Les opérateurs satellitaires de télécommunications à l'épreuve des contextes de conflit et à haut risque

Fonder et encadrer une diligence raisonnable renforcée en matière de droits humains

Mémoire présenté par Laurie ABSALON

Direction scientifique : Madame Charlotte MICHON, Charlotte Michon Avocats
Direction opérationnelle : Madame Cecilia DIAS, Eutelsat Group

Master Droit & Éthique des Affaires
Année universitaire 2025-2026

REMERCIEMENTS

L’achèvement de ce mémoire referme un parcours commencé il y a plusieurs années, et dont je mesure aujourd’hui qu’il ne s’est jamais accompli seul. À l’heure d’en écrire les dernières lignes, je souhaite exprimer ma reconnaissance à celles et ceux qui l’ont rendu possible.

Je remercie Madame Roxana Family, directrice du Master Droit & Éthique des Affaires, pour la qualité de la formation qu’elle dirige et pour l’exigence dont elle a fait preuve à notre égard tout au long de cette année. Elle a su donner à ce parcours une cohérence qui dépasse la seule acquisition de connaissances.

J’adresse également mes remerciements à Madame Charlotte Michon, qui a accepté d’assurer la direction scientifique de ce mémoire et dont les orientations ont contribué à en délimiter le sujet.

Ma gratitude va tout particulièrement à Madame Cecilia Dias, Senior Compliance Manager, qui a encadré mon alternance. Elle m’a accueillie dans une fonction que je découvrais, m’a confié des dossiers exigeants et m’a laissé la latitude d’y prendre position, tout en demeurant disponible chaque fois que j’en avais besoin. C’est en travaillant à ses côtés que j’ai compris ce que la conformité engage réellement lorsqu’elle se pratique, et ce mémoire porte la marque de cet apprentissage. Qu’elle trouve ici l’expression de ma reconnaissance sincère.

Je remercie également Madame Trisha Bunomally, Group Data Protection Officer, pour son écoute, sa disponibilité et la bienveillance avec laquelle elle m’a accueillie. J’adresse aussi ma reconnaissance à l’ensemble de l’équipe avec laquelle j’ai eu la chance de travailler, pour la qualité des échanges que nous avons eus tout au long de cette mission.

Mes remerciements les plus personnels vont enfin à mes proches. À mes parents, dont le soutien n’a jamais faibli au cours de ces années d’études et sans lesquels rien de ce parcours n’aurait été envisageable. À ma sœur, Emma, qui a toujours été là pour moi, à chaque étape et sans que j’aie jamais eu à le demander. Et à Anis, pour son écoute quotidienne, sa patience durant les mois qu’a demandés ce travail et son soutien indéfectible.

Que toutes et tous trouvent ici l’expression de ma sincère gratitude.

SOMMAIRE

Note de méthode et déclaration d'indépendance....4
Introduction....6

Partie 1. L'inadaptation du cadre ordinaire et les fondements d'une diligence renforcée et graduée....12

Chapitre 1. Un cadre normatif conçu pour la chaîne d'approvisionnement, et moins pour une infrastructure critique....12
Section 1. De l'engagement volontaire à l'obligation de moyens....12
Section 2. L'angle mort des contextes à haut risque....16
Section 3. La démonstration empirique du vide....20

Chapitre 2. Les fondements d'une diligence renforcée et graduée....25
Section 1. Le fondement tiré de la nature du service....25
Section 2. Le fondement tiré du contexte : construction d'une échelle....27
Section 3. Le fondement tiré du statut de l'opérateur....31

Partie 2. Le contenu opérationnel de la diligence graduée et ses tempéraments....35

Chapitre 1. Le contenu : construire une diligence calibrée sur le degré du contexte....35
Section 1. L'évaluation contextualisée....35
Section 2. La gouvernance de la décision d'urgence....37
Section 3. Les leviers d'action et leur mise en œuvre....38

Chapitre 2. Les tempéraments : la mesure juste de la responsabilité....41
Section 1. Le refus du garant universel....41
Section 2. La cartographie des risques encourus par l'opérateur....43
Section 3. Combler le vide : quatre voies....46

Conclusion....49

Bibliographie....51
Annexes....60
Annexe n° 1. Échelle graduée de vigilance : matrice de qualification et de conséquences....60
Annexe n° 2. Trame du dossier de décision de maintien ou de suspension....61
Annexe n° 3. Circuit de traitement d'une demande étatique de suspension....62
Annexe n° 4. Connaissance de l'usage : déclaration, signaux d'alerte, clausier et mécanisme d'alerte....63
Annexe n° 5. La chaîne d'usage : savoir, vérifier, influencer....64
Annexe n° 6. Déploiement de l'échelle graduée dans l'entreprise : feuille de route....65
Table des matières....66

Note de méthode et déclaration d'indépendance

Ce mémoire a été rédigé alors que j'effectuais mon alternance au sein d'Eutelsat Group, en qualité de Junior Compliance Officer. L'entreprise est un opérateur satellitaire de télécommunications, c'est-à-dire qu'elle appartient à la catégorie même dont le présent travail examine les obligations. Cette position appelle une explication, et il m'a paru préférable de la donner d'emblée plutôt que de la laisser deviner.

Ce que cette situation m'a apporté est une compréhension concrète du secteur : la manière dont une capacité satellitaire est commercialisée, la distance qui sépare l'opérateur de l'utilisateur final, le fonctionnement des obligations d'autorisation et de contrôle, et la difficulté pratique que représente, pour une direction de la conformité, une décision qui doit être prise en quelques heures sans que le droit indique le sens dans lequel trancher. C'est de cette expérience qu'est né le sujet.

Ce que cette situation m'interdisait était tout aussi net. Je n'ai utilisé aucune information interne, aucun document confidentiel ni aucune donnée couverte par le secret des affaires. L'intégralité des développements repose sur des sources publiques : textes normatifs, décisions de justice, rapports d'organisations internationales, communiqués et documents d'enregistrement universel accessibles à tous, presse et travaux doctrinaux. Les mentions faites d'Eutelsat Group renvoient exclusivement à des éléments rendus publics par l'entreprise elle-même ou par une autorité, notamment la procédure conduite devant l'Autorité de régulation de la communication audiovisuelle et numérique en 2022.

Ce mémoire a été rédigé avec l'assistance d'un outil d'intelligence artificielle générative, employé sous ma direction pour la recherche et la vérification de sources, des propositions de formulation et de structure, ainsi que la mise en forme du document. Le choix du sujet, la problématique, l'échelle graduée proposée et les arbitrages de fond procèdent de mon travail. Les éléments documentaires sur lesquels repose la démonstration ont, pour l'essentiel, été réunis par mes soins : publications réglementées de l'opérateur étudié, communiqués et sources institutionnelles mobilisés notamment au paragraphe 8.

Ce mémoire n'engage que son auteur et ne constitue pas une position de l'entreprise.

Introduction

Un satellite de télécommunications ne fait rien d'autre que transporter des signaux. Il reçoit ce qu'on lui envoie depuis le sol et le renvoie ailleurs. Là où les antennes-relais ont été détruites, ou n'ont jamais existé, il devient le seul moyen de téléphoner, d'envoyer une image ou de piloter un drone. L'entreprise qui l'exploite décide donc, très concrètement, de qui peut communiquer et de qui ne le peut plus.

Le 5 février 2026, les autorités ukrainiennes annoncent que les terminaux Starlink utilisés par les soldats russes ont cessé de fonctionner. Notons qu'un terminal est une petite antenne posée au sol, qui permet de se connecter au réseau de satellites et porte un numéro rattaché à son contrat de vente. Kiev et l'entreprise américaine ont dressé la liste des antennes régulièrement déclarées, puis désactivé à distance toutes les autres[1]. Résultat : en quelques heures, une entreprise privée a coupé les communications d'une armée en guerre.

Pourtant, le même geste avait produit l'effet inverse trois ans auparavant. Selon une enquête de l'agence Reuters publiée le 25 juillet 2025, la couverture aurait été interrompue à l'automne 2022 au-dessus d'une zone du sud de l'Ukraine, alors que l'armée ukrainienne y menait une offensive. Les unités engagées se seraient retrouvées sans liaison, incapables de piloter leurs drones et de coordonner leurs tirs. L'entreprise n'a jamais confirmé l'épisode et a contesté l'exactitude de l'enquête[2]. Que les faits soient ou non établis, ils posent une question à laquelle personne ne sait répondre : qui aurait dû décider, cette nuit-là, si la couverture devait être maintenue ? Aucune règle de droit ne le prévoyait, et aucune ne le prévoit encore.

Le droit français a rencontré la même question le 8 septembre 2022. Reporters sans frontières saisit l'Autorité de régulation de la communication audiovisuelle et numérique afin qu'elle mette en demeure un opérateur satellitaire français de cesser la diffusion de trois chaînes russes. Le 29 septembre, l'Autorité se déclare incompétente. Une ordonnance de référé du Conseil d'État, rendue le 9 décembre, devient nécessaire pour qu'elle réexamine sa position. Elle met l'opérateur en demeure le 14 décembre, lequel s'exécute dans le délai imparti[3]. Interrogé sur le fondement de cette compétence retrouvée, le ministère de l'Europe et des Affaires étrangères a précisé que l'Autorité avait pu intervenir parce que l'Ukraine, à la

[1] BALMFORTH (T.), « Ukraine says Starlink terminals used by Russia deactivated in blow to Moscow », Reuters, 5 février 2026.

[2] ROULETTE (J.), BRYAN-LOW (C.) et BALMFORTH (T.), « Musk ordered shutdown of Starlink satellite service as Ukraine retook territory from Russia », Reuters, 25 juillet 2025, à propos du secteur de Beryslav. Ni SpaceX ni M. Elon Musk n'ont confirmé l'épisode ; un porte-parole de la société a qualifié l'enquête d'inexacte.

[3] CE, ord. réf., 9 décembre 2022, Association Reporters sans frontières, n° 468969, suspendant, sur le fondement de l'article L. 521-1 du code de justice administrative, la décision du président de l'Arcom du 29 septembre 2022 et lui enjoignant de réexaminer la demande ; Arcom, mise en demeure d'Eutelsat SA, 14 décembre 2022. La demande visait la diffusion des chaînes Rossiya 1, Perviy Kanal et NTV.

différence de la Russie, avait ratifié la Convention européenne sur la télévision transfrontière[4]. Que le régulateur français ait pu agir, à l'égard d'un opérateur français, dans un conflit majeur aux frontières de l'Union, a donc tenu à ce qu'un État tiers eût ratifié une convention de 1989. Le régulateur n'était pas absent. Il était sans titre.

Le communiqué par lequel l'opérateur rend compte de son exécution, le 21 décembre 2022, porte cependant sur deux situations : la Russie, et l'Iran[5]. D'un côté un conflit armé international ; de l'autre un État qui n'est en guerre avec personne, mais qui use de sa maîtrise des flux pour couper une part de sa population de l'information. Les deux situations exposent l'opérateur à des risques comparables pour les droits fondamentaux, mais ne relèvent pas de la même qualification, et le droit international humanitaire n'a rien à dire de la seconde. Un travail limité au conflit armé laisserait échapper une part considérable du risque réel.

Ces épisodes ne ressemblent en rien aux affaires qui ont façonné le droit de la vigilance depuis quinze ans. On n'y trouve ni effondrement d'usine ni sous-traitant défaillant, mais une infrastructure dont la seule disponibilité met en jeu des droits fondamentaux. Dès 2022, le Haut-Commissariat aux droits de l'homme relevait que les coupures d'accès portent atteinte à un large ensemble de droits[6]. La particularité de l'opérateur satellitaire tient au fait que ce qu'il vend n'est pas un produit dont il faudrait garantir la sûreté, mais une capacité dont la présence et l'absence produisent l'une comme l'autre des effets sur les personnes. La même bande passante achemine les communications d'un hôpital de campagne et celles d'un poste de commandement. La suspendre protège d'un usage et prive de l'autre. Aucune option n'est neutre.

