conduit l'Union européenne, à son tour, à revoir sa défense européenne face à la dissipation de son patrimoine immatériel en adoptant le Règlement UE 2025/1759. Son entrée en vigueur en décembre 2025 engendrera une harmonisation de la protection des IG artisanales et industrielles sur l'ensemble du territoire européen. Bien que la convergence des politiques française et européenne reste une avancée majeure, elle restera confrontée à des défis de gouvernance et d'efficacité opérationnelle.

Alors que l'affaire Laguiole illustre la protection concrète du savoir-faire, la loi sur le secret des affaires élargit ce dispositif à l'ensemble des informations stratégiques des entreprises.

⁴³ L'enregistrement d'une IGPIA auprès de l'INPI entend placer entre les mains des producteurs le contrôle de la dénomination de leur territoire et de leur savoir-faire associé contre la captation étrangère (les contrefaçons et importations de Chine et du Pakistan notamment), tout en offrant une garantie de qualité et de traçabilité aux consommateurs sur l'origine géographique, le nom, la qualité, et la notoriété des produits issus de savoir-faire locaux.

⁴⁴ CPI., art., L.712-2-1.

⁴⁵ C. consom., articles L.121-1 et suivants.

La loi sur le secret des affaires : une réponse française à la guerre invisible de l'information

Dès les années 1980, les États-Unis ont saisi l'importance stratégique tant sur le plan politique, juridique et économique de l'espionnage industriel et numérique visant les entreprises privées. Le *Computer Fraud and Abuse Act*⁴⁶ de 1986 a constitué une réponse précoce et efficace à ces menaces, en instituant des sanctions pénales et civiles contre tout accès non autorisé à un système informatique dans le but d'obtenir une information confidentielle ou à accès restreint⁴⁷.

En outre, les États-Unis ont développé un ensemble de législations destinées à assurer la préservation des secrets d'affaires publics et privés. Contrairement à la vision française, ils ont adopté une approche unifiée du secret économique, ne distinguant pas entre les secrets liés aux intérêts fondamentaux de l'État et ceux protégeant les intérêts des entreprises : c'est ainsi qu'après l'entrée en vigueur de l'*Espionage Economic Act*⁴⁸ en 1996 pour sanctionner le vol de secrets technologiques et commerciaux (notamment au profit de puissances étrangères) ; les États-Unis cherchent à unifier la protection sur le territoire américain. Trente ans plus tard, le *Defend Trade Secrets Act*⁴⁹ est adopté afin de protéger toute information à valeur économique, aussi larges soient-elles.

Au-delà de l'objectif de protection du secret des affaires des deux lois américaines extraterritoriales précitées, celles-ci englobent un large spectre d'informations économiques souhaitant être gardées discrètes par les entreprises états-uniennes : à cet effet, toute information publique gardée secrète par son détenteur et présentant une valeur économique (couvrant aussi bien les informations financières, économiques et commerciales que les données techniques ou industrielles) ; sont protégées. Depuis, les États-Unis détiennent un levier de puissance juridique conséquent face aux actes d'espionnage commis pour un gouvernement, une organisation ou un agent étranger par le biais de sanctions aggravées ; comprenant aussi toute captation volontaire et non autorisée d'un secret d'affaires, qu'il soit stratégique ou non. En ce sens, ces lois, ayant une portée et une influence internationale, renforcent la sécurité économique du pays à l'échelle mondiale. Du côté européen, les entreprises cherchent à s'armer de façon similaire : pour ce faire, celles-ci accroissent leurs mesures internes de protection (cybersécurité, formation, contrôle d'accès..) et les institutions européennes cherchent à intensifier leur coopération internationale pour lutter contre l'espionnage économique. Quant à la France, celle-ci a cherché une protection plus large et répressive par la loi du 30 juillet 2018 relative à la

⁴⁶ *Computer Fraud and Abuse Act*, art. 18 U.S.C. § 1030.

⁴⁷ À savoir qu'à la même période, le dispositif français de protection des affaires reposait seulement sur la protection du secret de fabrication et quelques décisions jurisprudentielles relatives à la concurrence déloyale.

⁴⁸ L'*Economic Espionage Act (EEA)*, adopté le 11 octobre 1996, vise à protéger les entreprises américaines contre le vol de secrets d'affaires. Il définit ceux-ci comme toute information non publique, confidentielle et à valeur économique, qu'elle soit technique, industrielle, financière ou commerciale. La loi réprime toute appropriation délibérée de ces informations, avec des sanctions aggravées en cas d'implication étrangère, et prévoit une application extraterritoriale dès lors qu'un lien existe avec le territoire ou les ressortissants américains.

⁴⁹ Le *Defend Trade Secrets Act (DTSA)*, adopté aux États-Unis en 2016, protège toute information à valeur économique, qu'elle soit financière, commerciale, scientifique, technique ou d'ingénierie. Cette protection, plus large que celle du droit français, vise le secret économique national et couvre aussi bien les données matérielles qu'immatérielles (plans, formules, procédés, codes, etc.). La valeur économique, fondée sur la rareté, la stratégie ou l'avantage concurrentiel, en constitue le cœur. Pour être protégé, le détenteur doit avoir pris des mesures raisonnables de confidentialité, faute de quoi aucune protection juridique n'est accordée.

protection du secret des affaires⁵⁰. Par ailleurs, la France et les États-Unis abordent le régime du secret des affaires de manière opposée⁵¹.

C'est ainsi sous l'influence des lois états-uniennes que le législateur français créé la loi n°2018-670 du 30 juillet 2018 relative à la protection du secret des affaires : transposé de la Directive UE 2016/943 du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites ; les nouvelles dispositions du Code de commerce⁵² intègrent un régime spécifique de protection du secret des affaires devant les juridictions civiles et commerciales. Celles-ci intéressent tous les types de contentieux, civils et commerciaux, à l'occasion desquels les secrets des affaires pourraient se trouver menacés, notamment dans les contentieux de contrefaçon et de concurrence déloyale. Par conséquent, la nouvelle loi engendre des effets novateurs sur la protection des informations économiques sensibles : grâce à la souplesse du législateur, les dispositions du Code de commerce laissent une marge de manœuvre pour toute entreprise française usant du secret des affaires ; permettant ainsi la considération des diverses activités dans lesquelles l'information doit être protégée. De surcroît, la loi de 2018 permet une meilleure préservation légale du secret : elle permet désormais d'éviter une divulgation imprudente par la confidentialité et le droit à la communication des preuves durant les enquêtes et avant le procès⁵³. Par ailleurs, cette préservation est double : en plus d'assurer une meilleure protection de l'information pendant la phase préparatoire du procès, il est aussi possible (et surtout conseillé) d'assurer cette protection pendant le procès⁵⁴. De plus, toute personne ayant accès à ces informations est tenue à une obligation de confidentialité, consolidant la confiance des entreprises envers la justice civile⁵⁵.

RECOMMANDATIONS

Une coordination européenne ajustée du Règlement UE 2023/2411 sur les IGPIA et d'une future "EU Blocking Statute renforcée".

Investir dans des outils de traçabilité, de certification numérique, de veille et d'opposition aux dépôts de marques, brevets et noms de domaines abusifs.

⁵⁰ Loi n° 2018-670 du 30 juillet 2018 relative à la protection du secret des affaires.

⁵¹ En France, le Secret est appréhendé selon une logique descendante (top-down) : la protection s'est d'abord construite autour des secrets d'État, avant d'être progressivement étendue à la sphère privée, sans toutefois consacrer en droit pénal une véritable notion autonome de secret d'entreprise (L'article 410-1 du Code pénal français tente de prolonger la protection des secrets de l'État vers les entreprises, sans pour autant instaurer une véritable définition du secret d'entreprise) . À l'inverse, aux États-Unis, la conceptualisation du secret économique repose sur une approche ascendante (bottom-up), issue d'une vision plus libérale. Le modèle américain met donc en avant la protection des secrets d'affaires détenus par les entreprises, sans nécessairement s'appuyer sur une réelle législation cadre.

⁵² C.com., articles L.151-1 et suivants et R.152-1 et suivants ; ainsi que le titre (V), consacré à la protection du secret des affaires, introduit dans la partie réglementaire dudit Code.

⁵³ Les articles L.152-3 à L.152-5 du Code de commerce renforcent la protection du secret dès la phase préparatoire : le juge peut restreindre ou adapter l'accès aux documents confidentiels, garantissant ainsi un équilibre entre confidentialité, droit à la preuve et contradictoire. Il est à noter qu'avant la loi de 2018, l'article 145 du Code de procédure civile constituait un risque de révélation des secrets d'affaires avant le procès. A cet égard, le Juge devait limiter les mesures d'instruction aux seules informations pertinentes et proportionnées.

⁵⁴ Alors qu'avant 2018, l'absence de cadre juridique exposait encore les secrets à la publicité des audiences ou des jugements, poussant les entreprises vers l'arbitrage, plus confidentiel ; le juge peut désormais statuer en chambre du conseil, limiter la diffusion de pièces sensibles et adapter la motivation ou la publicité de sa décision.

⁵⁵ C. com., art. L.153-1.

Les entreprises doivent être sensibilisées et formées en interne sur le secret des affaires, la préservation du made in france et la captation d'informations stratégiques.

Le législateur a mis en place des régimes pour protéger le savoir-faire des entreprises des captations extérieures. L'économie française a également en soutien les services de renseignement pour identifier ces menaces.

C. L'entrée en jeu du monde du renseignement à fins de prévention des ingérences économiques prenant la forme de captations indues.

Afin de protéger les données des captations indues, la France s'est dotée d'un arsenal législatif visant à empêcher les ingérences économiques de cette nature. Ces mesures passent notamment par un rôle des agences de renseignement dans ce domaine. Cette participation est bienvenue car cela montre que la France a pris conscience de la criticité de la menace. C'est ainsi que la loi du 24 juillet 2015 relative au renseignement énumère une liste exhaustive des intérêts de la Nation pouvant légalement autoriser les services de renseignement à recourir à des techniques de renseignement. Parmi les 7 finalités visées figurent à la 3^e place « les intérêts économiques, industriels et scientifiques majeurs de la France ».

Néanmoins, l'étude de celui-ci fait apparaître un double constat ; d'une part les mesures sont purement défensives (1) et d'autre part elles souffrent de lacunes (2).

Des mesures purement défensives⁵⁶

La loi de 2015 précédemment citée est bienvenue car elle concourt à une meilleure protection. Néanmoins, rien ne permet, dans la loi, aux agences de renseignement, de pouvoir recueillir des informations par le biais d'une technique de renseignement et d'en faire profiter les entreprises ce qui fait de ce dispositif un dispositif qui, certes a le mérite d'exister, mais reste purement défensif.

Ce rapprochement avec le monde militaire a également pris la forme de la création de zones à régime restrictif (ZRR). Ces zones ont été créées par le décret 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. Là encore, cette mesure juridique est purement défensive : il s'agit de créer des zones à régime restrictif sur le principe en vigueur au sein du MINARM qui distingue des zones à accès restreint, des zones protégées⁵⁷, des zones réservées ou encore des zones de défense hautement sensibles⁵⁸.

Les agences de renseignement viennent également en aide à certaines entreprises ; c'est le cas de la Direction du Renseignement et de la Sécurité de la Défense (DRSD) qui peut effectuer des audits au sein des entreprises et qui apporte son concours pour sensibiliser le personnel de ces entreprises. Néanmoins, la DRSD agit, là aussi, dans le volet de la protection. En aucun cas les sensibilisations ne comportent un volet offensif. Cela se justifie par le périmètre des missions de la DRSD. En effet, selon l'article D. 3126-7 du code de la défense qui prévoit

⁵⁶ Cf. A. JUILLET, *Le renseignement économique, Sécurité et stratégie* 2025/1 n° 38, pp. 13-16

⁵⁷ Cf. article R. 2362-1 à R. 2362-7 du Code de la défense

⁵⁸ Cf. articles. R.2363-1 à R 2363-7 du code de la défense

que « la DRSD participe à l'élaboration des mesures nécessaires à la protection du personnel, des informations, des matériels et des installations sensibles intéressant la défense et en contrôle l'application (...) ».

Un second acteur doit être cité : il s'agit de la Direction Générale de la Sécurité Intérieure dont l'une des 4 missions principales est la mission de protection économique⁵⁹. Cela prend notamment la forme d'édition de « flash », rapports d'une petite dizaine de pages qui a vocation à « accompagner (les entreprises) dans la diffusion d'une culture de sécurité interne »⁶⁰[7].