C'est à ce type de situation que le droit international des droits humains a répondu. Depuis les Principes directeurs relatifs aux entreprises et aux droits de l'homme, adoptés en 2011 sous l'impulsion de John Ruggie, la responsabilité de l'entreprise de respecter les droits humains se traduit par un processus (identifier, prévenir, atténuer, réparer) et par une gradation de son implication (selon qu'elle cause l'atteinte, qu'elle y contribue, ou qu'elle y soit seulement liée par une relation d'affaires)[7]. Le Groupe de travail des Nations unies a précisé en 2020 que les

[4] Réponse du ministère de l'Europe et des Affaires étrangères à la question écrite n° 3485 de M. Benjamin Haddad, « Eutelsat S.A. – Lutte contre la propagande russe », Assemblée nationale, XVIe législature, question publiée au Journal officiel du 29 novembre 2022, p. 5728, réponse publiée au Journal officiel du 3 janvier 2023, p. 96.
[5] EUTELSAT COMMUNICATIONS, communiqué relatif à la cessation de la diffusion de certaines chaînes en Russie et en Iran, 21 décembre 2022.
[6] HAUT-COMMISSARIAT DES NATIONS UNIES AUX DROITS DE L'HOMME, Internet shutdowns : trends, causes, legal implications and impacts on a range of human rights, A/HRC/50/55, 13 mai 2022, établi en application de la résolution 47/16 du Conseil des droits de l'homme.
[7] HAUT-COMMISSARIAT DES NATIONS UNIES AUX DROITS DE L'HOMME, Principes directeurs relatifs aux entreprises et aux droits de l'homme : mise en œuvre du cadre de référence « protéger, respecter et réparer » des Nations unies, Nations unies, New York et Genève, 2011, spéc. principes 13, 17 à 21 et 24.

contextes de conflit appellent une intensification de cette diligence[8], et le Programme des Nations unies pour le développement en a formalisé la méthode en 2022 sous le nom de *heightened human rights due diligence*[9]. Plus le risque est grave, rapide et irréversible, plus la vigilance doit être intense.

Reste à savoir si ce raisonnement a une portée juridique. Or, c'est à ce stade que la difficulté juridique apparaît.

Les deux seuls textes qui imposent aujourd'hui un comportement, la loi du 27 mars 2017 et la directive (UE) 2024/1760 telle que révisée en février 2026, reposent l'un et l'autre sur un critère d'effectif de cinq mille salariés[10]. Or le principal opérateur satellitaire français n'en emploie que 1 639, dont 612 en France[11]. Il est hors du champ de l'un comme de l'autre. Ne demeure à sa charge qu'une obligation de publication, qui impose de rendre compte des incidences sans prescrire directement un comportement déterminé.

Résultat : voici un opérateur dont l'État français est le premier actionnaire, qui a conclu un contrat-cadre avec les forces armées, qui siège au consortium concessionnaire de la constellation souveraine européenne et dont les faisceaux couvrent l'Europe, le Moyen-Orient et l'Afrique. Aucune obligation contraignante de diligence en matière de droits humains ne pèse sur lui. Le constat vise une catégorie d'acteurs et non une entreprise. Le problème réside donc moins dans le comportement de l'entreprise que dans l'absence de cadre normatif applicable.

Ce vide aurait pu se combler, or il s'est élargi. La révision de février 2026 a relevé les seuils, allégé les obligations et abandonné le régime européen harmonisé de responsabilité civile[12]. Elle arrive donc à contretemps, la contrainte juridique se relâchant au moment même où ces infrastructures se trouvent le plus exposées.

Ensuite, la proposition de règlement européen sur l'espace du 25 juin 2025 recense treize législations nationales, d'autres États membres préparant ou révisant la leur[13]. Aucun de ses trois piliers ne porte sur les droits humains, et son entrée en vigueur est envisagée au 1er janvier 2030.

---

[8] GROUPE DE TRAVAIL DES NATIONS UNIES SUR LA QUESTION DES DROITS DE L'HOMME ET DES SOCIÉTÉS TRANSNATIONALES ET AUTRES ENTREPRISES, Entreprises, droits de l'homme et régions touchées par un conflit : vers une action renforcée, A/75/212, 21 juillet 2020.

[9] PROGRAMME DES NATIONS UNIES POUR LE DÉVELOPPEMENT, Heightened Human Rights Due Diligence for Business in Conflict-Affected Contexts : A Guide, PNUD, 2022.

[10] Loi n° 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre, art. 1er ; directive (UE) 2024/1760 du Parlement européen et du Conseil du 13 juin 2024, modifiée par la directive (UE) 2026/470 du 24 février 2026, JOUE L, 2026/470, 26 février 2026.

[11] EUTELSAT COMMUNICATIONS, Document d'enregistrement universel 2024-25, déposé auprès de l'Autorité des marchés financiers le 30 octobre 2025 sous le numéro D.25-0693, complété par l'amendement déposé le 24 novembre 2025 ; effectifs, section 3.3.1.4, p. 159. Les données de l'exercice clos le 30 juin 2026 sont issues du communiqué de résultats annuels du 7 août 2026.

[12] Directive (UE) 2026/470, préc.

[13] Proposition de règlement du Parlement européen et du Conseil relatif à la sécurité, à la résilience et à la durabilité des activités spatiales dans l'Union, COM(2025) 335 final, 25 juin 2025.

La négociation est en cours[14]. Dans le même intervalle, la constellation IRIS² a franchi les étapes qui la mèneront à une mise en service progressive dès 2029[15]. L'Europe construit donc une infrastructure de communication souveraine à vocation duale, sous un régime d'autorisation qui n'interroge pas ses effets sur les populations. La fenêtre législative est ouverte.

C'est cette brèche que le présent mémoire se propose d'examiner et, autant qu'il est possible à un travail de cette nature, de contribuer à combler.

Encore faut-il délimiter le champ. Sont ici visées les sociétés qui exploitent des capacités de communication par satellite et les commercialisent, directement ou par l'intermédiaire de distributeurs, de partenaires techniques ou de clients institutionnels. L'observation de la Terre, la navigation, les activités de lancement et la fourniture de contenus en sont écartées. Ce découpage n'est pas de commodité. Il isole une configuration singulière : celle d'un acteur qui vend une capacité de transport neutre en elle-même, sans maîtrise du contenu transporté ni, le plus souvent, connaissance directe de celui qui l'utilisera.

L'expression retenue dans le titre, « contextes de conflit et à haut risque », transpose une catégorie du droit de l'Union. Le règlement (UE) 2017/821 parle, lui, de « zones de conflit ou à haut risque », et range sous ce nom les zones en situation de conflit armé ou fragiles à l'issue d'un conflit, ainsi que celles où la gouvernance et la sécurité font défaut[16]. Le double glissement est délibéré. « Contextes » a été préféré à « zones » parce qu'une capacité satellitaire ne se localise pas comme un gisement, et la conjonction « et » marque que les deux hypothèses sont l'une et l'autre visées, sans qu'il faille les cumuler. La catégorie relève du droit dur, et elle n'exige pas qu'un conflit armé soit juridiquement caractérisé. Cependant, son défaut est qu'elle est conçue pour l'extraction minière : elle ne connaît que la défaillance de l'État. Le risque propre aux communications naît de sa maîtrise, c'est-à-dire de l'aptitude d'un appareil d'État solide à orienter ou restreindre les flux.

Deux exclusions et une précision achèvent ce cadrage. La responsabilité pénale internationale des personnes morales et le droit des conflits armés pris pour lui-même resteront hors du propos. Le droit international humanitaire n'est mobilisé qu'à titre de grille de qualification, le centre de gravité demeurant la diligence raisonnable en matière de droits

[14] Projet de rapport de la commission ITRE du Parlement européen, rapporteure E. Donazzan, 3 mars 2026, PE784.432v01-00 ; texte de compromis de la présidence du Conseil, mars 2026. Lors de la réunion du Conseil du 29 mai 2026, les États membres ont relevé que la portée du texte et le traitement des activités à double usage demeuraient des questions ouvertes.

[15] COMMISSION EUROPÉENNE, contrat de concession de la constellation IRIS² conclu avec le consortium SpaceRISE, 16 décembre 2024 ; accord de mise en œuvre du 7 août 2026.

[16] Règlement (UE) 2017/821 du Parlement européen et du Conseil du 17 mai 2017 fixant des obligations liées au devoir de diligence à l'égard de la chaîne d'approvisionnement pour les importateurs de l'Union qui importent de l'étain, du tantale et du tungstène, leurs minerais et de l'or provenant de zones de conflit ou à haut risque, art. 2, point f) ; voir également la recommandation (UE) 2018/1149 de la Commission du 10 août 2018.

humains, saisie comme un processus juridiquement appréciable et non comme un engagement volontaire. L'état du droit, ensuite, est arrêté au 21 août 2026, postérieurement à l'entrée en vigueur de la directive (UE) 2026/470 et à la signature de l'accord de mise en œuvre de la constellation IRIS².

Le présent sujet oblige d'abord à trancher une question restée en suspens : la diligence raisonnable est-elle un standard de conduite dont l'intensité varie avec le contexte, ou une obligation dont le contenu est fixé par un texte et qui ne vaut que dans le champ de ce texte ? Retenir la première permet de fonder une exigence renforcée hors de tout seuil et de la graduer. Retenir la seconde laisse les opérateurs satellitaires en apesanteur normative. Il faut au passage reprendre la question de l'imputation lorsque l'activité se déploie en cascade, objection que TotalEnergies a opposée au tribunal judiciaire de Paris, puis reprise à l'appui de son appel[17].

Ensuite, un opérateur qui doit décider de maintenir ou de suspendre un service en contexte à haut risque le fait sur une information partielle, sous une pression étatique, contractuelle et médiatique simultanée. Cette décision engage le risque pénal, le risque civil, la réputation et, depuis peu, la valeur actionnariale. Or, aucune méthode consolidée n'existe pour la préparer, la documenter ou la défendre.

Enfin, la fenêtre législative décrite plus haut est ouverte, et les véhicules susceptibles de recevoir une telle exigence existent déjà. Le régime d'autorisation des opérations spatiales permet ainsi de retirer ou de suspendre une autorisation lorsque l'opération apparaît de nature à compromettre le respect par la France de ses engagements internationaux, au nombre desquels figurent les conventions relatives aux droits humains[18]. Un mémoire ne modifie pas un règlement en cours de négociation. Il peut établir que l'instrument existe, et qu'aucune catégorie juridique nouvelle n'est nécessaire pour s'en servir.

Ces éléments conduisent à la question suivante :

> **Lorsqu'ils opèrent dans des contextes de conflit ou à haut risque, à quelles conditions une exigence de diligence raisonnable renforcée en matière de droits humains peut-elle être juridiquement imposée aux opérateurs satellitaires de télécommunications, et selon quelles modalités peut-elle être graduée et rendue effective sans transformer l'opérateur en garant d'usages qu'il ne maîtrise pas ?**

[17] TJ Paris, 25 juin 2026, n° RG 22/03403, Notre affaire à tous et autres c/ TotalEnergies SE, qui écarte l'objection. La société a annoncé son appel le 27 juillet 2026 ; la décision n'est donc pas définitive.
[18] Loi n° 2008-518 du 3 juin 2008 relative aux opérations spatiales, art. 4 et 9. Le rattachement est développé infra, § 18.

Cette interrogation sera notre fil conducteur : qui décide, à quel moment, et qui en répond, de l'État, de l'autorité de régulation ou de l'entreprise ?

Y répondre suppose deux démarches successives. Il faut d'abord établir que le cadre de vigilance ordinaire est structurellement inadapté aux opérateurs satellitaires intervenant dans de tels contextes, puis dégager les fondements d'une exigence renforcée susceptible d'être graduée selon l'intensité du risque (**Partie 1**). Il faut ensuite en déterminer le contenu à chaque degré de l'échelle et en fixer les limites, faute de quoi elle oscillerait entre une responsabilité si diluée qu'elle ne protégerait personne et des obligations si lourdes qu'elles paralyseraient toute décision (**Partie 2**).

Partie 1. L'inadaptation du cadre ordinaire et les fondements d'une diligence renforcée et graduée

Chapitre 1. Un cadre normatif conçu pour la chaîne d'approvisionnement, et moins pour une infrastructure critique

Section 1. De l'engagement volontaire à l'obligation de moyens

§ 1. Les Principes directeurs de 2011 et la structure de la diligence

Il faut partir d'un échec, car il explique la forme qu'a prise la diligence raisonnable. En 2003, un projet de normes sur la responsabilité des sociétés transnationales, construit sur l'idée que les entreprises seraient débitrices d'obligations de même nature que celles des États, est rejeté dès l'année suivante[19]. De cet enlisement naît une méthode différente : plutôt que de créer des obligations nouvelles, on décrira ce que les entreprises font déjà lorsqu'elles gèrent sérieusement un risque. John Ruggie présente en 2008 un cadre en trois piliers : obligation de l'État de protéger, responsabilité de l'entreprise de respecter, accès des victimes à des voies de recours[20], approuvé sans vote en 2011 sous la forme des Principes directeurs[21].