RECOMMANDATION

S'adosser aux agences de renseignement pour évoluer dans le champ offensif à l'instar de l'advocacy center américain qui mobilise les ressources d'agences américaines et notamment des agences de renseignement à fins de soutien aux entreprises américaines dans leurs opportunités commerciales à l'international.

Des dispositifs lacunaires

Outre le fait que les dispositifs examinés précédemment ne comportent aucun volet offensif, ils sont, de plus, lacunaires.

En effet, la création de ZRR est basée sur le volontariat. Par conséquent, si une structure ne possède pas de culture dans le domaine de la protection des données, elle ne verra pas l'utilité de mettre en place ce dispositif. Ces zones ont également fait l'objet de critiques : en premier lieu leur mise en place demande du temps car il faut respecter la procédure en vigueur. Il faut également prévoir la nécessité de dédier du personnel à la gestion des demandes d'accès aux ZRR.

Ensuite, il a été reproché à ces zones d'entraîner un contrôle sur les publications et les prises de paroles et d'imposer des restrictions « partout »⁶¹[9]. Certains chefs d'établissement préfèrent alors ne pas faire appel à ce dispositif ce qui peut s'avérer lourd de conséquence pour les données.

La DRSD, dans l'aide apportée aux entreprises souffre également d'un manque dans le domaine des ressources humaines. En effet, le personnel affecté à la DRSD n'est pas en nombre suffisant pour effectuer correctement les sensibilisations et, à l'instar du dispositif des ZRR, ce dispositif n'est basé sur le volontariat.

La situation est identique s'agissant du rôle de la DGSI.

RECOMMANDATION

Mettre en place des systèmes obligatoires et s'assurer de leur viabilité d'un point de vue financier et humain.

C'est une tautologie que de dire qu'aujourd'hui la majorité des données se trouve dans le cyberspace sous forme dématérialisée. On estime qu'à la fin de l'année le volume mondial de données digitales atteindra 181 zettaoctets soit l'équivalent de la capacité de stockage de plus de deux mille fois l'ensemble des données

⁵⁹ Cf. *L'action de la DGSI en matière de sécurité économique, Sécurité et stratégie 2025/1 n°38, pp. 10-12*

⁶⁰ Les bulletins sont disponibles sur le site de la DGSI.

⁶¹ Cf. *CGT, les zones à régime restrictif – fiche pratique et revendications, 17 avril 2025*

contenues dans toutes les bibliothèques du monde⁶². Il est donc impératif de mettre en place un cadre juridique robuste pour se prémunir des ingérences économiques qui prendraient la forme de cyberattaques.

D. Un arsenal juridique contre les cybermenaces bien pensé.

L'arsenal juridique qui vise le cyber est cohérent et complet puisque, si des instruments s'appliquent uniquement à certaines entreprises (1) d'autres ont un champ d'application plus large (2).

Les instruments propres à certaines entreprises.

En premier lieu, les entreprises évoluant dans les secteurs stratégiques sont soumises à des obligations particulières nées des arrêtés sectoriels pour le droit interne et de la transposition des directives NIS 1 et NIS 2 au niveau européen dans un second temps.

En France, l'article 22 de la loi de programmation militaire du 18 décembre 2013 est venu insérer dans le code de la défense, les articles Art. L. 1332-6-1 et suivants. Cet article vient définir la notion d'Opérateur d'Intérêt Vital et leur impose des règles relatives à la sécurité de leurs systèmes d'information d'intérêt vital par le biais d'arrêtés sectoriels. La France est ainsi l'un des tous premiers pays à s'appuyer sur la réglementation pour définir un dispositif efficace de cybersécurité de ces infrastructures critiques, c'est-à-dire indispensables au bon fonctionnement et à la survie de la Nation

Trois ans plus tard, l'Union européenne adopte la Directive NIS qui est basée sur la même philosophie. Les entreprises considérées comme Opérateur de Services Essentiels doivent mettre en place des mécanismes pour garantir la sécurité de leurs systèmes d'information. La différence tient au périmètre plus large de la notion d'OSE. Cette directive sera complétée en 2022 par la directive NIS2 qui impose à chaque État membre d'adopter une stratégie nationale en matière de cybersécurité, qui comprend des politiques de sécurité de la chaîne d'approvisionnement, de gestion des vulnérabilités et d'éducation et de sensibilisation à la cybersécurité. Les États membres doivent également établir et mettre à jour régulièrement une liste des opérateurs de services essentiels, en veillant à ce que ces entités respectent les exigences de la directive. De plus, outre les secteurs déjà couverts par la SRI 1, de nouvelles règles vont s'appliquer à de nouveaux acteurs

L'examen de ces dispositions fait donc apparaître des mécanismes juridiques bien adaptés. Néanmoins, la mise en place des règles de cybersécurité a un coût financier important pour les entreprises. De plus, leur interlocuteur en la matière est l'ANSSI. Or, cette agence n'est pas, d'un point de vue ressources humaines, dimensionnée correctement pour répondre efficacement à toutes les structures concernées par ce dispositif.

RECOMMANDATIONS

Prévoir des mécanismes d'aide financière pour les entreprises qui rencontreraient des difficultés de cette nature pour la mise en œuvre des obligations nées des directives NIS.

Doter l'ANSSI de ressources suffisantes pour appliquer efficacement les dispositions des directives NIS.

⁶² Cf. S. LABORDE-BALEN, *Big Data en 2025 : jusqu'où ira l'explosion des données mondiales ?*, Solutions numériques, fév 2025

En matière de stockage de données, il faut citer les entreprises qui manipulent des données de santé. En effet, l'article L. 1111-8 du code de la santé publique prévoit que « Toute personne physique ou morale qui héberge des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi médico-social pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil de ces données ou pour le compte du patient lui-même, doit être agréée ou certifiée à cet effet ». Néanmoins, la procédure de certification repose sur une évaluation de conformité au référentiel de certification. Cette conformité passe par un audit en deux étapes dont la première est la vérification de l'équivalence aux certifications ISO 27001 ou ISO 2000. Or, les normes ISO sont des normes héritées de la culture anglo-saxonne. Il y a donc une dépendance au monde anglo-saxon, même si elle est plus ténue.

Mais, et c'est un atout, l'arsenal législatif en la matière contient des normes qui s'appliquent à toute entreprise quelque soit son secteur.

Les instruments s'appliquant à l'ensemble des acteurs

Un aspect bienvenu est la prise en compte, au niveau européen de la nécessité de résilience : c'est l'enjeu du CRA. Le règlement sur la cyber résilience introduit des exigences obligatoires en matière de cybersécurité pour les fabricants et les détaillants, régissant la planification, la conception, le développement et la maintenance de ces produits. Ces obligations doivent être respectées à chaque étape de la chaîne de valeur. La loi oblige également les fabricants à fournir des soins pendant le cycle de vie de leurs produits. Certains produits critiques présentant un intérêt particulier pour la cybersécurité devront également faire l'objet d'une évaluation par un tiers par un organisme agréé avant d'être vendus sur le marché de l'UE.

Néanmoins, la question qui se pose est de savoir quels sont les tiers qui seront organisme agréé. Parce que dans ce domaine, force est de constater que les anglo-saxons ont la part belle (cf. ci-dessous).

Le document le plus abouti à notre sens reste le RGPD. En imposant un cadre strict quant à la donnée à caractère personnel tout au long de son cycle, collecte, stockage, utilisation, suppression, il offre un cadre protecteur aux données qui doit permettre de lutter contre les ingérences étrangères. Les problématiques de décision d'adéquation avec les USA notamment illustrent bien cette protection. Néanmoins dans les faits, rares sont les structures qui respectent à la lettre le RGPD, beaucoup tablant sur le fait que, eu égard au grand nombre de structures, la probabilité pour qu'ils se fassent contrôler est faible.

RECOMMANDATIONS

Développer les contrôles de la CNIL pour que les entreprises prennent conscience de l'impératif qu'elles ont de se mettre en cohérence avec le régime en place.

Enfin, un dernier instrument doit être cité : il s'agit de la déclaration qu'a émise la France à la fin des années 2010 concernant la lutte contre les cyberattaques et l'application du droit international appliqué à ce domaine⁶³[12].

Les dispositions dans ce domaine couvrent un large spectre puisque des textes ont été élaborés tant pour la protection des données à caractère personnel que pour faire face aux attaques de grande ampleur. Dans ce

⁶³ *CF. MINARM, Le droit international appliqué aux opérations dans le cyberspace, 2018.*

texte, la France affirme que « La France exerce sa souveraineté sur les systèmes d'information situés sur son territoire et met en œuvre les moyens nécessaires à la protection de cette souveraineté. En parallèle à un ensemble de mesures de sécurisation et de défense de ses systèmes, elle se réserve le droit de répondre à toute cyberattaque dont elle aurait été victime. Cette réponse peut aller jusqu'à l'utilisation de la force en fonction de la gravité de la cyber attaque »⁶⁴.

Par ce document, la France reconnaît indubitablement avoir une vision offensive. Cette vision a également fait l'objet d'une doctrine militaire de lutte informatique offensive⁶⁵. Dans ce document, le MINARM affirme que « les forces armées se dotent de l'ensemble du spectre des moyens de lutte informatique désormais nécessaires à la conduite des opérations : défensif, offensif et contre les manipulations de l'information nuisibles à nos opérations militaires ».

Si cet arsenal juridique permet de protéger les entreprises contre la captation directe de leur capital ou de leurs savoir-faire, il ne suffit pas à garantir la maîtrise des conditions économiques dans lesquelles elles évoluent. La vulnérabilité stratégique réside aussi dans les dépendances structurelles de l'économie européenne : accès aux ressources, technologies souveraines, chaînes de valeur et infrastructures critiques. Sur ces aspects la France doit s'améliorer : l'exemple du super ordinateur du MINARM, ASGARD, en est la preuve ; il a été conçu par Orange Cyberdéfense et par Hewlett Packard Entreprise, société américaine.

III. Dépendance structurelle : chaînes appro, énergie, standardisation US

L'économie européenne, bien qu'ancrée dans un modèle de libre-échange et d'interdépendance mondiale, se trouve confrontée à une dépendance structurelle vis-à-vis de puissances extérieures, au premier rang desquelles les États-Unis. Cette dépendance s'exprime à travers des dimensions multiples (technologique, juridique, énergétique) qui fragilisent son autonomie stratégique. Qu'il s'agisse du recours massif aux solutions cloud et aux services d'investigation américains (A), de la vulnérabilité des chaînes d'approvisionnement critiques (B), ou encore du déséquilibre énergétique né de la crise géopolitique récente (C), l'Union européenne voit sa compétitivité et sa capacité de décision durablement affectées. Cette partie s'attache ainsi à analyser ces fragilités systémiques, à interroger la réaffirmation de la souveraineté juridique européenne et à mesurer l'impact du facteur énergétique sur la performance économique du continent.

A. Les vulnérabilités dans les affaires transactionnelles : cloud, services juridique et d'investigation.

La France et l'UE demeurent exposées à une dépendance technologique et juridique qui fragilise leur autonomie de décision.

⁶⁴ Cf. document précité p. 6

⁶⁵ Cf. MINARM *Éléments publics de doctrine de lutte informatique offensive*, 2019

Cloud et données

Après l'échec des premiers "cloud souverains" exposant l'ensemble des acteurs économiques utilisant des services américains au Cloud Act et à la fuite de données sensibles, la stratégie française a basculé vers la recherche d'un "marché de confiance" fondé sur la certification SecNumCloud (ANSSI) avec localisation dans l'UE et maîtrise du droit applicable⁶⁶, et une doctrine d'usage de l'Etat (circulaire du 8 novembre 2018). En 2024, le Conseil d'Etat⁶⁷ a montré que le risque d'accès extraterritorial persiste (FISA/Section 702)⁶⁸ et mentionne le cas Health Data Hub⁶⁹ avec une injonction de clarifier le droit applicable et une recommandation de migration vers du SecNumCloud. Les projets Bleu, S3NS et le futur schéma européen EUCS sont cités par le Conseil d'Etat⁷⁰.

La certification EUCS⁷¹ vise à homogénéiser les "clouds de confiance" pour étendre cette protection à l'échelle européenne et éviter que les disparités nationales induisent la fuite du Cloud vers des acteurs hors-UE. En revanche, ce projet fait l'objet de pression et risque d'être dépossédé de nombreux critères. La CNIL recommande d'élever la condition d'un "recours à un prestataire exclusivement soumis au droit européen"⁷². De manière pratique, OVH préconise la généralisation de clauses "sur la localisation des données stockées" dans "tout appel d'offre public ou privé"⁷³.

Dépendance juridique (cabinets d'avocats et d'investigation "forensic")

Le rapport Gauvain (2019)⁷⁴ décrit la position de force des autorités américaines et de leurs pratiques transactionnelles (*Deferred Prosecution Agreements* et *Non Prosecution Agreements*) qui incitent à la coopération et créent une asymétrie procédurale pour les groupes non-américains, faisant face une "collusion organique, quasi-institutionnelle". De plus, la DPR 2023⁷⁵ recense les ingérences exploitant des opportunités juridiques liées à l'extraterritorialité, et alerte sur le risque de transferts d'informations critiques par des cabinets de conformité anglo-saxons au sein d'entreprises sensibles.

⁶⁶ Assemblée nationale, *La guerre économique*, Christophe Plassard, 18 juillet 2025, pages 65 à 67.

⁶⁷ Rapport du Conseil d'Etat, *La souveraineté*, 11 septembre 2024, p. 303.

⁶⁸ Section 702 of the Foreign Intelligence Surveillance Act (FISA).

⁶⁹ Délibération n° 2020-044 du 20 avril 2020 portant avis sur un projet d'arrêté complétant l'arrêté du 23 mars 2020 prescrivant les mesures d'organisation et de fonctionnement du système de santé nécessaires pour faire face à l'épidémie de covid-19 dans le cadre de l'état d'urgence sanitaire. CNIL.

⁷⁰ Rapport du Conseil d'Etat, *La souveraineté*, 11 septembre 2024, pages 305 et suivantes.

⁷¹ European Commission, *EU Cloud Certification Scheme*, 09 juin 2021.

⁷² CNIL, *Cloud : les risques d'une certification européenne permettant l'accès des autorités étrangères aux données sensibles*, 19 juillet 2024.

⁷³ Rapport Montaugé, 2019, pages 68 à 70, 145.

⁷⁴ Assemblée nationale, *Rapport d'information n° 4270 présenté par Raphaël Gauvain, Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et mesures à portée extraterritoriale*, Paris, juin 2019, page 15.

⁷⁵ Assemblée nationale, *Rapport public fait au nom de la délégation parlementaire au renseignement relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2022-2023*, 29 juin 2023, page 47.

La loi Sapin II et les CJIP ont relocalisé une partie des contentieux et réduit l'exposition à l'extraterritorialité US : co-conduite des dossiers Société Générale (2018) et Airbus (2020), avec 3,6 Md€ dont 2 Md€ en France pour Airbus ; le PNF devient partie prenante/leader⁷⁶. Cette dynamique répond aux alertes du rapport Gauvain sur l'asymétrie procédurale. De plus, des acteurs privés comme le Groupe ADIT, Forward Global et d'autres illustrent cette dynamique : ils permettent aux entreprises de conduire des enquêtes internes, des due diligences ou des audits conformes aux standards internationaux, sans transfert de données hors UE.

Ces structures contribuent à renforcer le "legal privilege" européen et à réduire l'exposition aux juridictions tierces.

L'absence de "géants" capables de répondre aux besoins

La politique européenne de la concurrence peut contrarier la consolidation industrielle : le Conseil d'Etat a rappelé en 2024⁷⁷ la tension structurelle entre objectifs de concurrence et politique industrielle, citant le blocage Alstom/Siemens (2019). Ainsi, comme dans le rapport Montaugé (2019)⁷⁸, une modification du droit de la concurrence est préconisée pour intégrer les enjeux de souveraineté industrielle, afin de favoriser l'émergence de champions européens, tout en maintenant un contrôle ex post de la concurrence.

RECOMMANDATIONS

Face aux vulnérabilités juridiques et technologiques dans la gestion des affaires transactionnelles, les recommandations qui ressortent des travaux parlementaires et institutionnels français et européens sont les suivantes :

- Élever la condition d'un "*recours à un prestataire exclusivement soumis au droit européen*" dans les appels d'offre de *Cloud*.
- Généraliser les clauses relatives à la localisation des données dans tous les appels d'offres publics et privés pourrait devenir une exigence nationale et européenne, garantissant un stockage sur territoire de l'Union et l'usage prioritaire de solutions certifiées « *cloud de confiance* ».
- Adapter le droit de la concurrence pour intégrer la notion de souveraineté industrielle, en permettant la création de champions européens dans les secteurs stratégiques (numérique, défense, énergie). Cette évolution suppose de réviser la politique des concentrations afin d'éviter que l'application stricte des règles antitrust n'entrave la constitution d'acteurs de taille critique capables de rivaliser avec les géants américains ou chinois.

Enfin, ces mesures doivent s'inscrire dans une politique industrielle européenne cohérente, fondée sur la préférence communautaire et la sécurité des chaînes d'approvisionnement.

⁷⁶ Rapport du Conseil d'Etat, *La souveraineté*, 11 septembre 2024, page 293.

⁷⁷ Rapport du Conseil d'Etat, *La souveraineté*, 11 septembre 2024, page 365.

⁷⁸ Rapport sur la souveraineté numérique, Franck Montaugé et Gérard Longuet, Sénat, 1^{er} octobre 2019, page 153.

La dépendance technologique ne peut être dissociée de la dépendance en matières premières : sans accès sécurisé aux ressources, aucune autonomie industrielle n'est possible.

B. La réaffirmation de la souveraineté juridique face à la vulnérabilité des chaînes d'approvisionnement critiques

La souveraineté juridique et économique des États européens se trouve aujourd'hui confrontée à une dépendance structurelle aux chaînes d'approvisionnement mondialisées, notamment dans le domaine des matériaux critiques et des technologies stratégiques. Les crises récentes (pandémie de Covid-19, tensions géopolitiques en mer de Chine, guerre en Ukraine) ont mis en lumière la fragilité des approvisionnements en ressources indispensables à la transition numérique et énergétique. Cette vulnérabilité, loin d'être uniquement économique, revêt une dimension juridique et stratégique : elle expose les États et l'Union européenne à des formes d'ingérence et de coercition économique, limitant leur capacité d'action autonome.

Dans ce contexte, la Loi Sapin II⁷⁹ peut être interprétée comme une première étape dans la construction d'un cadre juridique visant à renforcer la résilience économique nationale. Bien que centrée sur la transparence, la lutte contre la corruption et la protection du statut de lanceur d'alerte, elle participe indirectement à la sécurisation des chaînes d'approvisionnement en instaurant des mécanismes de conformité et de gouvernance plus rigoureux.

En favorisant la traçabilité et la responsabilité des entreprises, la loi tend à réduire les risques de dépendance illicite ou de captation stratégique par des acteurs étrangers. Elle constitue ainsi un instrument de souveraineté normative face aux pratiques d'extraterritorialité du droit, notamment américain.

À l'échelle européenne, cette préoccupation s'est traduite par plusieurs initiatives législatives visant à restaurer une autonomie industrielle et technologique. Le European Chips Act⁸⁰, entré en vigueur en septembre 2023, ambitionne de quadrupler la production de semi-conducteurs sur le continent d'ici 2030. Cette stratégie répond à un constat alarmant : près de 80 % de la production mondiale de puces est concentrée à Taiwan, exposant l'Europe à un risque majeur en cas de rupture géopolitique. Ce texte instaure des mécanismes d'investissement public-privé, encourage la relocalisation de la production et crée un cadre juridique commun destiné à coordonner les réponses aux crises d'approvisionnement. Il s'agit d'un acte de souveraineté industrielle, mais aussi juridique, par la réaffirmation d'un droit européen autonome dans un secteur hautement stratégique.

Dans la même dynamique, l'Union a adopté en mars 2024 le Critical Raw Materials Act (CRMA)⁸¹. Ce règlement fixe des objectifs contraignants pour réduire la dépendance aux importations de matières premières critiques (terres rares, manganèse, graphite, lithium, cobalt, nickel) dont l'extraction et le raffinage sont aujourd'hui dominés par la Chine.

⁷⁹ Loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique.

⁸⁰ Règlement (UE) 2023/1781 du Parlement européen et du Conseil du 13 septembre 2023 établissant un cadre de mesures pour renforcer l'écosystème des semi-conducteurs dans l'Union européenne.

⁸¹ Règlement (UE) 2024/1252 du Parlement européen et du Conseil du 11 avril 2024 établissant un cadre pour garantir un approvisionnement européen sécurisé et durable en matières premières critiques.

Le CRMA vise à sécuriser au moins 10 % de l'extraction, 40 % du raffinage et 25 % du recyclage de ces matériaux au sein du territoire européen d'ici 2030. Cette politique industrielle s'accompagne d'un encadrement juridique précis : facilitation des projets stratégiques, simplification des procédures d'autorisation et création de partenariats sécurisés avec des États tiers considérés comme « fiables ». L'Union cherche ainsi à transformer la dépendance économique en interdépendance maîtrisée, consolidant sa capacité à définir ses propres règles du jeu.

En définitive, ce renouveau législatif témoigne d'une redéfinition profonde du rapport entre droit et économie. Face à l'ingérence économique et à la fragmentation des chaînes d'approvisionnement mondiales, l'Europe tente de reprendre le contrôle de ses ressources critiques à travers le droit. Ces dispositifs, s'ils demeurent perfectibles, esquissent les contours d'une souveraineté juridique renouvelée, fondée sur la résilience, la transparence et la capacité d'imposer des normes autonomes dans un espace global concurrentiel.

RECOMMANDATIONS

Suite à ce constat, il est possible de formuler différentes propositions d'amélioration afin de diminuer cette dépendance :

D'une part, renforcer la cohérence du cadre juridique européen en harmonisant les dispositifs nationaux avec les initiatives européennes afin d'éviter les doublons et d'assurer une application homogène des principes de transparence, de gouvernance et de traçabilité.

En second lieu, consolider la résilience des chaînes d'approvisionnement en instaurant un organe (au niveau européen) chargé d'identifier et de suivre les vulnérabilités stratégiques (matières premières, composants, haute-technologie)

Dernier axe, orienté sur la gouvernance qualifiable de "démocratique" en associant la société civile et les parlements nationaux à l'élaboration et au suivi des politiques de souveraineté économique. Cette ambition viserait également à accroître la transparence des chaînes d'approvisionnement grâce à des obligations de reporting renforcées pour les entreprises opérant dans les secteurs critiques. Ultime aspect, la formation des acteurs économiques et juridiques (institutions publiques, magistrats, dirigeants d'entreprises) à la compréhension des enjeux de souveraineté et de conformité internationale.

La maîtrise des chaînes d'approvisionnement ne peut être dissociée de celle des sources d'énergie, puisqu'aucune production industrielle n'est possible sans un accès stable, sûr et abordable aux ressources énergétiques.

C. L'énergie, talon d'Achille de la compétitivité européenne

État des lieux et impact de l'énergie sur la compétitivité

La France importe aujourd'hui la majorité des énergies fossiles qu'elle utilise à savoir, pétrole, charbon et 83 % du gaz⁸². Elle a dû absorber la « crise énergétique » de 2022 : la facture énergétique nationale a culminé à 124,1 Md€ (2022) et reste très élevée (71,2 Md€ en 2023)⁸³. Pour limiter le choc, la consommation de gaz a chuté de 20 % entre 2021 et 2023⁸⁴.

Pour compenser, la France s'est lancée dans des importations massives de GNL (30,7 Gm³ importés en 2023, premier d'Europe)⁸⁵, en grande partie des États-Unis (43 % du GNL).

Paradoxalement, grâce à son parc nucléaire (64 % de la production électrique) et à un réseau fiable, la France est exportatrice nette d'électricité bas-carbone (nouveau record de 89 TWh nets exportés en 2024). Le « mix » électrique est parmi les plus décarbonés au monde (≈95 % décarboné en 2024), ce qui attire des investissements industriels.

Néanmoins, le coût de l'énergie pèse lourdement sur l'industrie. En 2019 les dépenses énergétiques totales représentaient 6,7 % du chiffre d'affaires industriel français (seuil inférieur à l'Allemagne à 7,8 %)⁸⁶. La crise a toutefois fait grimper ces coûts (≈+8 % de la VA 2019). On estime que près de la moitié de l'inflation sur les produits manufacturés en 2021-22 provient de l'énergie.