L'apport majeur de ce texte réside moins dans la consécration d'une responsabilité de respecter les droits humains que dans la formalisation des mécanismes permettant d'en apprécier la mise en œuvre effective. Le principe 17 définit la diligence raisonnable comme un processus continu en quatre temps : identifier et évaluer les incidences négatives réelles ou potentielles, en intégrer les conclusions et agir en conséquence, suivre l'efficacité des mesures prises, rendre compte de la manière dont les incidences sont traitées[22]. Un professionnel de la conformité reconnaîtra dans ce vocabulaire celui de l'article 17 de la loi Sapin II, ou du dispositif de lutte contre le blanchiment[23]. Même séquence, même logique probatoire, même déplacement de l'objet du contrôle : ce que l'on apprécie n'est pas l'absence d'incident, mais le sérieux du dispositif qui devait le prévenir.

Le deuxième apport tient à la gradation posée par le principe 13. L'entreprise peut causer une atteinte, y contribuer, ou lui être seulement liée par une relation d'affaires[24]. Dans les deux premiers cas, il s'agit de cesser le comportement et de concourir à la réparation ; dans le

[19] Normes sur la responsabilité en matière de droits de l'homme des sociétés transnationales et autres entreprises, E/CN.4/Sub.2/2003/12/Rev.2, 26 août 2003. La Commission des droits de l'homme a estimé, par sa décision 2004/116 du 20 avril 2004, que ce texte n'avait pas de valeur juridique.
[20] RUGGIE (J.), Protéger, respecter et réparer : un cadre pour les entreprises et les droits de l'homme, rapport du Représentant spécial du Secrétaire général, A/HRC/8/5, 7 avril 2008.
[21] Conseil des droits de l'homme, résolution 17/4 du 16 juin 2011, adoptée sans vote.
[22] Principes directeurs, préc., principe 17 et son commentaire.
[23] 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, art. 17 ; art. L. 561-1 et s. du code monétaire et financier.
[24] Principes directeurs, préc., principe 13 et son commentaire.

troisième, ni indemnisation ni aveu de faute, mais l'usage de l'influence dont on dispose sur l'auteur. Cette gradation permettra de situer l'opérateur satellitaire, qui est rarement auteur, parfois contributeur, le plus souvent lié.

Il convient de relever deux mécanismes. Le principe 19 organise l'effet de levier : lorsque l'influence est insuffisante, l'entreprise doit chercher à l'accroître et, à défaut, envisager la fin de la relation en pesant les conséquences du retrait pour les personnes[25], et le principe 24 l'autorise à hiérarchiser ses actions selon la gravité des atteintes, appréciée par leur ampleur, leur portée et leur caractère irrémédiable[26]. Les Principes directeurs contiennent donc deux échelles, l'une mesurant l'implication de l'entreprise, l'autre la gravité de l'atteinte. Aucune ne mesure le contexte. C'est cette troisième échelle que le mémoire entend construire.

En ce qui concerne leur portée, les Principes directeurs ne sont pas un traité et ne créent aucune obligation internationale à la charge des entreprises. Il serait toutefois inexact d'y voir un catalogue de bonnes pratiques. Leur vocabulaire, leur séquence et leur gradation se retrouvent, presque littéralement, dans la loi de 2017 comme dans la directive de 2024. Le droit souple a ainsi préparé les catégories que le droit contraignant a ensuite reprises.

Une question demeure : pourquoi une entreprise privée devrait-elle se charger d'un objectif relevant, par nature, de la responsabilité des États ? Pour Marie-Anne Frison-Roche, le droit de la compliance ne se réduit pas aux procédés par lesquels les entreprises donnent à voir qu'elles respectent les réglementations applicables. Il se définit par les buts monumentaux qu'il poursuit. Ces buts, que seule l'autorité politique est légitime à édicter, excèdent ce que les États peuvent atteindre seuls. Leur charge est internalisée dans les entreprises aptes à les concrétiser, que l'auteur nomme les opérateurs cruciaux[27]. Ainsi, le Politique fixe le but tandis que l'entreprise apporte la puissance d'exécution qui lui fait défaut[28].

Cette approche permet de distinguer la diligence de la simple conformité : l'entreprise ne se limite pas au respect des règles qui lui sont applicables, mais mobilise les moyens dont elle dispose au service d'un objectif qui la dépasse. Encore faut-il que cet objectif soit compatible avec celui poursuivi par l'autorité publique.

[25] Ibid., principe 19 et son commentaire.
[26] Ibid., principe 24.
[27] FRISON-ROCHE (M.-A.), « Les Buts Monumentaux, cœur battant du Droit de la Compliance », in FRISON-ROCHE (M.-A.) (dir.), Les Buts Monumentaux de la Compliance, coll. « Régulations & Compliance », Journal of Regulation & Compliance (JoRC) et Dalloz, 2022, p. 21 à 44.
[28] FRISON-ROCHE (M.-A.), « La dynamique des Buts Monumentaux du Droit de la Compliance », in Les Buts Monumentaux de la Compliance, préc., p. 1 à 19. L'auteur y présente la compliance comme une alliance entre des volontés politiques aux grandes prétentions et les entités aptes à les concrétiser.

§ 2. La juridicisation française et son office judiciaire

La France est le premier État à avoir converti cette norme de conduite en obligation légale. La loi du 27 mars 2017, adoptée quatre ans après l'effondrement du Rana Plaza, impose aux sociétés employant au moins cinq mille salariés en France, ou dix mille dans le monde en incluant leurs filiales, d'établir et de mettre en œuvre un plan de vigilance[29]. Son champ est large : atteintes graves aux droits humains, à la santé et à la sécurité des personnes et à l'environnement, résultant des activités de la société, de celles qu'elle contrôle et de celles des sous-traitants et fournisseurs avec lesquels elle entretient une relation commerciale établie.

Son contenu reprend la séquence des Principes directeurs. On y retrouve la cartographie des risques, l'évaluation régulière des filiales, sous-traitants et fournisseurs, les actions d'atténuation, le mécanisme d'alerte élaboré avec les organisations syndicales et le dispositif de suivi qui en évalue l'efficacité[30]. La loi exige la mise en œuvre effective d'un dispositif, non l'absence d'atteinte. Classique en droit des obligations, la distinction devient décisive en conformité, puisqu'elle détermine ce que l'entreprise doit être en mesure de démontrer.

Le Conseil constitutionnel, saisi dès l'origine, a validé l'essentiel du dispositif mais censuré l'amende civile qui devait en sanctionner la méconnaissance, les termes définissant les obligations étant trop imprécis pour fonder une sanction ayant le caractère d'une punition[31]. L'indétermination du contenu de la vigilance a donc été relevée par le juge constitutionnel avant même la première application de la loi.

Le juge judiciaire a progressivement précisé le contenu de cette obligation, après l'attribution au tribunal judiciaire de Paris d'une compétence exclusive en la matière[32]. Le jugement du 5 décembre 2023 dans l'affaire La Poste, premier à statuer au fond, puis l'arrêt de la cour d'appel de Paris du 17 juin 2025, dessinent une méthode de contrôle plutôt qu'un contenu substantiel[33]. Le juge ne dit pas quels risques retenir ni quelles mesures prendre : il vérifie que la cartographie procède d'une démarche méthodique et traçable, que les risques sont hiérarchisés selon des critères explicites, que les mesures se rattachent aux risques recensés et que les parties prenantes ont été associées. Le contrôle porte sur la rigueur du processus, non sur l'opportunité des choix.

[29] Loi n° 2017-399 du 27 mars 2017, préc., codifiée aux art. L. 225-102-4 et L. 225-102-5 du code de commerce.
[30] Art. L. 225-102-4, I, alinéa 4, du code de commerce.
[31] Cons. const., décision n° 2017-750 DC du 23 mars 2017, cons. 13 et s. Le Conseil a censuré l'amende civile en relevant l'imprécision des termes employés pour définir les obligations sanctionnées, tout en jugeant conformes à la Constitution les autres dispositions de la loi.
[32] Art. L. 211-21 du code de l'organisation judiciaire, issu de l'article 56 de la loi n° 2021-1729 du 22 décembre 2021 pour la confiance dans l'institution judiciaire : compétence exclusive du tribunal judiciaire de Paris.
[33] TJ Paris, 5 décembre 2023, n° RG 21/15827, Fédération Sud PTT c/ La Poste ; CA Paris, pôle 5, ch. 12, 17 juin 2025, n° RG 24/05193, confirmant le jugement. La chambre 5-12, dite des contentieux émergents, a été créée pour connaître du devoir de vigilance et de la responsabilité écologique.

Le jugement rendu contre TotalEnergies le 25 juin 2026 confirme cette ligne et en montre la limite[34]. Le tribunal juge le plan incomplet et enjoint de le compléter, mais refuse de fixer la cible comme d'interdire des projets déterminés. Il contrôle la méthode et s'arrête au seuil de la décision d'entreprise. Cette réserve fournit le standard de preuve. Ce que l'opérateur devra établir, lorsqu'une décision de maintien ou de suspension sera contestée, n'est pas qu'il a pris la bonne décision, mais qu'il l'a prise selon un processus documenté, hiérarchisé et concerté.

§ 3. L'européanisation et son reflux

L'Union s'est engagée dans la même voie par deux instruments distincts. La directive du 14 décembre 2022 impose d'abord de rendre compte, selon des normes détaillées, des incidences de l'entreprise sur les personnes et l'environnement comme des risques que ces enjeux font peser sur elle[35]. Ensuite, la directive du 13 juin 2024 impose d'identifier, prévenir, atténuer et faire cesser les incidences négatives le long de la chaîne d'activités, sous le contrôle d'autorités nationales et sous menace de sanctions administratives[36]. Cette distinction, qui peut sembler théorique, est pourtant décisive pour les opérateurs satellitaires, puisqu'elle détermine l'existence même d'une obligation à leur charge.

Ce mouvement s'est interrompu avant d'avoir produit ses effets. Une première directive du 14 avril 2025 a reporté les échéances de transposition et d'application[37]. Puis la directive du 24 février 2026 a révisé le texte de 2024 dans un sens substantiellement plus étroit[38]. Les seuils ont été relevés, la vigilance recentrée sur les partenaires directs, la cartographie exhaustive remplacée par une approche fondée sur les risques, le plafond des sanctions ramené de cinq à trois pour cent du chiffre d'affaires mondial, le plan de transition climatique supprimé et le régime harmonisé de responsabilité civile abandonné au profit d'un renvoi aux droits nationaux.

Cette révision peut d'abord apparaître comme un recul. Elle introduit toutefois une évolution importante : en remplaçant la cartographie exhaustive par une approche fondée sur les risques, le législateur européen reconnaît que l'intensité de la vigilance doit varier selon la probabilité et la gravité des atteintes. L'allègement du dispositif s'accompagne ainsi d'une reconnaissance plus explicite de cette modulation. C'est sur ce fondement que sera construite l'échelle graduée proposée plus loin *(infra, § 15)*.

[34] TJ Paris, 25 juin 2026, n° RG 22/03403, préc.
[35] Directive (UE) 2022/2464 du Parlement européen et du Conseil du 14 décembre 2022 en ce qui concerne la publication d'informations en matière de durabilité par les entreprises ; règlement délégué (UE) 2023/2772 de la Commission du 31 juillet 2023 établissant les normes ESRS.
[36] Directive (UE) 2024/1760 du Parlement européen et du Conseil du 13 juin 2024 sur le devoir de vigilance des entreprises en matière de durabilité, art. 5 à 16.
[37] Directive (UE) 2025/794 du Parlement européen et du Conseil du 14 avril 2025, dite « stop the clock », reportant les échéances de transposition et d'application.
[38] Directive (UE) 2026/470, préc.

Section 2. L’angle mort des contextes à haut risque

§ 4. Un droit de l’amont appliqué à un risque de l’aval

Toute la difficulté tient à une question de direction, car le droit de la vigilance regarde vers l’amont. La loi de 2017 vise les activités de la société, celles des sociétés qu’elle contrôle et celles des sous-traitants et fournisseurs avec lesquels est entretenue une relation commerciale établie[39]. La directive de 2024 raisonne sur une chaîne d’activités qui couvre largement les partenaires en amont, mais ne retient en aval que la distribution, le transport et l’entreposage du produit[40]. L’usage que l’acheteur fait de ce qu’il a acquis n’entre pas dans le champ. Cette exclusion n’est pas un oubli, puisqu’elle exprime une conception cohérente, selon laquelle l’entreprise répond de ce qu’elle organise et non de ce qu’elle vend.

Appliquée à un opérateur satellitaire, cette architecture manque son objet. L’amont d’un tel opérateur ne présente pas de risque caractéristique pour les droits humains : ses fournisseurs sont des constructeurs de satellites, des sociétés de lancement, des équipementiers de stations sol, dont les risques sont ceux de toute activité industrielle avancée. Le risque naît intégralement en aval. Il naît du client qui achète de la capacité, du distributeur qui la revend, de l’intermédiaire qui la met à disposition d’un tiers, et de l’utilisateur final dont l’opérateur, le plus souvent, ne connaît ni l’identité ni les intentions. Pour un opérateur satellitaire, le risque se déplace ainsi de la chaîne d’approvisionnement vers ce que l’on pourrait appeler la chaîne d’usage, dont les maillons sont représentés en annexe (cf. annexe n° 5 p. 64). On propose de nommer ce déplacement, car il commande tout le reste de l’analyse : là où le droit organise une *supply chain due diligence*, l’opérateur d’infrastructure appelle une *use chain due diligence*.