Des études économiques montrent d'ailleurs qu'une hausse de 10 % du prix de l'électricité réduirait les exportations industrielles françaises de l'ordre de 1,9 %, renforçant la vulnérabilité des secteurs électro-intensifs.⁸⁷

Défis réglementaires et géopolitiques

Le cadre juridique français et européen complexifie l'accès à une énergie compétitive. La sortie progressive de l'ARENH (tarif régulé nucléaire) fin 2025, remplacée par des contrats d'allocation longue durée (CAPN) négociés librement, inquiète les industriels quant à une augmentation des prix de marché. Par ailleurs, la fiscalité énergétique (CSPE, taxes intérieures sur le gaz et l'électricité) et le financement des renouvelables pèsent sur les tarifs finaux. Les obligations européennes de décarbonation (EU ETS, objectifs « Fit for 55 », futur CBAM) et le calendrier de neutralité carbone (2050) font du coût de l'énergie un enjeu concurrentiel majeur, surtout par

⁸² Ministère de l'aménagement du territoire et de la transition écologique - Bilan énergétique de la pour 2023 - DATA LAB - Avril 2025

⁸³ Insee - Consommation d'énergie dans l'industrie en 2023 - INSEE- 05/02/2025.

⁸⁴ D'où vient le gaz naturel importé en France - 05/02/2025 - Connaissance des énergies.

⁸⁵ SDES - DATALAB - Chiffres clés de l'énergie - édition 2025

⁸⁶ Caroline Mini et Mathieu Bordigoni, L'industrie face aux prix de l'énergie. Les marchés européens sont-ils en défaut ? - Les Notes de La Fabrique, Paris, Presses des Mines, 2022..

⁸⁷ Les thémas de la DGE – Quelle incidence de la hausse des prix de l'énergie sur l'industrie - Septembre 2023

rapport à des concurrents à ressources abondantes et peu contraintes. Côté marché, la réforme de juillet 2024 de l'UE (règlement IEM) permet la conclusion de contrats d'électricité à long terme (CfD/CAP) pour stabiliser les prix, mais renforce aussi le rôle de l'État en cas de crise (possibilité de plafonner les prix pour ménages/PME)⁸⁸.

Sur le plan géopolitique, la France reste entièrement dépendante du marché international pour le pétrole et le gaz. La guerre en Ukraine a fait chuter la part du gaz russe dans les importations européennes (de 41 % en 2019 à ~15 % en 2023)⁸⁹, et son acheminement via l'Ukraine a cessé fin 2024⁹⁰.

La France a compensé par le GNL, mais ces substituts restent coûteux. Toute tension (OPEP+, crise en Méditerranée, pression sur les prix du gaz global) se répercute immédiatement sur les coûts domestiques. La volatilité mondiale de l'énergie et les vulnérabilités stratégiques (stockage gaz seulement 1/3 de la conso annuelle⁹¹) constituent donc des menaces récurrentes pour la compétitivité française.

RECOMMANDATIONS

Axes technologiques et industriels : Accélérer massivement le déploiement d'énergies bas-carbone. Doubler d'ici 2030 la capacité éolienne et solaire (objectifs UE)⁹² tout en développant l'hydrogène vert et le petit nucléaire (SMR) pour compenser la fermeture programmée des centrales existantes⁹³. Soutenir la R&D et les investissements dans le stockage (batteries, gaz renouvelable) et la flexibilité du réseau (smart grids, PPA longue durée) pour lisser la fourniture et attirer des électro-intensifs (ex. automatisme de tarifs préférentiels en cas de production excédentaire).

Axes réglementaires : Mieux aligner la fiscalité sur l'intensité énergétique : affecter la taxe carbone ou le "versement nucléaire universel" aux réductions de charges ou subventions ciblées pour l'industrie électro-intense⁹⁴. Par exemple, alléger la CSPE/TICFE pour les sites clés (comme en Allemagne) ou compenser par un crédit d'impôt la hausse des coûts énergétiques. L'État doit aussi assurer la visibilité réglementaire (calendrier clair des appels d'offres renouvelables, stabilité du régime nucléaire) et pérenniser les mécanismes de contrats à long terme (CfD, CAPN) pour les gros consommateurs⁹⁵. Enfin, renforcer la coopération européenne (achats groupés de gaz, mutualisation des infrastructures) aiderait à amortir les chocs.

Axes économiques : Mettre à profit les financements publics (France 2030, plan de relance) pour décarboner l'industrie. Réorienter des aides vers les filières stratégiques (chimie, métallurgie) pour couvrir jusqu'à 50 % de l'investissement dans la décarbonation. Compenser le coût de l'énergie par une baisse du coût du travail (modulation des cotisations sociales) pour les secteurs exposés⁹⁶. Enfin, utiliser les tarifs de l'électricité pour

⁸⁸ Réforme du marché de l'électricité 22 mai 2024

⁸⁹ D'où vient le gaz naturel importé en France ? 02 janvier 2025

⁹⁰ D'où vient le gaz naturel importé en France ? 02 janvier 2025

⁹¹ D'où vient le gaz naturel importé en France ? 02 janvier 2025

⁹² Réforme du marché de l'électricité 22 mai 2024

⁹³ France 2030 : un plan d'investissement pour la France 13/10/2023

⁹⁴ Les notes du conseil d'analyse économique, n° 6, mai 2013

⁹⁵ Réforme du marché de l'électricité - 22 mai 2024

⁹⁶ Les notes du conseil d'analyse économique, n° 6, mai 2013

favoriser la relocalisation : exiger un contingent d'achat bas carbone pour les grandes implantations et proposer des prix compétitifs aux nouveaux sites industriels (via des subventions ou certificats verts).

En résumé, il s'agit de sécuriser l'accès à une énergie abondante et propre à moindre coût, en mobilisant à la fois l'innovation technologique et les leviers juridiques et économiques disponibles.

Conclusion et ouverture

Notons par ailleurs que depuis 2010, la France, l'Europe et plus largement le monde font face à une montée des ingérences informationnelles qui prennent de multiples formes, notamment à des fins économiques et politiques. Ces manipulations de l'information, souvent orchestrées par des puissances étrangères, constituent aujourd'hui un levier d'influence économique non négligeable. Elles visent à orienter l'opinion publique, à déstabiliser les marchés et à affaiblir la compétitivité des entreprises ciblées.

Les ingérences à dimension politique ont des effets économiques indirects mais considérables. En octobre 2024, en Moldavie, des fonds russes d'environ 15 millions de dollars ont été distribués à près de 130 000 personnes afin d'influencer le vote pro-Russie et anti-UE⁹⁷. Lors de la législature 2019-2024, le Parlement européen a mis en garde contre des campagnes d'ingérence étrangère, impliquant notamment des financements venus de l'extérieur et la diffusion massive de contenus manipulateurs sur les réseaux sociaux, ce qui a créé une atmosphère d'incertitude pour les électeurs⁹⁸. Cette mesure apparaît à la fois pertinente et nécessaire, toutefois, la mise en œuvre effective de cette mesure se heurte à plusieurs difficultés pratiques. Il demeure particulièrement complexe d'identifier avec certitude l'origine des financements ou des campagnes d'influence, surtout lorsqu'ils transitent par des acteurs privés ou des plateformes numériques étrangères. De plus, cette régulation doit s'opérer dans le respect des libertés fondamentales, notamment celle d'expression, ce qui rend délicate la définition d'un équilibre entre protection de la démocratie et préservation des droits individuels. Ainsi, son efficacité dépendra étroitement de la coopération internationale et de la capacité des institutions européennes à mettre en place des mécanismes de contrôle à la fois transparents et proportionnés.

Au-delà de ces exemples, les manipulations informationnelles accentuent la polarisation politique et retardent les décisions économiques. L'influence d'acteurs étrangers sur le plan informationnel peut ainsi contribuer à une instabilité politique pouvant ensuite engendrer par exemple la dissolution de l'Assemblée nationale, qui de suite interrompt immédiatement tous les travaux parlementaires. Les projets de loi non adoptés ou non finalisés deviennent alors caducs et doivent être redéposés pour être repris. Ainsi, la combinaison de la désinformation, des ingérences étrangères et des blocages institutionnels qu'elles peuvent provoquer crée un climat d'incertitude peu favorable à l'investissement et à la stabilité économique. D'après le World Economic Forum (WEF), la désinformation est désormais l'un des principaux risques à court terme pour les économies, elle peut entraîner des pertes de recettes, une baisse des cours boursiers, ou un coût important de gestion de crise pour les entreprises. Les pertes moyennes dépassent quatre millions d'euros par incident entre perte de clients, communication de crise et procédures judiciaires. Ces attaques sapent la confiance des investisseurs et exposent les entreprises à des rachats hostiles ou à des faillites, renforçant la dépendance économique vis-à-vis d'acteurs étrangers. Selon une étude menée sur les entreprises du S&P 500, présentée dans le rapport « *Fake News, Corruption and Compliance in the Private Sector* » publié par Transparency International le 21 octobre 2024, la diffusion de fausses informations entraîne en moyenne une perte de 3,1 % de la valeur de

⁹⁷ Résolution du Parlement européen, 9 octobre 2024, renforcement de la résilience de la Moldavie face à l'ingérence russe dans la perspective des prochaines élections présidentielles et du référendum constitutionnel sur l'intégration européenne (2024/2821(RSP)).

⁹⁸ Parlement Européen, "Ingérence étrangère : comment le Parlement lutte contre la menace qui pèse sur la démocratie européenne", mis à jour le 15 mai 2025.

marché dans les trois mois suivant l'événement et jusqu'à 5,8 % pour certaines entreprises ciblées, comparativement à des sociétés similaires non affectées⁹⁹.

Ces ingérences constituent ainsi une menace systémique pour la souveraineté économique. Dans le cadre d'Horizon Europe, plus d'un tiers des plus de 300 millions d'euros de soutien à la recherche sur la démocratie ont été mobilisés pour financer la recherche et l'innovation afin de mieux détecter et comprendre les activités de manipulation de l'information et d'ingérence étrangères menées depuis l'étranger, ainsi que d'autres influences indues sur la prise de décision politique¹⁰⁰. Le Digital Services Act (DSA)¹⁰¹, pleinement applicable depuis février 2024, oblige les grandes plateformes numériques à évaluer et réduire les risques liés à la désinformation. Il impose également plus de transparence dans les algorithmes et la modération de contenus. Le Code of Practice on Disinformation¹⁰², désormais intégré au DSA, devient à partir de juillet 2025 un code de bonnes pratiques volontaires contre la désinformation. S'y ajoute le European Media Freedom Act (EMFA), entré en vigueur le 7 mai 2024 et applicable à partir d'août 2025¹⁰³. Ce règlement européen vise à protéger la liberté et l'indépendance des médias, à renforcer la transparence sur leur propriété et à encadrer l'usage des financements publics. Il interdit les ingérences politiques dans les décisions éditoriales, encadre strictement le recours aux logiciels espions contre les journalistes et crée un Conseil européen des services de médias chargé d'assurer une application harmonisée du cadre. En garantissant un espace médiatique plus transparent et indépendant, l'EMFA complète le DSA et la législation nationale pour réduire l'influence des acteurs étrangers sur l'information. Toutefois, ces textes demeurent marqués par un certain manque d'exhaustivité et des zones d'incertitude. Pour le DSA, plusieurs notions restent floues, comme celle de « contenu manifestement illicite », dont la définition varie selon les législations nationales, ou les notions de « risques systémiques » et de « mesures de mitigation », dont les critères d'évaluation et de proportionnalité ne sont pas clairement établis. Les concepts d'« acteurs très importants en ligne » et de « transparence des algorithmes » laissent également une large marge d'appréciation aux plateformes, tout comme les règles de modération et de publicité ciblée, qui ne sont pas précisées de manière uniforme. Ces imprécisions compliquent l'application pratique du DSA et peuvent générer des divergences entre États membres. L'EMFA, quant à lui, bien qu'il renforce la protection contre les ingérences politiques et les atteintes à la liberté des médias, confronte l'Union à la délicate question de la répartition des compétences en matière audiovisuelle. Si la création du Conseil européen des services de médias tend à favoriser une harmonisation des pratiques, la diversité des régimes nationaux limite encore l'effectivité et la portée uniforme de ces instruments.

Les ingérences informationnelles ne relèvent donc plus seulement de la guerre idéologique ou politique. Elles sont devenues un instrument stratégique de déstabilisation économique. En fragilisant à la fois la gouvernance politique et la compétitivité des entreprises, elles mettent en péril la résilience des États et la confiance dans les marchés. La France et l'Europe, particulièrement visées depuis plus d'une décennie, doivent désormais renforcer leurs capacités de protection et de réaction afin de préserver leur autonomie économique et démocratique.

⁹⁹ *Transparency International, "FAKE NEWS, CORRUPTION AND COMPLIANCE IN THE PRIVATE SECTOR", 21 octobre 2024.*

¹⁰⁰ *Commission Européenne, "COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ DES RÉGIONS", 12 décembre 2023.*

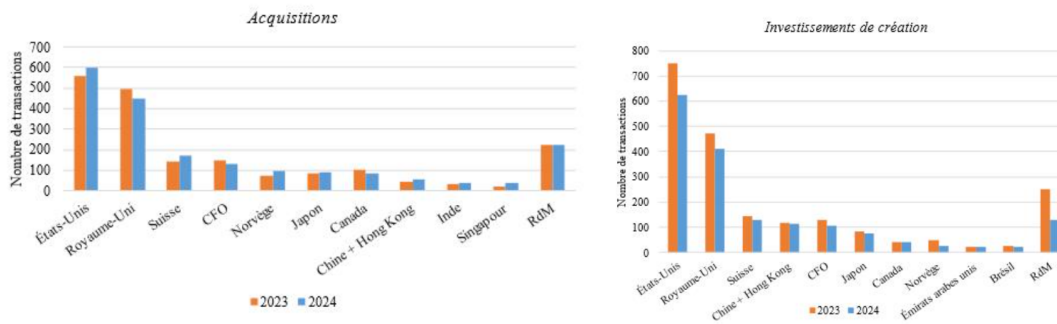
¹⁰¹ *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance).*

¹⁰² *European Commission, "The Code of Conduct on Disinformation", 13 février 2025*

¹⁰³ *Regulation (EU) 2024/1083, a common framework for media services in the internal market (European Media Freedom Act)*

ANNEXES

Annexe 1. Origine des investissements étrangers dans l'UE, selon leur finalité (investissements visant la création ou l'acquisition du capital d'une entreprise).



RAPPORT DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL - Cinquième rapport annuel sur le filtrage des investissements directs étrangers dans l'Union (14/10/2025).

NB : CFO: Centres financiers offshore. RdM: Reste du monde.

Annexe 2. Tableau récapitulatif des degrés et nature de l'impact par type de vulnérabilité

| Types de vulnérabilités - Degrés et nature de l'impact | | | |
|--|---|--------------------------|---------------------------|
| Type de vulnérabilité | Impact sur la souveraineté juridique | Impact économique | Nature de l'impact |
| Extraterritorialité du droit américain | ★★★★★ | ★★★★☆ | Direct |
| Dépendance aux clouds étrangers | ★★★★★ | ★★★★☆ | Direct |
| Investissements étrangers hostiles / prédation d'actifs | ★★★★★ | ★★★★★ | Direct |
| Ingérences informationnelles et manipulation numérique | ★★★★☆ | ★★★★☆ | Indirect |
| Dépendance industrielle et technologique | ★★★★☆ | ★★★★★ | Indirect |
| Présence des cabinets étrangers "incontournables" (forensic, compliance, lawfare) | ★★★★★ | ★★★★☆ | Direct |
| Cyber-vulnérabilités et absence d'hébergement souverain | ★★★★★ | ★★★★☆ | Direct |
| Faiblesse du droit de la concurrence européen | ★★★★☆ | ★★★★★ | Indirect |

Annexe 3- Exemples emblématiques des entreprises frappées par l'extraterritorialité américaine.

| Entreprise | Pays d'origine | Année de sanction | Montant total des sanctions | Secteur | Impact stratégique / Observations |
|-------------------------|----------------|-------------------|--|--------------------------|--|
| Airbus | France/Europe | 2020 | ≈ 3,9 milliards \$ (dont ≈ 2,1 Md\$ aux autorités françaises, britannique et américaines dans le volet FCPA) | Aéronautique & Défense | Plus grosse sanction anticorruption multi-juridictionnelle de l'histoire → pression sur industrie stratégique européenne |
| Alstom | France | 2014 | 772 millions \$ | Énergie & Infrastructure | Impact direct sur la vente de la branche énergie à General Electric → perte d'autonomie industrielle |
| TotalEnergies | France | 2013 | 398 millions \$ | Énergies hydrocarbures | Surveillance renforcée des investissements dans pays à risques (Iran) |
| TechnipFMC | France / UK | 2019 & 2010 | ≈ 830 millions \$ cumulés | Ingénierie pétrolière | Deux condamnations successives pression forte sur gouvernance |
| Société Générale | France | 2018 | 585 millions \$ (part USA, sur 1 Md\$ total FR + USA) | Banque finance | 1ère CJIP coordonnée FR/USA → coopération judiciaire renforcée |

| Entreprise | Pays d'origine | Année de sanction | Montant total des sanctions | Secteur | Impact stratégique / Observations |
|----------------------|----------------|-------------------|-----------------------------|--------------------------|---|
| Siemens | Allemagne | 2008 | 1,6 milliard \$ | Industrie & technologies | Grand précédent illustrant la portée extraterritoriale du FCPA |
| Telia Company | Suède | 2017 | 965 millions \$ | Télécoms | Leadership américain sur la lutte anticorruption (même hors dollar) |

Annexe 4. Recommandations détaillées de la partie consacrée aux vulnérabilités dans les affaires transactionnelles

| Domaine | Recommandation | Nature juridique | Commentaires |
|-------------------------------|---|-----------------------|---|
| Cabinets d'avocats / forensic | Créer un label 'cabinet de confiance' européen (confidentialité, hébergement UE, absence de conflits d'intérêts) | Adaptation fine | Basé sur la directive Services 2006/123/CE – coordination avec les ordres professionnels |
| | Constituer un réseau européen 'Forensic & Compliance' (adossé à l'AFA ou au BEPI) | Adaptation fine | Extension de compétences du Parquet européen – coordination administrative UE |
| | Former magistrats et juristes d'entreprise à la compliance extraterritoriale et à la loi de blocage | Adaptation fine | Extension des modalités d'application du cadre Sapin II et formation AFA |
| Cloud et données | Généraliser les clauses de localisation et de souveraineté des données dans les contrats publics et stratégiques | Adaptation fine | Compatible avec le Code de la commande publique – nécessite clause type ou décret |
| | Rendre obligatoire le recours à un cloud certifié SecNumCloud pour les OIV et opérateurs publics / Et veiller au SecNumCloud | Nouveau droit positif | Renforcement des obligations existantes pour les OIV – mesure déjà amorcée |
| | Créer un cadre européen commun de mutualisation des clouds souverains (GAIA-X, NumSpot) | Adaptation fine | S'appuie sur DMA/DSA – nécessite gouvernance publique renforcée |
| | Imposer la notification préalable à la CNIL ou à l'AFA pour tout transfert de données d'enquête hors UE | Adaptation fine | Extension RGPD + loi de blocage 1968 – contrôle accru CNIL/AFA |
| Champions européens | Introduire un critère de 'souveraineté économique' dans l'évaluation des concentrations et aides d'État | Adaptation fine | Requiert modification des lignes directrices de la Commission (2021/C 291/01) |

| | | |
|---|---------------------------------|--|
| Créer un ' palier souverain ' de dérogation au droit de la concurrence pour les secteurs stratégiques | Nouveau cadre juridique à créer | Nécessiterait un règlement européen spécifique ('Règlement souveraineté industrielle') |
| Mettre en place un Fonds européen de souveraineté finançant/accompagnant les fusions et technologies critiques | Nouveau droit positif | Prolongement du programme STEP – institutionnalisation du fonds |
| Introduire des clauses miroirs dans les marchés publics européens (protectionnisme réciproque) | Adaptation fine | Possible via modification du règlement UE 2022/1031 sur les marchés publics internationaux |

Annexe 5. Liste des recommandations.

| N° de la recommandation | Recommandation |
|-------------------------|--|
| 1 | <p>Promouvoir, au sein du Conseil de l'UE, une révision du règlement de 1996 afin d'y inclure une clause de réciprocité : toute mesure américaine à portée extraterritoriale entraînerait des contre-mesures équivalentes en Europe (gel d'actifs, amende, ou restriction d'accès au marché européen).</p> <p>Coordonner la reconnaissance mutuelle des dispositifs de conformité : création d'un protocole bilatéral de consultation préalable pour réduire les risques de double sanction. Création d'un groupe de travail permanent réunissant le PNF, l'Agence française anticorruption, le DOJ, et la SEC (Securities and Exchange Commission) pour harmoniser les programmes de conformité transnationaux.</p> |
| 2 | <p>Il est important pour la France de continuer ses efforts dans sa mise en œuvre du contrôle des exportations. Que ce soit pour son savoir-faire industriel en actualisant sa législation et en conservant la rigueur et la performance des processus de contrôles actuellement mises en place.</p> <p>Il est également important que les acteurs de la BITD française poursuivent leurs efforts d'information et de mise en conformité vis-à-vis des législations étrangères contraignantes, US et chinoise, afin d'éviter le risque de lourdes sanctions économiques, mais également une profonde ingérence étrangères.</p> |
| 3 | <p>Malgré un cadre juridique robuste, l'application du blocage demeure inégale entre États membres, avec peu de notifications ou de recours au <i>claw-back</i>. Plusieurs rapports parlementaires et évaluations de la Commission appellent à :</p> <ul style="list-style-type: none"> - Standardiser les pratiques de motivation des entreprises (modèle <i>Bank Melli</i>) ; - Clarifier les critères de l'article 5§2 (autorisation en cas de préjudice grave) ; - Soutenir des contentieux pilotes pour activer le <i>claw-back</i> ; - Créer des indicateurs de suivi (KPI), publiés dans les rapports annuels (article 7(a)). <p>Dans cette perspective, la véritable dissuasion ne réside pas uniquement dans les textes, mais dans la capacité à élever le coût anticipé de la coercition pour l'État émetteur. La combinaison du blocage, du soutien contentieux, et des leviers de rétorsion calibrés permettrait ainsi à l'UE de réduire la sur-</p> |

| | |
|---|--|
| | conformité privée et de rétablir un espace autonome de décision pour ses opérateurs. (voir la bibliographie contenant les rapports parlementaires et évaluations de la Commission). |
| 4 | <p>Maintenir un dispositif de défense commerciale robuste et poursuivre les efforts engagés pour en perfectionner les modalités d'application (meilleur suivi des importations, réactivité accrue, transparence des aides étrangères).</p> <p>Toutefois, ces mesures entraînent des rétorsions ciblées de la part des États tiers, il est essentiel de concentrer prioritairement la protection sur les secteurs où une souveraineté est nécessaire (acier, énergie, technologies de transition, véhicules électriques), plutôt que d'élargir le champ des enquêtes. Une stratégie trop extensive risquerait de diluer l'efficacité du dispositif et d'alimenter une escalade commerciale préjudiciable à d'autres filières exportatrices européennes.</p> <p>L'enjeu est donc de protéger sans se disperser, en privilégiant une approche ciblée, proportionnée et stratégique.</p> |
| 5 | Dès lors, il convient de soutenir un règlement européen ambitieux sur les investissements sortants listant les pays et les secteurs stratégiques à risque, devant faire l'objet de contrôle renforcé. Par ailleurs, la France doit être précurseur, et ne pas attendre le règlement européen qui n'advient pas avant 2027 avec une application à l'horizon 2028. Cela passe par la création, par décret, d'un dispositif rattaché à la Direction Générale du Trésor. La difficulté résidera dans l'établissement d'un mécanisme de notification volontaire, prenant en compte les lourdeurs administratives et les risques pour leurs investissements |
| 6 | <p>Une coordination européenne ajustée du Règlement UE 2023/2411 sur les IGPIA et d'une future "EU Blocking Statute renforcée".</p> <p>Investir dans des outils de traçabilité, de certification numérique, de veille et d'opposition aux dépôts de marques, brevets et noms de domaines abusifs.</p> <p>Les entreprises doivent être sensibilisées et formées en interne sur le secret des affaires, la préservation du made in france et la captation d'informations stratégiques</p> |
| 7 | S'adosser aux agences de renseignement pour évoluer dans le champ offensif à l'instar de l'advocacy center américain qui mobilise les ressources d'agences américaines et notamment des agences de renseignement à fins de soutien aux entreprises américaines dans leurs opportunités commerciales à l'international |
| 8 | Mettre en place des systèmes obligatoires et s'assurer de leur viabilité d'un point de vue financier et humain |