L’objection est immédiate, et TotalEnergies l’a opposée au tribunal judiciaire de Paris avant de la reprendre à l’appui de son appel. La société soutient que soumettre une entreprise au contrôle des risques résultant de l’utilisation de ses produits par ses clients excède les objectifs de la loi, et relève que la directive n’a pas retenu les activités des clients dans son champ[41]. Le tribunal a écarté l’argument, qui n’en est pas moins sérieux : étendre la vigilance à l’aval revient à faire répondre une entreprise de comportements qu’elle n’a ni organisés ni rémunérés, et dont elle n’a souvent aucune connaissance. Poussée à son terme, cette extension ferait de tout fournisseur le garant des usages de son produit, ce que le présent mémoire se refuse à soutenir.

Il existe pourtant une réponse, et elle vient non du droit de la vigilance mais de la conformité. Le contrôle des exportations est tout entier un droit de l’usage final : le régime des

[39] Art. L. 225-102-4, I, du code de commerce, préc. Sur la notion de relation commerciale établie, voir la jurisprudence rendue en matière de rupture brutale, art. L. 442-1, II, du code de commerce.
[40] Directive (UE) 2024/1760, préc., art. 3, § 1, point g), définissant la chaîne d’activités.
[41] TOTALENERGIES SE, communiqué du 27 juillet 2026 ; moyen écarté par TJ Paris, 25 juin 2026, préc.

biens à double usage n'interroge pas la manière dont le bien a été produit mais celle dont il sera employé, et il impose à l'exportateur une diligence lorsque des éléments portés à sa connaissance laissent craindre une utilisation contraire aux droits humains[42]. Le régime des sanctions fonctionne de même, en obligeant à vérifier le destinataire et non le fournisseur. Le praticien vit donc avec deux logiques opposées : une vigilance qui regarde en arrière, un contrôle des exportations qui regarde en avant. Le droit sait construire une obligation tournée vers l'aval, mais il ne l'a pas fait pour les droits humains. C'est cette dissymétrie, plus encore que l'exclusion par les seuils, qui explique que l'opérateur satellitaire échappe au dispositif.

Si le droit de la compliance se définit par les buts qu'il poursuit et non par la position occupée par l'entreprise dans une chaîne économique, alors l'opposition entre l'amont et l'aval perd son caractère décisif : ce qui commande l'étendue de l'obligation n'est pas le sens du flux contractuel, mais l'aptitude de l'opérateur à peser sur la réalisation du but[43]. Un opérateur satellitaire n'est pas moins crucial parce que le risque se situe chez son client plutôt que chez son fournisseur ; il l'est davantage, la capacité fournie étant l'instrument même de l'atteinte redoutée.

Cependant, le législateur français comme le législateur européen ont raisonné en termes de chaîne, et le juge n'a pas consacré cette définition. Adopter celle-ci comme prémisse reviendrait à substituer à la lettre des textes une construction doctrinale, ce qu'un travail cherchant à établir une obligation opposable ne peut se permettre. La voie suivie ici sera donc plus étroite : non pas écarter la distinction de l'amont et de l'aval, mais montrer que le service satellitaire ne s'y laisse pas ranger, et que cette impossibilité de classement est elle-même l'indice d'une lacune du droit positif.

§ 5. La catégorie existante : les zones de conflit ou à haut risque

Le droit de l'Union n'ignore pas que le contexte géographique peut suffire à déclencher une obligation de diligence. Il l'a admis dès 2017, dans un texte que la doctrine du devoir de vigilance mobilise rarement : le règlement fixant des obligations de diligence à l'égard de la chaîne d'approvisionnement pour les importateurs d'étain, de tantale, de tungstène et d'or[44]. Son architecture constituera le modèle de la proposition défendue au terme de ce mémoire.

---

[42] Règlement (UE) 2021/821 du Parlement européen et du Conseil du 20 mai 2021 instituant un régime de l'Union de contrôle des exportations, du courtage, de l'assistance technique, du transit et des transferts en ce qui concerne les biens à double usage, art. 4 et 5.

[43] FRISON-ROCHE (M.-A.) (dir.), Régulation, supervision, compliance, Dalloz, 2017 ; FRISON-ROCHE (M.-A.) (dir.), Les outils de la Compliance, coll. « Régulations & Compliance », Journal of Regulation & Compliance (JoRC) et Dalloz, 2021, 323 p., spéc. l'approche juridique des outils de la compliance construite à partir de la définition par les buts monumentaux.

[44] Règlement (UE) 2017/821, préc., art. 1er et annexe I. Le règlement ne s'applique qu'au-delà de seuils de volume annuel d'importation, définis par métal.

Son fait générateur n'est ni la taille de l'entreprise ni la nature de son activité, mais la provenance du minerai. L'obligation se déclenche lorsque celui-ci est extrait d'une zone de conflit ou à haut risque, que l'article 2 définit comme une zone en situation de conflit armé ou fragile à l'issue d'un conflit, ainsi qu'une zone caractérisée par une gouvernance et une sécurité déficientes, voire inexistantes, tel un État défaillant, et par des violations courantes et systématiques du droit international[45]. Le contenu de l'obligation reprend la suite habituelle : système de gestion, identification et gestion des risques, vérification par un tiers indépendant, communication publique[46].

Le règlement comporte en outre un dispositif décisif : une obligation déclenchée par le contexte supposant que l'on sache le reconnaître, la Commission est chargée d'établir, avec des experts externes, une liste indicative, non exhaustive et régulièrement mise à jour de ces zones[47]. Le législateur n'a donc pas laissé chaque importateur qualifier seul la situation d'un territoire, puisqu'il a admis qu'une telle qualification excède les moyens d'une entreprise, tout en lui refusant un caractère contraignant qui aurait figé l'appréciation et emporté des conséquences diplomatiques.

Quatre enseignements se dégagent, tous mobilisés par la suite. D'abord, une obligation de diligence peut être déclenchée par le contexte plutôt que par la taille de l'entreprise. Ensuite, elle peut viser un secteur déterminé sans être discriminatoire, dès lors que ce secteur présente un risque caractérisé. Sa vérification peut être confiée à un auditeur indépendant plutôt qu'à une administration. Enfin, une qualification officielle du contexte peut lui servir de point de départ sans lier l'entreprise. Ce modèle fonctionne depuis 2021 et rien, dans sa logique, ne le réserve aux minerais.

§ 6. L'inadaptation de cette catégorie aux services de communication

C'est ici que le modèle révèle ses limites. La définition retenue en 2017 vise avant tout les situations caractérisées par une gouvernance et une sécurité déficientes, voire inexistantes, autrement dit celles d'un État défaillant. La catégorie européenne ne connaît qu'une forme de danger, celle qui procède de l'effacement de l'autorité publique. Elle a été écrite pour des territoires où nul ne contrôle l'accès à la mine et où la traçabilité du minerai se perd faute d'administration capable de la garantir. Le risque y tient à l'absence d'interlocuteur.

[45] Ibid., art. 2, point f).
[46] OCDE, Guide OCDE sur le devoir de diligence pour des chaînes d'approvisionnement responsables en minerais provenant de zones de conflit ou à haut risque, 3e éd., Éditions OCDE, Paris, 2016.
[47] Règlement (UE) 2017/821, préc., art. 14, § 2. La Commission recourt à des experts externes pour établir une liste indicative, non exhaustive et régulièrement mise à jour des zones de conflit ou à haut risque.

Or le secteur des communications connaît un second risque, de nature inverse et probablement plus fréquent. Le rapport du Haut-Commissariat aux droits de l'homme consacré aux coupures d'accès le documente : ces interruptions ne sont pas le fait d'États effondrés, mais d'autorités disposant du plein contrôle de leur infrastructure, qui les ordonnent au moment d'une élection, d'une contestation ou d'un examen national[48]. L'appareil administratif fonctionne, la chaîne de commandement est identifiée, la demande est régulière au regard du droit interne. Dans cette seconde configuration, le risque procède précisément de la capacité de l'État à exercer effectivement son contrôle sur les communications.

Le risque naît autant de la défaillance de l'État que de sa maîtrise. Et ces deux risques n'appellent pas la même diligence. Face à un État défaillant, l'opérateur affronte un problème de connaissance : qui utilise réellement la capacité vendue, derrière quel intermédiaire, à quelle fin ? Face à un État en pleine possession de ses moyens, il affronte un problème d'arbitrage. La demande émane d'une autorité légitime, elle est formellement régulière, et c'est son objet qui porte atteinte aux droits. La première situation appelle principalement un effort de connaissance, tandis que la seconde impose un arbitrage, que nul texte n'autorise expressément l'entreprise à rendre.

Cette asymétrie tient à la nature des objets régis. Un minerai est extrait d'un territoire, il en sort et circule hors de l'atteinte de celui qui le gouverne. Une capacité de communication est au contraire délivrée au-dessus d'un territoire et s'adresse à ceux qui y vivent. Elle demeure, pendant toute la durée du service, à portée de l'autorité qui y exerce le pouvoir. L'opérateur n'a pas seulement des clients dans un pays ; il a un interlocuteur souverain qui peut, à tout moment, lui demander d'agir. La catégorie de 2017 ne voit pas cette configuration, parce que le minerai ne la présente jamais.

La soft law onusienne permet-elle de combler cette lacune ? Le guide du Programme des Nations unies pour le développement retient une conception large des contextes affectés par un conflit, qui ne se limite pas aux seuls conflits armés au sens du droit international humanitaire[49]. Son périmètre reste toutefois arrimé à la violence, armée ou généralisée : le contrôle des canaux de communication et la fermeture d'internet n'y figurent qu'au nombre des signaux précurseurs, non comme une catégorie autonome. La lacune est donc générale et l'adaptation proposée inédite. Aucun instrument contraignant ne qualifie aujourd'hui, comme contexte appelant une diligence renforcée, la situation d'un État solide qui use de son autorité sur les communications

[48] HCDH, A/HRC/50/55, préc.
[49] PNUD, Heightened Human Rights Due Diligence for Business in Conflict-Affected Contexts, préc.

contre sa propre population. C'est pour combler cet écart qu'une échelle à quatre degrés sera proposée, distinguant le haut risque par défaillance du haut risque par maîtrise *(infra, § 14)*.

§ 7. Le comblement par la soft law et ses limites

Face à ce silence, une production normative abondante s'est développée aux Nations unies. Le Groupe de travail sur les entreprises et les droits de l'homme a consacré en 2020 un rapport aux régions touchées par un conflit, formulant l'exigence d'une diligence renforcée[50]. Le Programme des Nations unies pour le développement en a tiré en 2022 un guide opérationnel articulant deux analyses distinctes : les risques que l'activité fait peser sur les personnes et ses effets sur la dynamique du conflit[51]. Le projet B-Tech du Haut-Commissariat transpose par ailleurs les Principes directeurs aux technologies numériques[52], tandis que le rapport de 2022 sur les coupures d'accès fournit le raisonnement de proportionnalité applicable aux interruptions de service[53].

Ces instruments, dépourvus de force obligatoire, n'ont-ils qu'un intérêt documentaire ? Les recommandations de l'Agence française anticorruption ne créent aucune obligation, et nul ne songerait pourtant à construire un programme sans s'y conformer, parce qu'elles constituent le référentiel du contrôle[54]. Le droit souple onusien remplit ici deux fonctions comparables, puisqu'il fournit un standard.

Lorsque la loi de 2017 exige des actions adaptées d'atténuation sans en préciser le contenu, le juge se réfère à ce qu'une entreprise diligente était censée savoir et faire, état de l'art que ces guides décrivent. Il sert aussi de référentiel dans l'appréciation de la faute, une entreprise opérant dans un contexte de conflit documenté sans avoir mis en œuvre aucune mesure recommandée s'exposant à voir son comportement qualifié de fautif au sens du droit commun.

Section 3. La démonstration empirique du vide

§ 8. L'exclusion par les seuils : l'application chiffrée

Il ne s'agit pas ici de soutenir que le droit de la vigilance s'applique mal aux opérateurs satellitaires, mais qu'il ne s'applique pas. Il suffit de confronter les seuils des deux textes contraignants aux données que ces entreprises publient.

---

[50] Groupe de travail des Nations unies, A/75/212, préc.
[51] PNUD, Heightened Human Rights Due Diligence for Business in Conflict-Affected Contexts, préc.
[52] HCDH, projet B-Tech, Applying the UN Guiding Principles on Business and Human Rights to Digital Technologies, notes de cadrage, 2020 et s.
[53] HCDH, A/HRC/50/55, préc.
[54] Agence française anticorruption, recommandations destinées à aider les personnes morales de droit public et de droit privé à prévenir et à détecter les faits de corruption, JORF du 12 janvier 2021. Ces recommandations sont dépourvues de force obligatoire mais constituent le référentiel des contrôles.

La loi de 2017 retient un critère unique, celui de l'effectif, fixé à cinq mille salariés en France ou dix mille dans le monde, filiales incluses. La directive de 2024, révisée en février 2026, en retient deux, cumulatifs : cinq mille salariés et un milliard cinq cents millions d'euros de chiffre d'affaires net mondial[55]. Le tableau ci-dessous rapproche ces seuils des données publiées par les quatre opérateurs de référence.

Opérateur	Effectif	Chiffre d'affaires net	Seuil loi 2017	Seuil CS3D révisée	Seuil CSRD révisée
Eutelsat	612 en France 1 639 dans le monde	1 235,9 M€ (exercice 2025-2026)	Non atteint	Non atteint (aucun des deux critères)	Atteint (les deux critères)
SES	3 845	2 627 M€ (exercice 2025)	Hors champ (siège au Luxembourg)	Non atteint : chiffre d'affaires atteint, effectif inférieur à 5 000	Atteint (les deux critères)
Hispasat	≈ 550	212,1 M€ (exercice 2025)	Hors champ (siège en Espagne)	Non atteint en propre*	Non atteint en propre*
Viasat	≈ 7 000	4,64 Md$ (exercice 2025-2026)	Hors champ (siège aux États-Unis)	Non atteint (chiffre d'affaires réalisé dans l'Union)	Sans objet

** Hispasat n'atteint pas individuellement les seuils de la directive sur le devoir de vigilance ni ceux de la directive sur la publication d'informations en matière de durabilité, telles que révisées. Depuis son intégration au groupe Indra à la fin de l'année 2025, son activité est toutefois susceptible d'être appréhendée au niveau consolidé de ce groupe, lequel dépasse les seuils applicables.*

Eutelsat Communications[56], seul opérateur du panel dont le siège est en France, employait 612 salariés en France et 1 639 dans le monde au 30 juin 2025, pour un chiffre d'affaires de 1 235,9 millions d'euros au titre de l'exercice clos le 30 juin 2026, tout en exploitant trente et un satellites géostationnaires et une constellation de plus de six cents satellites en orbite basse[57]. L'effectif atteint douze pour cent du premier palier de la loi de 2017 et seize pour cent du second, et aucun des deux critères cumulatifs de la directive révisée n'est atteint : ni les cinq mille salariés, ni le milliard cinq cents millions d'euros. L'exclusion ne tient donc pas à un seul critère que la croissance pourrait faire franchir ; elle est doublement acquise.

[55] Loi n° 2017-399, préc., art. 1er ; directive (UE) 2024/1760, préc., art. 2, tel que modifié par la directive (UE) 2026/470.

[56] Eutelsat Communications S.A. est la dénomination sociale de la société cotée, sous laquelle les comptes consolidés sont arrêtés et le document d'enregistrement universel déposé auprès de l'Autorité des marchés financiers. Eutelsat Group est le nom sous lequel le groupe se présente depuis le rapprochement avec OneWeb intervenu en 2023, et celui qui figure dans la note de méthode liminaire. Les seuils d'assujettissement s'appréciant au niveau de la société mère consolidante, c'est la dénomination sociale qui est retenue dans les développements chiffrés.

[57] Effectifs et chiffres d'affaires publiés par les opérateurs. Eutelsat : Document d'enregistrement universel 2024-25, préc., effectifs au 30 juin 2025, section 3.3.1.4, p. 159, et communiqué de résultats annuels du 7 août 2026 pour l'exercice clos le 30 juin 2026 ; la flotte comprend trente et un satellites géostationnaires et plus de six cents satellites en orbite basse. SES : Annual Report 2025, l'acquisition d'Intelsat ayant été achevée le 17 juillet 2025 et portant la flotte à environ cent vingt satellites. Hispasat : Informe Anual 2025, l'opérateur ayant été intégré au groupe Indra à la fin de l'année 2025. Viasat : Annual Report on Form 10-K pour l'exercice clos le 31 mars 2026, déposé le 29 mai 2026.

Les trois autres opérateurs échappent aux mêmes textes, mais par des voies distinctes. SES et Hispasat, établies au Luxembourg et en Espagne, sont hors du champ de la loi française, qui ne vise que les sociétés dont le siège se trouve en France ; Viasat, société américaine, y échappe pour la même raison, bien qu'elle dépasse largement les seuils en valeur absolue. Si la directive révisée saisit les entreprises de pays tiers, c'est en effet à raison du chiffre d'affaires qu'elles réalisent dans l'Union, que cet opérateur n'atteint pas.

Avec ces mêmes chiffres, l'opérateur français franchit sans difficulté les seuils de la directive sur la publication d'informations en matière de durabilité, portés en février 2026 à mille salariés et quatre cent cinquante millions d'euros. Sur la base de ces mêmes données, la même entreprise est donc tenue de rendre compte de ses incidences sur les droits humains sans être tenue d'aucun comportement à leur égard. L'opérateur français n'est donc ni partiellement soumis ni soumis à un régime allégé : il demeure hors du champ des deux textes qui imposent une conduite, tout en restant soumis aux obligations de publication en matière de durabilité.

Le cas de SES permet d'isoler clairement ce mécanisme. Depuis l'acquisition d'Intelsat, finalisée le 17 juillet 2025, l'opérateur exploite environ cent vingt satellites et réalise un chiffre d'affaires de 2 627 millions d'euros, largement supérieur au seuil européen. Il demeure pourtant hors du champ de la directive, son effectif de 3 845 salariés restant inférieur au seuil de cinq mille. Ainsi, une entreprise peut accroître fortement sa taille économique et son empreinte orbitale sans pour autant franchir un seuil fondé sur le nombre de salariés. Hispasat illustre une autre limite : l'opérateur n'atteint aucun seuil pris isolément, mais son intégration au groupe Indra à la fin de l'année 2025 peut conduire à apprécier sa situation au niveau consolidé, les directives tenant également compte de l'entreprise mère ultime. L'exclusion apparaît dès lors structurelle : elle concerne précisément les activités pour lesquelles le rapport entre les effectifs et la portée du service est le plus déséquilibré, comme c'est le cas des infrastructures critiques. À titre d'exemple, 612 salariés en France peuvent exploiter une flotte couvrant plusieurs dizaines de pays, tandis qu'une entreprise employant plus de cinq mille salariés peut être assujettie indépendamment de la portée de son activité. Il ne s'agit pas de remettre en cause la logique de la loi, conçue pour un autre objet, mais de constater qu'un critère pertinent dans un secteur ne l'est pas nécessairement dans un autre. En l'état du droit, la vigilance de ces opérateurs repose donc largement sur leurs propres dispositifs.

§ 9. Le reliquat : rendre compte sans avoir à se comporter

Une obligation subsiste néanmoins. La directive relative à la publication d'informations en matière de durabilité, dont les seuils ont aussi été relevés en 2026 mais restent nettement

inférieurs à ceux de la vigilance, maintient les principaux opérateurs européens dans son champ[58]. Ils publient donc un rapport de durabilité établi selon les normes européennes, parmi lesquelles deux normes thématiques viseraient exactement les personnes affectées par une interruption de service : celle des communautés affectées et celle des consommateurs et utilisateurs finals[59].

Encore faut-il observer ce que ce reporting contient. L'opérateur français rend compte de la validation de ses objectifs climatiques par la Science Based Targets initiative, d'une réduction de 64 % de ses émissions depuis 2021 et du raccordement de plus d'un million huit cent mille utilisateurs en Afrique[60]. La démonstration se trouve toutefois ailleurs, dans l'analyse de double matérialité elle-même. Les deux normes qui viseraient les personnes affectées y sont déclarées non matérielles, dans l'intégralité de leurs points de données. L'entreprise ajoute que les communautés affectées n'ont pas été consultées, et que le processus ne s'est concentré ni sur des activités ni sur des zones géographiques particulières, une approche générale ayant été appliquée à toutes les opérations[61].

Le reporting n'est pas silencieux sur les droits humains : engagement, déclaration relative à l'esclavage moderne, code fournisseurs, dispositif d'alerte. Mais ces développements visent les salariés et la chaîne d'approvisionnement, c'est-à-dire l'amont, et la consultation menée en matière de droits humains est celle des collaborateurs. Les seules occurrences d'interruption de service figurent au chapitre des risques opérationnels, où elles désignent des pannes d'équipement et des microcoupures en orbite. La matière qui ferait l'objet d'une diligence si elle était exigée demeure hors du récit, non par dissimulation, mais parce qu'aucune norme ne conduit à l'y faire entrer.

Ce reliquat n'est pas sans effet, et deux conséquences seront réutilisées en seconde partie. Pour publier, il faut recenser, mesurer et conserver, de sorte que le reporting engendre une matière probatoire. Une déclaration inexacte expose son auteur, sur le terrain des pratiques commerciales trompeuses comme du droit commun.

---

[58] Directive (UE) 2022/2464, préc., telle que modifiée par la directive (UE) 2026/470.

[59] Règlement délégué (UE) 2023/2772, préc., normes ESRS S3 (communautés affectées) et S4 (consommateurs et utilisateurs finals).

[60] EUTELSAT COMMUNICATIONS, communiqué de résultats annuels de l'exercice 2025-26, 7 août 2026, rubrique « Responsabilité sociale de l'entreprise ». Les indicateurs mis en avant portent sur la trajectoire climatique validée par la Science Based Targets initiative, la réduction des émissions de scopes 1 et 2, l'inclusion numérique et la mise en conformité de la gouvernance avec la directive (UE) 2022/2464.

[61] EUTELSAT COMMUNICATIONS, Document d'enregistrement universel 2024-25, préc., état de durabilité : tableau de correspondance des points de données, où l'ensemble des exigences relevant des normes ESRS S3 et S4 est porté en « non matériel » ; section relative au processus de double matérialité, dont il ressort que les communautés affectées n'ont pas été directement consultées et que le processus ne s'est pas concentré sur les activités, relations commerciales ou secteurs géographiques associés à un risque accru d'incidences négatives.

§ 10. La carence institutionnelle : l'enseignement de l'affaire Arcom

Un vide normatif pourrait être compensé par une autorité disposant d'un pouvoir d'injonction. L'épisode de l'automne 2022 permet de vérifier cette hypothèse en conditions réelles, et son enseignement est plus troublant que le simple constat d'une absence de régulateur.

Les faits ont été rappelés en introduction. L'Autorité de régulation de la communication audiovisuelle et numérique s'est d'abord déclarée incompétente, avant que le juge des référés du Conseil d'État ne suspende cette décision et qu'elle ne mette l'opérateur en demeure[62]. Le fondement de cette compétence retrouvée relevait du droit de l'audiovisuel : c'est en qualité de distributeur de services de télévision, et non en qualité d'opérateur de communications électroniques, que l'entreprise a été atteinte. L'opérateur n'est pas éditeur de programmes. La loi de 1986 ne lui impose que d'identifier les éditeurs auprès du régulateur et de les informer du régime applicable. Cette qualification n'était mobilisable que parce qu'un instrument conventionnel, la Convention européenne sur la télévision transfrontière, liait l'État de destination des programmes[63].

Trois conséquences en découlent. La compétence exercée était accidentelle. Elle tenait à la nature du contenu diffusé et à un hasard conventionnel, non à la qualité de l'opérateur ni à la gravité de la situation. Elle n'est pas transposable, au sens où un opérateur satellitaire fournit surtout de la capacité de transmission de données, et si la question s'était posée à propos d'un faisceau loué à un client institutionnel, aucun régulateur n'aurait eu de titre à intervenir. Le volet iranien de la décision, enfin, ne reposait pas sur le même fondement : deux degrés de contexte, deux régimes distincts.

Le paysage institutionnel confirme ce diagnostic dans la mesure où l'autorité de régulation des communications électroniques exerce une compétence économique et technique, dépourvue de tout volet relatif aux droits humains. Celle qui délivre les autorisations d'opérations spatiales contrôle la sécurité des opérations et les intérêts de la défense. L'Autorité des marchés financiers, elle, ne connaît que de l'information publiée. Restent les autorités instituées par la directive de 2024, qui ne connaîtront que des entreprises entrant dans son champ, dont ces opérateurs sont précisément exclus. Aucune n'a mandat pour apprécier la diligence d'un opérateur d'infrastructure en contexte de conflit.