| | |
|------------------|--|
| <p>9</p> | <p>Prévoir des mécanismes d'aide financière pour les entreprises qui rencontreraient des difficultés de cette nature pour la mise en œuvre des obligations nées des directives NIS.</p> <p>Doter l'ANSSI de ressources suffisantes pour appliquer efficacement les dispositions des directives NIS.</p> |
| <p>10</p> | <p>Développer les contrôles de la CNIL pour que les entreprises prennent conscience de l'impératif qu'elles ont de se mettre en cohérence avec le régime en place.</p> |
| <p>11</p> | <p>Face aux vulnérabilités juridiques et technologiques dans la gestion des affaires transactionnelles, les recommandations qui ressortent des travaux parlementaires et institutionnels français et européens sont les suivantes :</p> <ul style="list-style-type: none"> ● Élever la condition d'un <i>“recours à un prestataire exclusivement soumis au droit européen”</i> dans les appels d'offre de <i>Cloud</i>. ● Généraliser les clauses relatives à la localisation des données dans tous les appels d'offres publics et privés pourrait devenir une exigence nationale et européenne, garantissant un stockage sur territoire de l'Union et l'usage prioritaire de solutions certifiées <i>« cloud de confiance »</i>. ● Adapter le droit de la concurrence pour intégrer la notion de souveraineté industrielle, en permettant la création de champions européens dans les secteurs stratégiques (numérique, défense, énergie). Cette évolution suppose de réviser la politique des concentrations afin d'éviter que l'application stricte des règles antitrust n'entrave la constitution d'acteurs de taille critique capables de rivaliser avec les géants américains ou chinois. <p>Enfin, ces mesures doivent s'inscrire dans une politique industrielle européenne cohérente, fondée sur la préférence communautaire et la sécurité des chaînes d'approvisionnement.</p> |
| <p>12</p> | <p>Suite à ce constat, il est possible de formuler différentes propositions d'amélioration afin de diminuer cette dépendance :</p> <p>D'une part, renforcer la cohérence du cadre juridique européen en harmonisant les dispositifs nationaux avec les initiatives européennes afin d'éviter les doublons et d'assurer une application homogène des principes de transparence, de gouvernance et de traçabilité.</p> <p>En second lieu, consolider la résilience des chaînes d'approvisionnement en instaurant un organe (au niveau européen) chargé d'identifier et de suivre les vulnérabilités stratégiques (matières premières, composants, haute-technologie)</p> <p>Dernier axe, orienté sur la gouvernance qualifiable de <i>“démocratique”</i> en associant la société civile et les parlements nationaux à l'élaboration et au suivi des politiques de souveraineté économique. Cette ambition viserait également à accroître la transparence des chaînes d'approvisionnement grâce à des</p> |

| | |
|----|--|
| | obligations de reporting renforcées pour les entreprises opérant dans les secteurs critiques. Ultime aspect, la formation des acteurs économiques et juridiques (institutions publiques, magistrats, dirigeants d'entreprises) à la compréhension des enjeux de souveraineté et de conformité internationale |
| 13 | <p>Axes technologiques et industriels : Accélérer massivement le déploiement d'énergies bas-carbone. Doubler d'ici 2030 la capacité éolienne et solaire (objectifs UE)¹⁰⁴ tout en développant l'hydrogène vert et le petit nucléaire (SMR) pour compenser la fermeture programmée des centrales existantes¹⁰⁵. Soutenir la R&D et les investissements dans le stockage (batteries, gaz renouvelable) et la flexibilité du réseau (smart grids, PPA longue durée) pour lisser la fourniture et attirer des électro-intensifs (ex. automatisme de tarifs préférentiels en cas de production excédentaire).</p> <p>Axes réglementaires : Mieux aligner la fiscalité sur l'intensité énergétique : affecter la taxe carbone ou le "versement nucléaire universel" aux réductions de charges ou subventions ciblées pour l'industrie électro-intense¹⁰⁶. Par exemple, alléger la CSPE/TICFE pour les sites clés (comme en Allemagne) ou compenser par un crédit d'impôt la hausse des coûts énergétiques. L'État doit aussi assurer la visibilité réglementaire (calendrier clair des appels d'offres renouvelables, stabilité du régime nucléaire) et pérenniser les mécanismes de contrats à long terme (CfD, CAPN) pour les gros consommateurs¹⁰⁷. Enfin, renforcer la coopération européenne (achats groupés de gaz, mutualisation des infrastructures) aiderait à amortir les chocs.</p> <p>Axes économiques : Mettre à profit les financements publics (France 2030, plan de relance) pour décarboner l'industrie. Réorienter des aides vers les filières stratégiques (chimie, métallurgie) pour couvrir jusqu'à 50 % de l'investissement dans la décarbonation. Compenser le coût de l'énergie par une baisse du coût du travail (modulation des cotisations sociales) pour les secteurs exposés¹⁰⁸. Enfin, utiliser les tarifs de l'électricité pour favoriser la relocalisation : exiger un contingent d'achat bas carbone pour les grandes implantations et proposer des prix compétitifs aux nouveaux sites industriels (via des subventions ou certificats verts).</p> <p>En résumé, il s'agit de sécuriser l'accès à une énergie abondante et propre à moindre coût, en mobilisant à la fois l'innovation technologique et les leviers juridiques et économiques disponibles.</p> |

¹⁰⁴ Réforme du marché de l'électricité 22 mai 2024

¹⁰⁵ France 2030 : un plan d'investissement pour la France 13/10/2023

¹⁰⁶ Les notes du conseil d'analyse économique, n° 6, mai 2013

¹⁰⁷ Réforme du marché de l'électricité - 22 mai 2024

¹⁰⁸ Les notes du conseil d'analyse économique, n° 6, mai 2013

Glossaire

| Terme | Définition |
|--|---|
| Concepts généraux | |
| Souveraineté juridique | Capacité d'un État à exercer pleinement son autorité normative et décisionnelle sans influence extérieure. |
| Ingérence économique | Action d'un État ou d'un acteur étranger visant à influencer ou contraindre l'économie d'un autre pays. |
| Extraterritorialité du droit | Application d'une législation nationale à des personnes ou faits situés hors du territoire de l'État concerné. |
| Lawfare | Usage stratégique du droit comme instrument de puissance ou de contrainte géopolitique. |
| Coercition économique | Pression exercée par des moyens commerciaux, financiers ou juridiques pour influencer la politique d'un autre État. |
| Captation économique / patrimoniale | Acquisition, directe ou indirecte, de savoir-faire, d'actifs ou d'entreprises stratégiques d'un autre pays. |
| Dépendance structurelle | Situation de vulnérabilité liée à la dépendance envers des ressources, technologies ou normes extérieures. |
| Souveraineté industrielle | Capacité d'un pays à maîtriser ses chaînes de production et technologies critiques. |
| Compliance | Conformité d'une organisation à des règles, lois et standards internationaux. |
| Over-compliance (sur-conformité) | Application excessive de règles étrangères par crainte de sanctions, au détriment de la souveraineté nationale. |
| Espionnage industriel | Obtention illégale d'informations stratégiques d'une entreprise à des fins concurrentielles ou politiques. |
| Cybermenace / cyberattaque | Action malveillante visant à compromettre des systèmes informatiques ou des données sensibles. |
| Chaînes d'approvisionnement critiques | Ensemble des flux logistiques essentiels à la production de biens stratégiques. |
| Résilience économique / juridique | Capacité à anticiper, absorber et surmonter des chocs ou ingérences extérieures. |

| | |
|--|--|
| Soft power | Capacité d'influence d'un pays par la culture, les valeurs ou le droit plutôt que par la force. |
| Hard power | Usage de moyens militaires ou coercitifs pour atteindre des objectifs stratégiques. |
| Secret des affaires | Protection juridique des informations stratégiques d'une entreprise contre l'obtention ou l'usage illicite. |
| Textes, dispositifs et lois | |
| Loi de blocage (1968) | Loi française interdisant la transmission d'informations économiques à des autorités étrangères sans autorisation. |
| Loi Sapin II (2016) | Texte français de lutte contre la corruption et pour la transparence de la vie économique. |
| Décret Montebourg (2014) | Décret renforçant le contrôle des investissements étrangers dans les secteurs stratégiques. |
| Loi sur le secret des affaires (2018) | Loi protégeant les informations confidentielles à valeur économique. |
| Loi de programmation militaire (2013) | Texte encadrant notamment les obligations de cybersécurité des opérateurs d'importance vitale. |
| Règlement de blocage (CE n°2271/96) | Règlement européen neutralisant les effets des lois extraterritoriales étrangères. |
| Directive NIS / NIS2 | Directives européennes imposant des obligations de cybersécurité aux opérateurs essentiels. |
| Critical Raw Materials Act (CRMA) | Règlement européen visant à sécuriser l'accès aux matières premières critiques. |
| European Chips Act | Texte européen visant à relocaliser et renforcer la production de semi-conducteurs. |
| Règlement UE 2025/1759 (IGPIA) | Règlement européen sur les indications géographiques pour produits artisanaux et industriels. |
| Computer Fraud and Abuse Act (1986) | Loi américaine sanctionnant l'accès non autorisé à des systèmes informatiques. |
| Espionage Economic Act (1996) | Loi américaine réprimant le vol de secrets technologiques et commerciaux. |
| Defend Trade Secrets Act (2016) | Loi américaine protégeant les secrets commerciaux à l'échelle fédérale. |
| Foreign Corrupt Practices Act (FCPA) | Loi américaine sanctionnant la corruption d'agents publics étrangers. |

| | |
|---|--|
| Sarbanes–Oxley Act | Loi américaine encadrant la gouvernance et la transparence des sociétés cotées. |
| Cloud Act | Loi américaine autorisant l'accès des autorités aux données stockées par des prestataires américains, même à l'étranger. |
| RGPD (Règlement général sur la protection des données) | Règlement européen encadrant le traitement des données personnelles. |
| Cyber Resilience Act (CRA) | Règlement européen imposant des obligations de cybersécurité aux fabricants de produits numériques. |
| ARENH | Accès régulé à l'électricité nucléaire historique, dispositif français de régulation énergétique. |
| Institutions et acteurs | |
| ANSSI | Agence nationale de la sécurité des systèmes d'information. |
| AFA | Agence française anticorruption. |
| DGSI | Direction générale de la sécurité intérieure. |
| DRSD | Direction du renseignement et de la sécurité de la défense. |
| SGDSN | Secrétariat général de la défense et de la sécurité nationale. |
| SISSE | Service de l'information stratégique et de la sécurité économiques. |
| PNF | Parquet national financier. |
| CNIL | Commission nationale de l'informatique et des libertés. |
| INPI | Institut national de la propriété industrielle. |
| DOJ | Department of Justice (États-Unis). |
| SEC | Securities and Exchange Commission (États-Unis). |
| OMC | Organisation mondiale du commerce. |
| OCDE | Organisation de coopération et de développement économiques. |

| | |
|---|---|
| UE | Union européenne. |
| DG TRADE | Direction générale du commerce de la Commission européenne. |
| MINARM | Ministère des Armées. |
| DGA | Direction générale de l'armement. |
| Commission européenne | Institution exécutive de l'Union européenne. |
| Conseil de l'UE | Institution représentant les gouvernements des États membres. |
| Parlement européen | Institution législative de l'Union européenne représentant les citoyens. |
| Notions économiques et industrielles | |
| BITD | Base industrielle et technologique de défense. |
| CJIP | Convention judiciaire d'intérêt public, mécanisme de transaction pénale pour les entreprises. |
| ITAR | International Traffic in Arms Regulations, réglementation américaine des exportations d'armement. |
| EAR | Export Administration Regulations, réglementation américaine des exportations technologiques. |
| ACI | Instrument anti-coercition de l'Union européenne. |
| TRQ | Tariff Rate Quota, contingent tarifaire douanier. |
| Dumping / Antidumping | Pratique de vente à prix inférieur au coût de production / Mesures correctrices correspondantes. |
| OIV | Opérateur d'importance vitale. |
| OSE | Opérateur de services essentiels. |
| SecNumCloud / EUCS | Schémas de certification européens pour un « cloud de confiance ». |
| Cloud souverain | Infrastructure cloud hébergée et régie par le droit national ou européen. |
| End User Certificate / Non-Transfer Clause | Clauses contractuelles garantissant la non-réexportation de matériels sensibles. |

| | |
|--|---|
| <p>Enforcement Regulation</p> | <p>Règlement européen permettant des contre-mesures commerciales.</p> |
| <p>ACI/Enforcement (couplage)</p> | <p>Mécanisme européen combinant mesures de défense et de rétorsion commerciale.</p> |

Bibliographie

Textes législatifs et réglementaires

Textes européens

Traité sur le fonctionnement de l'Union européenne (TFUE), art. 107.