---

[62] CE, ord. réf., 9 décembre 2022, préc. ; Arcom, mise en demeure du 14 décembre 2022, préc.

[63] Convention européenne sur la télévision transfrontière, Strasbourg, 5 mai 1989. Sur les obligations propres à l'opérateur satellitaire, loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication, art. 19 et 33-1-III : l'opérateur, qui n'est pas fournisseur de programmes, est tenu de communiquer au régulateur les informations permettant d'identifier les éditeurs des chaînes diffusées et d'informer ceux-ci du régime qui leur est applicable.

La lacune est donc à la fois normative, aucun texte n'imposant ce comportement, et institutionnelle, aucune autorité n'étant clairement compétente pour en contrôler la mise en œuvre. Cette seconde dimension est la plus souvent négligée, alors qu'elle conditionne l'effectivité de toute règle que l'on voudrait créer. Une obligation sans autorité n'est qu'une déclaration d'intention, ce à quoi il faudra répondre en désignant un point de contact et une autorité chargée du suivi *(infra, § 38)*.

Chapitre 2. Les fondements d'une diligence renforcée et graduée

Section 1. Le fondement tiré de la nature du service

§ 11. La dualité structurelle de la capacité

Le premier fondement d'une exigence renforcée tient à ce que l'opérateur satellitaire vend. Dans le régime des exportations, un bien à double usage est un bien identifiable. Il figure sur une liste, il possède des caractéristiques techniques déterminées, et c'est cette identification préalable qui déclenche le contrôle[64]. La dualité est une propriété du produit, constatable avant toute transaction.

La capacité de communication n'obéit pas à cette logique. Aucune caractéristique technique ne distingue un usage civil d'un usage militaire. C'est le même signal, la même fréquence, le même faisceau, et une liaison peut acheminer dans la même seconde la coordination d'une équipe médicale et celle d'une unité engagée. La dualité ne constitue pas un usage détourné du produit : elle en est la définition.

Cette caractéristique distingue le secteur satellitaire de celui auquel on le compare le plus souvent, les technologies de surveillance. Un logiciel d'interception est conçu pour intercepter. Sa fonction est sa finalité, et le fournisseur qui le vend à un appareil répressif ne peut prétendre ignorer ce à quoi il servira. C'est ce qui rend l'affaire Amesys juridiquement lisible. Rien de tel pour une capacité satellitaire, qui n'est conçue pour rien en particulier. Cette différence protège l'opérateur d'une imputation trop facile. Elle lui interdit aussi de se retrancher derrière la neutralité de son produit, puisque cette neutralité est ce qui rend l'usage imprévisible.

En conséquence, une diligence fondée sur le produit est ici impraticable, faute de filtrage technique, de liste de biens sensibles ou de caractéristique déclenchant un contrôle. Si la vigilance ne peut porter sur ce qui est vendu, elle ne peut porter que sur celui à qui l'on vend et sur l'environnement de délivrance. Le client et le contexte deviennent les seules variables observables. Ce déplacement justifie de construire l'exigence sur une échelle de contextes

[64] Règlement (UE) 2021/821, préc., art. 2 et annexe I.

plutôt que sur une nomenclature de produits, et impose de passer de la connaissance du client à celle de l'usage *(infra, § 22)*.

§ 12. La criticité : la privation comme atteinte

Le deuxième fondement tient à ce qu'emporte l'absence du service. Dans le modèle ordinaire de la vigilance, l'atteinte résulte de ce que l'entreprise fait ou permet : cesser l'activité met fin au risque. La relation d'affaires interrompue est le remède, et le désengagement constitue l'issue prudente. Cette structure ne se retrouve pas ici.

Le Haut-Commissariat aux droits de l'homme a établi que les interruptions d'accès aux communications affectent un ensemble de droits bien plus large que la seule liberté d'expression[65]. Sont en cause l'accès à l'information et la liberté de réunion, mais aussi le droit à la santé lorsque les services de secours deviennent injoignables, le droit à l'éducation et au travail lorsque l'activité s'est dématérialisée, la protection des données lorsque les usagers se replient sur des canaux non sécurisés, et le droit à un recours effectif lorsque la documentation des violations devient impossible. En période de conflit, cette liste s'étend à ce qui conditionne la survie : l'alerte des populations, la coordination des acteurs humanitaires, la localisation des blessés, la preuve des atteintes.

La nature du dommage varie donc avec le degré du contexte, ce qui justifie l'échelle proposée plus loin. Dans un environnement à haut risque sans conflit ouvert, la privation atteint le débat public, le travail journalistique et la capacité de contestation, dont elle fait un instrument d'isolement politique. En situation de conflit armé, elle atteint en outre l'intégrité physique des personnes. Une méthode qui appliquerait la même grille aux deux situations serait fausse dans les deux cas.

La conséquence essentielle est qu'il n'existe pas d'option neutre. Maintenir le service, c'est accepter qu'il puisse servir à des fins attentatoires ; le suspendre, c'est priver des civils d'un accès dont dépendent leurs droits et parfois leur sécurité. Le remède ordinaire de la vigilance, la sortie de relation, devient ici un facteur de risque. Cette configuration est rare en conformité, où l'abstention est presque toujours la position sûre. Elle explique que la diligence attendue de ces opérateurs ne puisse se résumer à une politique de refus et doive être conçue comme une méthode d'arbitrage documenté plutôt que comme un dispositif d'exclusion.

§ 13. L'irréversibilité et la temporalité de la décision

Le troisième fondement tient au temps. La désactivation d'un terminal ou l'extinction d'un faisceau sont instantanées, sans préavis technique, sans déplacement, sans intervention

[65] HCDH, A/HRC/50/55, préc.

matérielle. Cet avantage opérationnel est, du point de vue de la diligence, une difficulté majeure. La décision peut être exécutée avant qu'aucune évaluation n'ait été conduite, et une injonction reçue le soir peut l'être dans l'heure.

Elle signifie aussi que la réversibilité est trompeuse. Techniquement, un service interrompu peut être rétabli ; humainement, ce qui s'est produit pendant l'interruption ne l'est pas. L'appel de secours qui n'a pas abouti, le convoi humanitaire qui n'a pas été redirigé, le témoignage qui n'a pas été transmis ne se rattrapent pas au rétablissement du signal. Or le caractère non remédiable de l'atteinte figure, tant dans les Principes directeurs que dans le droit de l'Union, parmi les critères déterminant sa gravité, et par conséquent l'intensité de la vigilance due[66].

Il faut donc distinguer deux temps de la diligence. Celui de la préparation d'abord : cartographier, qualifier les contextes, définir les seuils d'escalade, désigner les décideurs, rédiger les clauses, entraîner les équipes, au rythme ordinaire de la conformité (cf. annexe n° 6 p. 65). Celui de l'exécution ensuite, en temps réel, qui ne permet aucune élaboration nouvelle. Une diligence renforcée n'est donc pas une diligence plus fréquente, mais une diligence dont l'essentiel a été accompli avant que la question ne se pose. L'enjeu est donc moins la rapidité de l'analyse au moment de la crise que la préparation du processus de décision en amont.

Section 2. Le fondement tiré du contexte : construction d'une échelle

§ 14. Proposition d'une échelle graduée de vigilance

Les développements précédents montrent que la vigilance ordinaire est insuffisante, sans pour autant définir le niveau de vigilance à lui substituer. Une exigence renforcée uniforme serait toutefois difficilement applicable : étendue à l'ensemble du portefeuille de l'opérateur, elle serait disproportionnée ; limitée aux seules situations extrêmes, elle laisserait de côté une grande partie des situations à risque. D'où la proposition de raisonner par degrés, au moyen d'une échelle modulant l'intensité et surtout la nature de la diligence selon le contexte de délivrance.

Degré 0 : le contexte ordinaire. La vigilance de droit commun s'applique : identification du cocontractant, vérification des listes de sanctions, clauses d'usage acceptable, revue périodique du portefeuille. Rien n'y est propre au secteur, et l'essentiel des relations d'affaires relève de ce degré.

Degré 1 : le haut risque par défaillance. Le contexte se caractérise par une gouvernance ou une sécurité déficientes, la présence d'acteurs armés non étatiques ou une chaîne de distribution que l'opérateur ne parvient pas à reconstituer. Le risque dominant y est un risque de

[66] Principes directeurs, préc., principe 14 et commentaire du principe 24 ; directive (UE) 2024/1760, préc., critères de gravité.

méconnaissance, l'opérateur ignorant qui utilise réellement la capacité vendue. La diligence porte donc sur l'identification de l'utilisateur réel.

Degré 2 : le haut risque par maîtrise. Le contexte se caractérise à l'inverse par un appareil d'État pleinement fonctionnel exerçant un contrôle documenté sur l'accès à l'information : restrictions récurrentes, exigences de surveillance, demandes d'interruption. Le problème n'est plus de connaître mais d'arbitrer. La diligence porte alors sur la légitimité de la demande et sur la traçabilité de la réponse.

Degré 3 : le conflit armé. Le contexte relève des seuils du droit international humanitaire. Il cumule les deux risques précédents et y ajoute une dimension propre : la capacité fournie peut contribuer à la conduite des hostilités, et l'infrastructure elle-même se trouver exposée. La diligence intègre alors la qualification humanitaire et l'appréciation des effets sur les usagers civils partageant la ressource.

Les degrés 1 et 2 ne diffèrent pas seulement par leur intensité : ils correspondent à des risques de nature différente et appellent donc des réponses distinctes. Au degré 1, la difficulté tient principalement à l'identification de l'utilisateur réel et suppose un travail d'investigation. Au degré 2, les faits sont connus ; la difficulté réside dans l'arbitrage à opérer face à une demande émanant d'un État. Or aucun instrument existant ne distingue clairement ces deux situations : le règlement de 2017 appréhende essentiellement la défaillance de l'État[67], tandis que les instruments onusiens raisonnent à partir des contextes de conflit. L'échelle proposée vise précisément à combler cet écart, plutôt qu'à transposer simplement un cadre existant.

Il convient alors de situer cette proposition par rapport à un mouvement doctrinal récent. Les travaux réunis sous la direction de Marie-Anne Frison-Roche mesurent l'intensité variable de l'obligation de vigilance secteur par secteur : opérateurs financiers, établissements bancaires, opérateurs numériques, opérateurs énergétiques[68]. L'idée que la vigilance ne présente pas partout la même intensité est donc acquise, et l'auteur voit dans cette obligation la pointe avancée de la compliance, celle par laquelle le dispositif progresse et se discute[69].

Ainsi, les opérateurs satellitaires sont absents de cette cartographie sectorielle, alors qu'ils cumulent les traits qui la justifient ailleurs : position d'infrastructure, capacité non substituable,

[67] Règlement (UE) 2017/821, préc., art. 2, point f).

[68] ROUAUD (A.-C.), « L'intensité de l'obligation de vigilance selon les secteurs : le cas des opérateurs financiers » ; FRANÇON (M.), « L'intensité du devoir de vigilance dans le secteur bancaire » ; LOISEAU (G.), « L'intensité de l'obligation de vigilance selon les secteurs : le cas des opérateurs numériques » ; LAMOUREUX (M.), « L'obligation de vigilance des opérateurs énergétiques », in FRISON-ROCHE (M.-A.) (dir.), L'Obligation de Compliance, coll. « Régulations & Compliance », Journal of Regulation & Compliance (JoRC) et Éditions Lefebvre-Dalloz, 2025, 816 p.

[69] FRISON-ROCHE (M.-A.), « La Vigilance, pointe avancée et part totale de l'Obligation de Compliance », in L'Obligation de Compliance, préc.

exposition directe aux demandes des États. La nature de la modulation retenue importe ensuite davantage. Cette doctrine module l'intensité selon le secteur d'activité, donnée stable, attachée à l'entreprise et connue d'avance ; l'échelle proposée ici module selon le contexte d'exploitation, donnée variable, attachée au territoire et susceptible de changer en quelques jours. Les deux modulations ne s'excluent pas, elles se composent : un même opérateur relève d'une intensité sectorielle à laquelle s'ajoute un coefficient contextuel. C'est cette seconde dimension, que la doctrine n'a pas construite, que le présent mémoire entend proposer. La matrice qui en résulte figure en annexe (cf. annexe n° 1 p. 60).

§ 15. La gravité comme facteur d'intensification et son fondement en droit positif

Une question demeure : la modulation de la vigilance selon le contexte conduit-elle à créer une catégorie que le droit positif ignore ? La réponse est négative, et quatre fondements convergents l'établissent.

Les Principes directeurs, d'abord, dont le principe 24 autorise l'entreprise à hiérarchiser son action selon la gravité des atteintes[70]. La priorisation par la gravité est admise dès l'origine ; or traiter d'abord le plus grave, c'est admettre que l'intensité de la diligence varie, ce qui est le principe même d'une échelle.

La loi française, ensuite, qui exige des actions adaptées d'atténuation des risques. L'adjectif n'est pas décoratif, puisqu'il impose un rapport entre la mesure et le risque, donc une variation de la première en fonction du second. Le juge, en contrôlant que les mesures annoncées se rattachent effectivement aux risques cartographiés, applique cette exigence de correspondance[71].

Le règlement sur les minerais module déjà, pour sa part, l'obligation en fonction du contexte géographique et démontre qu'un tel critère de déclenchement est opératoire en droit de l'Union[72].

Enfin, la directive de février 2026, dont on a dit qu'elle affaiblissait le dispositif, a substitué à la cartographie exhaustive une approche fondée sur les risques[73]. Elle a ainsi consacré en droit dur ce qui n'était qu'une pratique. L'entreprise n'est pas tenue de tout surveiller avec la même attention, mais de concentrer ses moyens là où la probabilité et la gravité des atteintes le justifient. L'échelle proposée ne contredit donc pas le droit positif européen, dont elle applique le principe directeur à un secteur qu'il n'avait pas envisagé. Cette même approche par les

[70] Principes directeurs, préc., principe 24.
[71] Art. L. 225-102-4, I, 3°, du code de commerce ; CA Paris, 17 juin 2025, préc.
[72] Règlement (UE) 2017/821, préc., art. 1er.
[73] Directive (UE) 2026/470, préc.

risques sera invoquée plus loin pour limiter l'exigence *(infra, § 29)* ; sa cohérence tient à ce qu'elle commande les deux mouvements.

§ 16. Le degré supérieur : l'articulation avec le droit international humanitaire

Le degré 3 de l'échelle fait entrer un corpus qui ne s'adresse pas à l'entreprise. Le droit international humanitaire lie les parties au conflit ; il n'impose pas d'obligations directes aux sociétés commerciales, sauf par le canal de la responsabilité pénale individuelle de leurs dirigeants. Il n'en constitue pas moins, pour l'opérateur, une grille d'analyse indispensable, à trois titres.

Il fournit d'abord le seuil de qualification : c'est par référence aux articles 2 et 3 communs aux Conventions de Genève que se détermine l'existence d'un conflit armé, et donc le passage du degré 2 au degré 3[74]. Elle n'est pas laissée à l'appréciation discrétionnaire de l'entreprise, mais s'appuie sur des critères objectifs et sur les constatations d'organisations spécialisées.

Vient ensuite le statut de la ressource. Constitue un objectif militaire le bien qui, par sa nature, son emplacement, sa destination ou son utilisation, apporte une contribution effective à l'action militaire et dont la destruction offre un avantage militaire précis[75]. Un bien à double usage n'échappe pas à cette qualification du seul fait de son usage civil : dès lors qu'il contribue effectivement à l'action militaire, il peut devenir une cible licite, sous réserve de proportionnalité. La règle produit un effet rarement relevé : en acceptant qu'une partie au conflit utilise sa capacité à des fins militaires, l'opérateur expose son propre segment, station sol, faisceau ou satellite, à devenir un objectif, et avec lui les usagers civils qui partagent cette ressource. Le risque n'est plus seulement que le service soit détourné ; il est qu'il devienne dangereux pour ceux qui en dépendent légitimement.

Ce corpus trace enfin la limite au-delà de laquelle le personnel de l'entreprise sort de la protection due aux civils. La participation directe aux hostilités, dont l'interprétation reste discutée, vise les actes susceptibles de causer un dommage à une partie au conflit et présentant un lien de causalité direct avec ce dommage[76]. Une assistance technique fournie en temps réel à une opération militaire s'en rapproche davantage qu'une fourniture de capacité contractuelle. La frontière importe moins que son existence. Elle impose à l'opérateur, au degré 3, de définir ce que ses équipes peuvent et ne peuvent pas faire.

[74] Art. 2 et 3 communs aux quatre Conventions de Genève du 12 août 1949 ; sur les critères de qualification, voir la jurisprudence du Tribunal pénal international pour l'ex-Yougoslavie, aff. Tadić, 2 octobre 1995.
[75] Protocole additionnel I aux Conventions de Genève, 8 juin 1977, art. 52, § 2.
[76] CICR, Guide interprétatif sur la notion de participation directe aux hostilités en droit international humanitaire, Genève, 2009.

Section 3. Le fondement tiré du statut de l’opérateur

§ 17. L’opérateur adossé à la puissance publique

Les deux premiers fondements tiennent au service et au contexte. Le troisième tient à ce qu’est devenu l’opérateur lui-même. Les Principes directeurs comportent, à cet égard, une disposition rarement mobilisée. Le principe 4 énonce que lorsque l’État détient, contrôle, finance ou soutient une entreprise, ou lorsqu’il recourt à ses services, il doit prendre des mesures supplémentaires pour exiger d’elle une diligence raisonnable en matière de droits humains[77]. L’attente n’est plus celle qui pèse sur une société ordinaire. Renforcée par le lien avec la puissance publique, elle pèse d’abord sur celle-ci.

Appliquée au secteur satellitaire européen, cette disposition trouve un terrain favorable, où trois liens se superposent. L’État français est d’abord devenu le premier actionnaire du principal opérateur français[78]. Il en est ensuite le client, cet opérateur fournissant des services aux forces armées dans le cadre d’un contrat public[79]. Il lui a enfin concédé une mission, l’opérateur appartenant au consortium chargé de déployer et d’exploiter la constellation souveraine européenne[80].

Au terme d’augmentations de capital d’un milliard cinq cents millions d’euros réalisées fin 2025, l’Agence des participations de l’État a souscrit pour 749,3 millions, soit la moitié de l’opération, portant la participation publique à 29,65 % du capital. L’État n’est pas un actionnaire parmi d’autres. Il est le premier, et il a investi dans cette seule opération plus de la moitié du chiffre d’affaires annuel de l’entreprise. Le ministre y a vu la consolidation d’un acteur situé au cœur des infrastructures critiques, le dirigeant la réaffirmation du caractère stratégique des télécommunications spatiales.

Ce lien s’est doublé d’un dispositif dont la portée dépasse celle d’une participation ordinaire : une convention de protection des actifs stratégiques, signée avec l’État et destinée à protéger ses intérêts de souveraineté dans le domaine spatial. Elle lui confère un droit d’agrément préalable sur certains transferts d’actifs, des exigences de nationalité au sein des

[77] Principes directeurs, préc., principe 4 et son commentaire.

[78] MINISTÈRE DE L’ÉCONOMIE, DES FINANCES ET DE LA SOUVERAINETÉ INDUSTRIELLE, ÉNERGÉTIQUE ET NUMÉRIQUE, « Souveraineté industrielle et numérique : l’État devient le premier actionnaire d’Eutelsat », communiqué de presse n° 199, 12 décembre 2025. L’Agence des participations de l’État a souscrit à hauteur de 749,3 millions d’euros à une série d’augmentations de capital d’un montant total de 1,5 milliard d’euros, portant la participation de l’État à 29,65 % du capital.

[79] L’accord-cadre NEXUS, conclu avec le ministère des Armées et des Anciens combattants pour un montant maximal d’un milliard d’euros sur huit ans, a donné lieu à un premier contrat subséquent, dit CENTAURE, conclu avec la Direction générale de l’armement en juin 2026, comportant un engagement ferme initial de 138 millions d’euros sur quatre ans pour la mise à disposition de capacités en orbite basse. Source : EUTELSAT COMMUNICATIONS, communiqué de résultats annuels de l’exercice 2025-26, 7 août 2026.

[80] Contrat de concession IRIS² du 16 décembre 2024 et accord de mise en œuvre du 7 août 2026, préc.

instances dirigeantes, l'obligation de maintenir en France des activités sensibles, et surtout les modalités de fourniture à l'État de certains services de communication par satellite. Et à cela s'ajoute, dans la principale filiale d'exploitation, une action spécifique : l'État peut y nommer administrateurs et censeurs, et opposer son veto aux décisions touchant les activités sensibles[81].

L'État ne s'est donc pas contenté d'entrer au capital. Il s'est réservé, par contrat et par action spécifique, le pouvoir d'empêcher certaines décisions et de fixer les conditions dans lesquelles la capacité lui est fournie. Sur la question de savoir qui décide, une réponse partielle existe déjà en droit positif, mais elle est asymétrique : elle organise la protection des intérêts souverains de l'État, non celle des personnes affectées par l'usage de la capacité. Le même instrument qui permettrait de faire prévaloir une considération de droits humains n'a été conçu que pour faire prévaloir une considération de souveraineté.

L'État qualifie donc cette activité d'infrastructure critique, il en devient le premier actionnaire, il en achète les services pour ses armées et lui concède un programme souverain. Mais pour autant, il ne lui impose aucune obligation de diligence en matière de droits humains, faute d'atteindre les seuils. Le principe 4 postule exactement l'inverse, puisque c'est du lien avec la puissance publique que devrait naître un surcroît d'exigence. Ainsi, la situation française présente, en un même point, le maximum de lien étatique et le minimum d'obligation.

§ 18. Le rattachement par le droit spatial

L'article VI du Traité de 1967 pose que les États portent la responsabilité internationale des activités nationales dans l'espace, y compris lorsqu'elles sont menées par des entités non gouvernementales, et que ces activités doivent faire l'objet d'une autorisation et d'une surveillance continue de la part de l'État concerné[82]. La responsabilité de l'État ne se limite donc pas à ses propres opérations. Elle s'étend à celles des sociétés qu'il autorise, singularité du droit spatial par rapport au droit international commun.

La loi française de 2008 relative aux opérations spatiales met en œuvre cette obligation. Elle soumet à autorisation préalable l'exercice des opérations spatiales, confie l'instruction technique à l'établissement public compétent, et prévoit que l'autorisation peut être refusée, retirée ou suspendue lorsque l'opération apparaît de nature à compromettre les intérêts de la défense nationale ou le respect par la France de ses engagements internationaux[83].

[81] EUTELSAT COMMUNICATIONS, Amendement au document d'enregistrement universel 2024-25, déposé le 24 novembre 2025, section 7.3.4.2 « Convention de protection des actifs stratégiques » et section 4.4.5 relative aux facteurs de risque liés à la structure de l'actionnariat et à l'existence d'accords spécifiques et d'actions spécifiques. Le droit de veto porte sur les activités sensibles telles que définies par le règlement intérieur du comité de sécurité.
[82] Traité sur les principes régissant les activités des États en matière d'exploration et d'utilisation de l'espace extra-atmosphérique, 27 janvier 1967, art. VI.
[83] Loi n° 2008-518 du 3 juin 2008, préc., art. 2 (autorisation préalable), art. 4 (garanties morales, financières et professionnelles et conformité à la réglementation technique), art. 5 (prescriptions pouvant avoir pour objet

Le Pacte international relatif aux droits civils et politiques, la Convention européenne des droits de l'homme et les Conventions de Genève constituent des engagements internationaux de la France au sens de ce texte. Une opération spatiale contribuant à des atteintes graves aux droits humains serait donc de nature à compromettre le respect de ces engagements. Le levier existe ; il n'a, semble-t-il, jamais été mobilisé sur ce fondement, l'appréciation s'étant concentrée sur la sécurité des biens et les intérêts de défense.

§ 19. La diligence renforcée comme contrepartie de la puissance conférée

Les trois fondements exposés dans ce chapitre, nature du service, contexte de délivrance et statut de l'opérateur, se renforcent mutuellement. Leur convergence permet une justification unifiée, tenant à l'économie générale du secteur.

Un opérateur satellitaire n'exerce pas une activité librement accessible. Il exploite deux ressources rares et attribuées, positions orbitales et fréquences, réparties dans le cadre de l'Union internationale des télécommunications et notifiées par les administrations nationales[84]. Il exerce ensuite son activité sous un régime d'autorisation administrative, sans lequel aucune opération n'est licite. Il bénéficie enfin, de plus en plus fréquemment, de financements publics et de commandes publiques. Rien, dans cette activité, ne procède du seul jeu de la liberté d'entreprendre : chaque élément de la position dont l'opérateur dispose lui a été conféré par une autorité publique, nationale ou internationale.

Il est alors cohérent que cette position s'accompagne d'exigences que l'on n'imposerait pas à une entreprise ordinaire : la diligence renforcée n'est ni une sanction ni une charge, mais la contrepartie d'une puissance qui n'a pas été acquise sur un marché. Ce raisonnement rejoint l'alliance décrite par la doctrine de la compliance, mais en révèle la limite : elle suppose un but fixé par une autorité légitime, dont l'entreprise n'est que l'exécutant[85]. Or l'hypothèse étudiée est celle où cette condition fait défaut. Lorsque l'État qui a délivré l'autorisation est aussi celui qui demande la coupure, ou lorsque deux États adressent des injonctions inconciliables, le schéma de l'alliance trouve sa limite, l'entreprise pouvant être confrontée à des injonctions politiques concurrentes sans que le droit lui indique laquelle doit prévaloir.