<https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:12016E107>

Directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 *sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites (Texte présentant de l'intérêt pour l'EEE)*, disponible sur <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016L0943>

Règlement (UE) 2024/1252 du Parlement européen et du Conseil du 11 avril 2024 *établissant un cadre pour garantir un approvisionnement européen sécurisé et durable en matières premières critiques*, disponible sur <https://eur-lex.europa.eu/eli/reg/2024/1252/oj?locale=fr>

Règlement (UE) 2023/2411 relatif à *la protection des indications géographiques pour les produits artisanaux et industriels et modifiant les règlements (UE) 2017/1001 et (UE) 2019/1753*, disponible sur <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32023R2411>

Règlement (UE) 2023/1781 du Parlement européen et du Conseil du 13 septembre 2023 *établissant un cadre de mesures pour renforcer l'écosystème des semi-conducteurs dans l'Union européenne* disponible sur <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32023R1781>

Règlement (UE) 2023/2411 sur les IG artisanales et industrielles : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=OJ:L_202302411

Règlement (UE) 2019/452 du Parlement européen et du Conseil du 19 mars 2019 *établissant un cadre pour le filtrage des investissements directs étrangers dans l'Union*, disponible sur <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32019R0452>

Règlement (UE) 2017/1001 *relatif à la marque de l'Union européenne*, disponible sur <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32017R1001>

Recommandation (UE) 2025/63 de la Commission du 15 janvier 2025 *relative à l'examen des investissements sortants dans des domaines technologiques essentiels pour la sécurité économique de l'Union*, disponible sur https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=OJ:L_202500063

Textes français

LOI n° 2018-670 du 30 juillet 2018 *relative à la protection du secret des affaires*, disponible sur <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037262111>

Loi n° 2016-1691 du 9 décembre 2016 *relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique* disponible sur <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033558528>

Loi n° 68-678 du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères disponible sur <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000501326>

Décret n° 2014-479 du 14 mai 2014 relatif aux investissements étrangers soumis à autorisation préalable disponible sur <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000028933611>

Codes

Code de la consommation - IG non agricoles disponible sur https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006069565/LEGISCTA000032222755/

Code de la propriété intellectuelle - IG disponible sur https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006069414/LEGISCTA000028742898/

Foreign Corrupt Practices Act (FCPA), U.S. DOJ., disponible sur <https://www.justice.gov/criminal-fraud/fcpa>

Section 702 of the Foreign Intelligence Surveillance Act (FISA), disponible sur <https://www.intel.gov/foreign-intelligence-surveillance-act/fisa-section-702>

Rapports d'information Union européenne

EUROPEAN COMMISSION (2021), *EU Cloud Certification Scheme*, disponible sur <https://ec.europa.eu/newsroom/cipr/items/713799/en>

COMMISSION EUROPEENNE, (2021), Rapport au Parlement européen et au Conseil sur *la mise en œuvre de l'article 7(a) du règlement (CE) n° 2271/96 ("règlement de blocage")*, disponible sur <https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52021DC0535>

COMMISSION EUROPEENNE (2021), Communication *Renforcer l'ouverture, la solidité et la résilience de l'économie européenne*, disponible sur <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52021DC0032>

COMMISSION EUROPEENNE, (2021), *Consultation publique sur la révision du règlement de blocage* disponible sur :https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13129-Unlawful-extra-territorial-sanctions-a-stronger-EU-response-amendment-of-the-Blocking-Statute-/public-consultation_fr

Commission européenne, *Rapport sur le règlement de blocage*, COM(2021) 535 final.
<https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52021DC0535>

Rapports d'information institutions françaises

PLASSARD, Ch. (2025), *La guerre économique*, disponible sur https://www.assemblee-nationale.fr/dyn/17/rapports/cion_fin/l17b1757_rapport-information.pdf

CONSEIL D'ETAT (2024), *Rapport sur la souveraineté*, disponible sur <https://www.conseil-etat.fr/publications-colloques/etudes/etudes-annuelles/etude-annuelle-sur-la-souverainete>

SENAT (2023), *Rapport d'information n° 595 Cinq plans pour reconstruire la souveraineté économique de la France*, Commission des affaires économiques, juin 2023, disponible sur <https://www.senat.fr/rap/r21-755/r21-755.html>

ASSEMBLEE NATIONALE (2023), *Rapport public fait au nom de la délégation parlementaire au renseignement relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2022-2023*, disponible sur https://www.assemblee-nationale.fr/dyn/16/rapports/dpr/l16b1454_rapport-information.pdf

ASSEMBLEE NATIONALE, (2019), *Rapport d'information n° 4270 présenté par Raphaël Gauvain, Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et mesures à portée extraterritoriale*, disponible sur : <https://www.vie-publique.fr/files/rapport/pdf/194000532.pdf>

ASSEMBLEE NATIONALE (2019), *Rapport d'information n° 4270 présenté par Raphaël Gauvain, Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et mesures à portée extraterritoriale*, disponible sur <https://www.vie-publique.fr/files/rapport/pdf/194000532.pdf>

MONTAUGE F., LONGUET G. (2019), *Rapport sur la souveraineté numérique*, disponible sur <https://www.senat.fr/rap/r19-007-1/r19-007-11.pdf>

CNIL (2020), *Délibération n° 2020-044 du 20 avril 2020 portant avis sur un projet d'arrêté complétant l'arrêté du 23 mars 2020 prescrivant les mesures d'organisation et de fonctionnement du système de santé nécessaires pour faire face à l'épidémie de covid-19 dans le cadre de l'état d'urgence sanitaire*. Disponible sur https://www.cnil.fr/sites/cnil/files/atoms/files/deliberation_du_20_avril_2020_portant_avis_sur_projet_darrete_relatif_a_lorganisation_du_systeme_de_sante.pdf

FRANCE DIPLOMATIE (2019), *Contrôle des exportations de matériels de guerre*, disponible sur <https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/securite-desarmement-et-non->

[proliferation/desarmement-et-non-proliferation/commerce-transport-et-exportations-d-armes-et-materiels-sensibles/article/controle-des-exportations-de-materiels-de-guerre](https://www.sgdsn.gouv.fr/nos-missions/anticiper-et-prevenir/controler-les-exportations-de-materiels-de-guerre)

SGDSN (2022), *Contrôle les exportations de matériels de guerre*, disponible sur <https://www.sgdsn.gouv.fr/nos-missions/anticiper-et-prevenir/controler-les-exportations-de-materiels-de-guerre>

ANSSI, *Arrêtés sectoriels*, disponible sur <https://cyber.gouv.fr/publications/publication-des-premiers-arretes-sectoriels-relatifs-la-ssi-des-oiv>

MINISTERE DES ARMEES, *Les réglementations américaines du contrôle des exportations*, disponible sur <https://www.defense.gouv.fr/sites/default/files/ministere-armees/Prospectez%20le%20march%C3%A9%20de%20d%C3%A9fense%20am%C3%A9ricain%20en%20appliquant%20les%20r%C3%A9glementations%20en%20mati%C3%A8re%20de%20contr%C3%B4le%20des%20exportations%20%28ITAR%20et%20EAR%29.pdf>

MINARM (2018), *Le droit international appliqué aux opérations dans le cyberspace*, disponible sur <https://www.defense.gouv.fr/sites/default/files/ministere-armees/Droit%20international%20appliqué%20aux%20opérations%20dans%20le%20cyberspace.pdf>

MINARM (2019), *Éléments publics de doctrine de lutte informatique offensive*, disponible sur <https://www.defense.gouv.fr/sites/default/files/comcyber/doctrine%20militaire%20de%20lutte%20informatique%20offensive.pdf>

DGSI, *bulletins flash ingérence*, disponible sur <https://www.dgsi.interieur.gouv.fr/dgsi-a-vos-cotes/contre-espionnage/conseils-aux-entreprises-flash-ingerence>

DGEC/SDES (2023), *Bilan énergétique de la France 2023*, disponible sur <https://www.statistiques.developpement-durable.gouv.fr>

INPI (2021) *Cahier des charges, Indication Géographique, Couteau de Laguiole*, disponible sur <https://base-indications-geographiques.inpi.fr/sites/default/files/CDC%20homologué%20couteau%20de%20Laguiole.pdf>

REPRESENTATION PERMANENTE DE LA FRANCE AUPRES DE L'OFFICE DES NATIONS ET DES ORGANISATIONS INTERNATIONALES A VIENNE (2019), *Contrôle des exportations*, disponible sur <https://onu-vienne.delegfrance.org/controle-des-exportations-1313>

REPRESENTATION PERMANENTE DE LA FRANCE AUPRES DE L'OFFICE DES NATIONS ET DES ORGANISATIONS INTERNATIONALES A VIENNE (2022), *Arrangement de Wassenaar*, disponible sur <https://onu-vienne.delegfrance.org/Arrangement-de-Wassenaar-971>

Sites officiels

Site officiel de l'Advocacy Center disponible sur <https://www.trade.gov/advocacy-center-services>

Site de l'Office of the United States Trade Representative (USTR), Section 301 Tariffs Review, 2019–2020., disponible sur <https://ustr.gov>

Jurisprudences

TRIBUNAL UE, Affaire T-508/08, Laguiole, disponible sur <https://curia.europa.eu/juris/document/document.jsf?docid=44567&doclang=FR>

TRIBUNAL DE L'UE, Affaire T-579/16, Laguiole, disponible sur <https://curia.europa.eu/juris/document/document.jsf?docid=189623&doclang=fr>

TRIBUNAL DE L'UE, Affaire T-623/13, Laguiole disponible sur <https://curia.europa.eu/juris/document/document.jsf?docid=158721&doclang=FR>

Articles

AFP, *Terres rares : la Chine renforce les contrôles sur l'exportation des technologies liées à ces métaux stratégiques*, *Le monde*, 9 octobre 2025 disponible sur : https://www.lemonde.fr/economie/article/2025/10/09/terres-rares-la-chine-renforce-les-controles-sur-l-exportation-des-technologies-liees-a-ces-metaux-strategiques_6645421_3234.html

ALSTOM SA (2024), *Alstom Pleads Guilty and Agrees to Pay \$772 Million Criminal Penalty*, U.S. DOJ, 22 déc. disponible sur <https://www.justice.gov/archives/opa/pr/alstom-pleads-guilty-and-agrees-pay-772-million-criminal-penalty-resolve-foreign-bribery-charges>

AUTAIN R., DUQUENNE S. (2025), *Intelligence et renseignement économiques : une pratique stratégique au service l'entreprise*, *Sécurité et stratégie* n°38, pp. 17-21

BEAUCILLON Ch., (2024), *"Secondary Sanctions: What's in a Name?"* in *The Cambridge Handbook of Secondary Sanctions and International Law*, Cambridge University Press.

CABINET BOUCHARA (n.d), *La saga judiciaire Laguiole*, disponible sur <https://www.cabinetbouchara.com/la-saga-judiciaire-laguiole/>

CGT (2025), *les zones à régime restrictif – fiche pratique et revendications*, disponible sur <https://cgt.fercsup.net/les-dossiers/enseignement-superieur/le-securitaire/article/les-zones-a-regime-restrictif-zrr-fiche-pratique-et-revendications>

CHALMIN Ph. (2022), *Souveraineté et dépendance*, *Revue Défense Nationale* n°487 pp. 46-51

CLERMONT B. (2022), *Le Rafale, un outil de souveraineté et de puissance au service de la France*, *Revue Défense Nationale*, n°847, pp. 59-65

CLUB DROIT (2025), *Le décret Montebourg, entre héritage protectionniste et renouveau permanent*, disponible sur <https://www.portail-ie.fr/univers/2025/le-decret-montebourg-de-2014-entre-heritage-protectionniste-et-renouveau-permanent/>

CNIL (2024), « *Cloud : les risques d'une certification européenne permettant un accès étranger* », 19 juillet 2024. disponible sur <https://www.cnil.fr/fr/cloud-les-risques-dune-certification-europeenne-permettant-lacces-des-autorites-etrangeres>

COLLECTIF (2025), *L'action de la DGSI en matière de sécurité économique*, Sécurité et stratégie n°38, pp. 10-12

COLLECTIF (2024), *Livre blanc sur les investissements sortants* disponible sur <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52024DC0024>

COLON D. (2024), *La Guerre de l'information, Les États à la conquête de nos esprits*, Editions Tallandier.

COMMISSION EUROPÉENNE (2025), *Commission launches record number of trade defence investigations in 2024, 28 juillet 2025*, disponible sur https://policy.trade.ec.europa.eu/news/commission-launches-record-number-trade-defence-investigations-2024-2025-07-28_en

COMMISSION EUROPÉENNE (2024), *Anti-Dumping Investigations – Procedural Framework, DG TRADE, 2024*, disponible sur https://policy.trade.ec.europa.eu/enforcement-and-protection/trade-defence/anti-dumping-measures/anti-dumping-investigations_en

COMMISSION EUROPÉENNE (2023), *EU trade defence measures in force – Annual Statistics 2023, IP/24/4829, 17 juin 2024.*, disponible sur https://ec.europa.eu/commission/presscorner/detail/en/ip_24_4829

COMMISSION EUROPÉENNE (2021), *A New Industrial Strategy for Europe — Strategic Autonomy and Economic Security, COM(2021) 350 final*, disponible sur https://research-and-innovation.ec.europa.eu/strategy/strategy-research-and-innovation/europe-world/international-cooperation/strategic-autonomy-and-european-economic-and-research-security_en

DALLOZ (2025). § 3 - L'Indication Géographique protégeant les produits industriels et artisanaux (IGPIA). Dans Répertoire de droit européen. Dalloz

DEBAECQUE AVOCATS, (2023), *Protection des IGPIA en Europe*, disponible sur <https://debaecque-avocats.com/protection-des-igpia-europe/>

DE MAISON ROUGE O. (2024), *Un renseignement économique et financier à parfaire*, *Revue internationale d'intelligence économique*, n°16, pp. 13-35

DE MAISON ROUGE O. (2016), *Le droit du renseignement*, LexisNexis.

DE MAISON ROUGE O. (2012), *Le droit de l'intelligence économique : Patrimoine informationnel et secrets d'affaires*, Edition Lamy.

DEPRAU A. (2014), *Intelligence économique et protection du patrimoine informationnel*, Éditions Universitaires Européennes.

FEREY A. (2018), *Droit de la guerre ou guerre du droit ? Réflexion française sur le lawfare*, Revue Défense Nationale, pp. 55-60.

GALLOUX J-C. (2017), *L'adoption de la directive sur les secrets des affaires*, RTD. com., disponible sur <https://shs.hal.science/halshs-02259891>

HARBULOT Ch. (2019), *La mutation du renseignement économique*, Prospective et stratégie, n°10, pp. 53-61.

INPI. (n.d.). Une protection européenne pour les indications géographiques artisanales et industrielles, disponible sur <https://www.inpi.fr/a-la-une/une-protection-europeenne-pour-les-indications-geographiques-artisanales-et-industrielles>

JUILLET A. (2025), *Le renseignement économique*, Sécurité et stratégie n° 38, pp. 13-16

LABORDE-BALEN S. (2025), *Big Data en 2025 : jusqu'où ira l'explosion des données mondiales ?*, Solutions numériques, disponible sur : <https://www.solutions-numeriques.com/communiques/big-data-en-2025-jusquou-ira-lexplosion-des-donnees-mondiales/>

KAMINA P. (2024), *Droit anglo-américain des propriétés intellectuelles*, T.2, 2e édition, disponible sur <https://univ-lyon3.hal.science/hal-04489179v1>

KARATHANASIS Th. (2022), *Instrumentalisation du droit et interférences hybrides, un enjeu sécuritaire pour l'Union européenne*, Cahiers de la sécurité et de la justice, n°55, pp. 105-112

MARRO-BERNADOU S. (2024), *note de lecture sur l'ouvrage de Daniel MAINGUY, Droit de la « guerre atypique » : Réflexions sur les conflits non armés et non militaires (lawfare, guerre économique et informationnelle)*, Paris, LGDJ, 2023, 336 p., Etudes Françaises de renseignement et de cyber, n°2, pp. 283-287

MOFCOM (Chine) (2024), *Anti-Dumping Investigation on EU Brandy*, 5 janvier 2024. disponible sur <http://english.mofcom.gov.cn>

MOFCOM (Chine) (2024), *Anti-Dumping Investigation on EU Pork*, 17 juin 2024. disponible sur <http://english.mofcom.gov.cn>

MONTARDI L. (2025), *Investissements étrangers dans les secteurs stratégiques : nouvel angle mort de la veille économique des États*, Sécurité et stratégie, n°38, pp. 40-45

PEREZ E. (2025), *L'intelligence économique, clé stratégique pour un secteur énergétique en mutation*, Sécurité et stratégie, n°38, pp. 22-24.

PHILIPPE A. (2025), *guerres économiques mondiales*, France Soir

PITRON E. (2025), *Le renseignement économique dans le secteur privé : le nécessaire respect d'un cadre éthique et juridique exigeant*, Sécurité et stratégie, n°38, pp. 30-34

REUTERS (2025), *China expands rare earth restrictions, targets and chips users*, disponible sur https://www.reuters.com/world/china/china-tightens-rare-earth-export-controls-2025-10-09/?utm_source=chatgpt.com

REUTEURS (2025), *China tightens rare-earth export controls*, disponible sur <https://www.reuters.com/world/china/china-tightens-rare-earth-export-controls-2025-10-09>

TOUMI A-S, LAMBAUDIE F., PAQUE X., SUAREZ A. et JEULIN E. (2022), *Guerre de l'information "Guide de survie pour entreprise", Comment se défendre et passer à l'attaque légalement dans la jungle informationnelle et concurrentielle à laquelle doit désormais faire face toute entreprise ?*, Mémoire rédigé dans le cadre de l'Ecole de Guerre Économique, disponible sur <https://www.ege.fr/infoguerre/guerre-de-linformation-guide-de-survie-pour-lentreprise>

WARUSFEL B (2023), *Le droit peut-il encore protéger le secret ?* Publication Titre VII, disponible sur <https://www.conseil-constitutionnel.fr/publications/titre-vii/le-droit-peut-il-encore-proteger-le-secret>

WEIL B. (2025), « *FCPA Enforcement Actions Against Foreign Companies from OECD Convention Peer Countries* », FCPA Professor, 10 janv. 2025, disponible sur <https://fcpaprofessor.com/fcpa-enforcement-actions-against-foreign-companies-from-oecd-convention-peer-countries>

Table des matières

| | |
|--|-----------|
| SOMMAIRE | 3 |
| INTRODUCTION | 4 |
| <u>I. COERCITION ECONOMIQUE : EMBARGOS, RESTRICTION EXPORT, ACCES MARCHES, SANCTIONS EXTRATERRITORIALES</u> | 5 |
| A. ENTRE PRESSION AMERICAINE ET SOUVERAINETE FRANÇAISE : LE POIDS DE L'EXTRATERRITORIALITE DU DROIT DANS LA COMPETITION ECONOMIQUE | 5 |
| B. LE CONTROLE DES EXPORTATIONS, UN OUTIL JURIDIQUE FACE AUX DEPENDANCES ETRANGERES | 7 |
| C. MESURES DE RETORSION AGRESSIVES : DROITS DE DOUANE US, COORDINATION UE-US ET REGLEMENT DE BLOCAGE | 9 |
| « ENTERINER » DES RETORSIONS TARIFAIRES PAR DES ACCORDS UE-US (CADRE, TRQ, SNAPBACK) | 10 |
| PROTEGER ET RIPOSTER A L'ECHELLE EUROPEENNE : LE REGLEMENT DE BLOCAGE ET LES OUTILS OFFENSIFS. | 10 |
| D. DUMPING EXTRA-EUROPEEN | 12 |
| <u>II. FACE AUX POLITIQUES ETRANGERES DE CAPTATION, DES INSTRUMENTS DE CONTROLE DES INVESTISSEMENTS ET UN CONTRE-RENSEIGNEMENT ECONOMIQUE ET INDUSTRIEL A AMELIORER</u> | 14 |
| A. UN INSTRUMENT EN CONSTANTE AMELIORATION : LE CONTROLE DES INVESTISSEMENTS ENTRANTS ET SORTANTS | 14 |
| B. LA PROTECTION DU PATRIMOINE INFORMATIONNEL PRIVE : UNE LUTTE CONTRE L'ESPIONNAGE ECONOMIQUE | 16 |
| LA GENEVE DU LAWFARE DEFENSIF FRANÇAIS : LA LOI DE BLOCAGE DE 1968 | 17 |
| LAGUIOLE OU L'EVEIL D'UN SAVOIR-FAIRE FRANÇAIS MENACE | 17 |
| LA LOI SUR LE SECRET DES AFFAIRES : UNE REPOSE FRANÇAISE A LA GUERRE INVISIBLE DE L'INFORMATION | 19 |
| C. L'ENTREE EN JEU DU MONDE DU RENSEIGNEMENT A FINS DE PREVENTION DES INGERENCES ECONOMIQUES PRENANT LA FORME DE CAPTATIONS INDUES. | 21 |
| DES MESURES PUREMENT DEFENSIVES | 21 |
| DES DISPOSITIFS LACUNAIRES | 22 |
| D. UN ARSENAL JURIDIQUE CONTRE LES CYBERMENACES BIEN PENSE. | 23 |
| LES INSTRUMENTS PROPRES A CERTAINES ENTREPRISES. | 23 |
| LES INSTRUMENTS S'APPLIQUANT A L'ENSEMBLE DES ACTEURS | 24 |
| <u>III. DEPENDANCE STRUCTURELLE : CHAINES APPRO, ENERGIE, STANDARDISATION US</u> | 25 |
| A. LES VULNERABILITES DANS LES AFFAIRES TRANSACTIONNELLES : CLOUD, SERVICES JURIDIQUE ET D'INVESTIGATION. | 25 |
| CLOUD ET DONNEES | 26 |

| | |
|--|-----------|
| DEPENDANCE JURIDIQUE (CABINETS D'AVOCATS ET D'INVESTIGATION "FORENSIC") | 26 |
| L'ABSENCE DE "GEANTS" CAPABLES DE REpondre AUX BESOINS | 27 |
| B. LA REAFFIRMATION DE LA SOUVERAINETE JURIDIQUE FACE A LA VULNERABILITE DES CHAINES D'APPROVISIONNEMENT CRITIQUES | 28 |
| C. L'ENERGIE, TALON D'ACHILLE DE LA COMPETITIVITE EUROPEENNE | 30 |
| ÉTAT DES LIEUX ET IMPACT DE L'ENERGIE SUR LA COMPETITIVITE | 30 |
| DEFIS REGLEMENTAIRES ET GEOPOLITIQUES | 30 |
| CONCLUSION ET OUVERTURE | 33 |
| ANNEXES | 35 |
| ANNEXE 1. ORIGINE DES INVESTISSEMENTS ETRANGERS DANS L'UE, SELON LEUR FINALITE (INVESTISSEMENTS VISANT LA CREATION OU L'ACQUISITION DU CAPITAL D'UNE ENTREPRISE). | 35 |
| ANNEXE 2. TABLEAU RECAPITULATIF DES DEGRES ET NATURE DE L'IMPACT PAR TYPE DE VULNERABILITE | 36 |
| ANNEXE 3- EXEMPLES EMBLEMATIQUES DES ENTREPRISES FRAPPEES PAR L'EXTRATERRITORIALITE AMERICAINE. | 37 |
| ANNEXE 4. RECOMMANDATIONS DETAILLEES DE LA PARTIE CONSACREE AUX VULNERABILITES DANS LES AFFAIRES TRANSACTIONELLES | 39 |
| ANNEXE 5. LISTE DES RECOMMANDATIONS. | 41 |
| GLOSSAIRE | 45 |
| CONCEPTS GÉNÉRAUX | 45 |
| TEXTES, DISPOSITIFS ET LOIS | 46 |
| INSTITUTIONS ET ACTEURS | 47 |
| NOTIONS ECONOMIQUES ET INDUSTRIELLES | 48 |

| | |
|---|-----------|
| BIBLIOGRAPHIE | 50 |
| TEXTES LEGISLATIFS ET REGLEMENTAIRES | 50 |
| TEXTES EUROPEENS | 50 |
| TEXTES FRANÇAIS | 51 |
| CODES | 51 |
| RAPPORTS D'INFORMATION UNION EUROPEENNE | 51 |
| RAPPORTS D'INFORMATION INSTITUTIONS FRANÇAISES | 52 |
| SITES OFFICIELS | 53 |
| JURISPRUDENCES | 54 |
| ARTICLES | 54 |
| TABLE DES MATIERES | 58 |
| DROITS D'AUTEURS | 61 |

Droits d'auteurs

Promotion MSIJ/SIJ 01 – octobre 2025

Ce mémoire est une œuvre protégée par le droit d'auteur (article L. 111-1 et suivants du code de la propriété intellectuelle). Toute reproduction ou représentation intégrale ou partielle, par quelque procédé que ce soit, faite sans le consentement des auteurs et de leurs ayants droit, est illicite et constitue une contrefaçon sanctionnée par les articles L. 335-2 et suivants du code de la propriété intellectuelle.

Aucune diffusion, reproduction adaptation ou utilisation de ce document, en dehors de la consultation individuelle et privée, n'est autorisée sans l'accord écrit préalable des auteurs.