Cette hypothèse n'est pas théorique, et la structure capitalistique de l'opérateur français l'illustre. À l'issue de l'opération de décembre 2025, l'État français est le premier actionnaire,

d'assurer le respect par la France de ses engagements internationaux) et art. 9 (retrait ou suspension). Décret n° 2009-643 du 9 juin 2009, art. 12 : la décision est prise par le ministre chargé de l'espace après avis du ministre de la défense, le titulaire disposant de trente jours pour faire valoir ses observations.

[84] Constitution et Convention de l'Union internationale des télécommunications ; Règlement des radiocommunications, procédures de notification et de coordination des assignations de fréquence et des positions orbitales.

[85] FRISON-ROCHE (M.-A.), « Les Buts Monumentaux, cœur battant du Droit de la Compliance », préc. Le raisonnement suppose un but édicté par le Politique et concrétisé par l'opérateur, donc une convergence entre eux.

mais partage cette qualité d'actionnaire de référence avec le gouvernement britannique, aux côtés d'investisseurs privés indien et français[86]. Deux États souverains, dont les politiques étrangères peuvent diverger, siègent au capital de la même entreprise, qui exploite une capacité susceptible d'être demandée par l'un et refusée par l'autre. La question de savoir qui décide n'a donc rien d'un cas d'école. Elle est inscrite dans la composition même de l'actionnariat.

La construction doctrinale a été pensée pour des buts que les États partagent au moins dans leur principe : lutte contre la corruption, préservation du climat, protection des données. Elle est mise en échec par des buts sur lesquels ils s'opposent, ce qui est le cas de l'accès aux communications en temps de conflit, hypothèse qui n'a rien de marginal pour un opérateur satellitaire puisqu'elle est son ordinaire dès qu'il dessert une zone disputée. La vigilance renforcée ne peut donc se limiter à élever le niveau d'exigence, il lui faut désigner l'instance qui tranche.

[86] Communiqué de presse n° 199 du 12 décembre 2025, préc. Outre l'État français, les actionnaires de référence ayant participé à l'opération sont le gouvernement britannique, Bharti Space, CMA CGM et le Fonds stratégique de participations.

Partie 2. Le contenu opérationnel de la diligence graduée et ses tempéraments

Chapitre 1. Le contenu : construire une diligence calibrée sur le degré du contexte

Section 1. L'évaluation contextualisée

§ 20. La qualification préalable du contexte

Une échelle n'a d'utilité que si l'on sait y situer une situation donnée. La première diligence attendue de l'opérateur n'est donc pas la cartographie de ses risques, mais la qualification des contextes dans lesquels il délivre son service. Cette opération, qui n'a d'équivalent dans aucun dispositif de conformité existant, doit être organisée avec la même rigueur qu'une classification de risque en matière de blanchiment. Elle suppose d'abord des sources, comme des rapports d'organisations internationales, des décisions de juridictions régionales, des travaux d'organisations non gouvernementales spécialisées ou encore des listes de mesures restrictives.

Elle appelle ensuite une procédure. Qui qualifie ? La conformité, le plus souvent, sur avis des directions commerciale et technique. À quel niveau la qualification est-elle validée, à quelle fréquence est-elle revue, et par quelle voie d'urgence peut-elle être modifiée ? Une qualification annuelle serait sans valeur. Les situations qui font passer un pays du degré 0 au degré 2 se forment en quelques semaines, parfois en quelques jours.

Elle suppose enfin une trace : une note datée, motivée, mentionnant les sources et les indices ayant conduit au degré retenu. Cette note est le premier élément du dossier de décision et le premier document qu'un juge examinerait. Une entreprise capable d'établir qu'elle avait qualifié un contexte au degré 2 six mois avant l'incident, et qu'elle en avait tiré des conséquences opérationnelles, se trouve dans une position radicalement différente de celle qui découvre la situation le jour où elle est mise en cause.

Cependant, cette exigence fait reposer sur l'entreprise une appréciation politique qu'elle n'a ni vocation ni légitimité à porter seule. Qualifier un État de contexte à haut risque par maîtrise n'est pas un acte neutre. C'est pourquoi la proposition défendue plus loin comporte un mécanisme de qualification officielle, transposé du règlement sur les minerais, fournissant aux opérateurs une référence extérieure *(infra, § 37)*.

§ 21. La cartographie des risques appliquée à un portefeuille de capacité

Une fois le contexte qualifié, la cartographie peut être conduite. C'est ici que les exigences dégagées par le juge français trouvent leur pleine utilité, car elles fournissent une méthode transposable : démarche méthodique et traçable, hiérarchisation selon des critères explicites,

correspondance entre les risques identifiés et les mesures annoncées, association des parties prenantes[87].

Transposée à un portefeuille de capacité satellitaire, elle conduit à croiser six axes. Trois tiennent à la ressource et à sa destination : la zone de couverture, la nature de la capacité, le type de client. Trois tiennent à ce que l'opérateur peut savoir et à ce qu'une décision coûterait : le canal de distribution, les antécédents publics du client et du pays, et la criticité du service pour les populations civiles.

§ 22. Du Know Your Customer au Know Your Use

Les dispositifs existants de connaissance du client, issus de la lutte contre le blanchiment et du respect des sanctions internationales, sont déjà en place chez tout opérateur sérieux. Ils vérifient l'identité du cocontractant, ses bénéficiaires effectifs, son absence des listes de mesures restrictives. Ils sont nécessaires et notoirement insuffisants, pour une raison simple : un client parfaitement identifié, parfaitement licite et parfaitement solvable peut faire de la capacité acquise un usage attentatoire. Ainsi, l'identité ne dit rien de l'usage.

Le modèle de la transposition existe pourtant, et il se trouve dans le régime des exportations. L'article 5 du règlement de 2021 soumet à autorisation l'exportation de biens de cybersurveillance non listés lorsque l'exportateur, au terme de ses propres procédures de diligence, a connaissance d'éléments indiquant un risque d'usage lié à la répression interne ou à des violations graves des droits humains[88]. Ce mécanisme présente trois qualités : il ne crée pas d'obligation générale de contrôle, ce qui le rend proportionné ; il fait naître l'obligation des constatations de l'entreprise elle-même, ce qui interdit de se réfugier dans l'ignorance volontaire ; et il oriente le contrôle vers l'usage plutôt que vers le produit, ce qui est précisément ce que la nature duale de la capacité impose *(supra, § 11)*.

Transposé au secteur satellitaire, ce mécanisme prend la forme d'une connaissance de l'usage, reposant sur une déclaration d'usage final et sur une liste de signaux d'alerte arrêtée à l'avance. Définir ces signaux par avance conditionne l'efficacité du dispositif, et c'est ce qui empêche l'entreprise de décider, après coup, que ce qu'elle a vu ne méritait pas d'être vu *(cf. annexe n° 4 p. 63)*.

La gradation intervient ici de manière particulièrement nette. Au degré 1, la difficulté est d'identifier l'utilisateur réel derrière une chaîne opaque. La diligence est alors une enquête, et elle porte sur les faits. Au degré 2, l'utilisateur est parfaitement connu, puisqu'il s'agit souvent

[87] CA Paris, 17 juin 2025, préc. ; TJ Paris, 5 décembre 2023, préc.
[88] Règlement (UE) 2021/821, préc., art. 5 ; recommandation (UE) 2024/2659 de la Commission du 11 octobre 2024 concernant des orientations pour l'exportation de biens de cybersurveillance au titre de l'article 5 du règlement (UE) 2021/821.

d’une administration, et rien ne reste à découvrir. La diligence est alors une appréciation, et elle porte sur la finalité. Un dispositif conçu pour le premier cas est inopérant dans le second, et c’est l’une des raisons pour lesquelles les programmes de conformité existants, tous construits sur la vérification d’identité, laissent le degré 2 sans réponse.

Section 2. La gouvernance de la décision d’urgence

§ 23. L’architecture décisionnelle de crise

La question la plus concrète que soulève ce sujet est aussi la plus rarement posée : qui, dans l’entreprise, a le pouvoir d’interrompre un service ? La réponse détermine tout le reste, car elle désigne à la fois celui qui décidera dans l’urgence et celui dont la décision sera examinée ensuite. Or il n’est pas rare que cette compétence ne soit explicitement attribuée à personne. Elle est alors exercée de fait par celui qui, la nuit venue, se trouve en mesure d’agir. Une diligence renforcée suppose donc une attribution formelle de compétence, dont le niveau varie avec le degré du contexte : direction de la conformité au degré 1, comité mixte associant conformité, juridique et direction générale au degré 2, direction générale et information du conseil d’administration au degré 3. Le circuit correspondant, avec les délais et les traces attendues à chaque étape, est proposé en annexe *(cf. annexe n° 3 p. 62)*.

§ 24. La traçabilité de l’arbitrage : le dossier de décision comme objet juridique

Il a été établi qu’aucune option n’est neutre *(supra, § 12)* et que le juge du devoir de vigilance contrôle la méthode sans se substituer à l’entreprise sur le fond *(supra, § 2)*. Ces deux propositions conduisent à une conclusion unique : la seule chose que l’opérateur puisse démontrer, et donc la seule sur laquelle il puisse être jugé, est la qualité du processus par lequel il a tranché. C’est pourquoi le dossier de décision doit être conçu, dès l’origine, comme un objet juridique et non comme un compte rendu interne.

Sa composition peut être normalisée, des faits tels qu’ils étaient connus au moment de la décision jusqu’aux mesures d’accompagnement retenues, en passant par la qualification du contexte, la base légale invoquée et les options écartées (cf. annexe n° 2 p. 61). Ce formalisme n’est pas bureaucratique. Il reproduit ce que le juge cherchera à reconstituer, et l’organise au moment où l’information est encore disponible.

Cette pratique n’a rien d’inédit en conformité. Les décisions prises en matière de sanctions internationales ou de contrôle des exportations font l’objet d’une documentation comparable, précisément parce que le contrôle en est différé. La documentation constituée au titre du reporting de durabilité peut, par ailleurs, servir de support à cette exigence *(supra, § 9)*. Ce qui doit changer est l’objet de la traçabilité : il ne s’agit plus de démontrer que l’entreprise s’est

conformée à une règle, mais qu'elle a arbitré entre des conséquences humaines contradictoires en connaissance de cause. Le contrôle portera donc principalement sur les conditions dans lesquelles la décision a été préparée, motivée et documentée.

Cette exigence probatoire n'est pas propre à la matière. La doctrine a décrit un mouvement de juridictionnalisation de la compliance, par lequel le modèle du procès pénètre l'ensemble du dispositif : les décisions prises au titre de la compliance sont destinées à être discutées devant un juge et doivent donc être construites, dès l'origine, comme des pièces produisibles[89]. Le dossier décrit ici en est l'application à la décision de maintien ou de suspension d'une capacité ; le circuit correspondant est détaillé en annexe (cf. annexe n° 3 p. 62). Il ne s'agit pas d'un formalisme ajouté à la gestion de crise, mais de la constitution en temps réel du seul élément qui permettra d'établir que l'arbitrage a été rendu et non subi.

§ 25. Le mécanisme d'alerte calibré sur le contexte

Les dispositifs d'alerte ont été conçus pour des salariés : la directive sur la protection des lanceurs d'alerte et sa transposition française organisent des canaux accessibles au personnel et à certains tiers en relation professionnelle avec l'entreprise[90]. Celui de la loi de 2017 est élaboré avec les organisations syndicales représentatives. Ces dispositifs sont utiles, mais structurellement inaptes à recueillir l'alerte d'un civil affecté par une interruption de service à des milliers de kilomètres.

Les Principes directeurs en fournissent les critères : légitime, accessible, prévisible, équitable, transparent, compatible avec les droits et fondé sur le dialogue avec les groupes auxquels il est destiné[91]. Appliqués à notre objet, ils imposent quatre adaptations, détaillées en annexe. L'accessibilité linguistique d'abord. La sécurité de l'alertant ensuite, lorsque l'alerte vise l'État où il réside. La médiation par des tiers de confiance. Et un délai compatible avec une atteinte en cours *(cf. annexe n° 4 p. 63)*.

Section 3. Les leviers d'action et leur mise en œuvre

§ 26. L'outillage contractuel

Le contrat est le premier instrument dont dispose l'opérateur, et souvent le seul à produire un effet juridique direct sur le comportement du client. Encore faut-il le rédiger pour être exécuté, et non pour être produit en défense. Quatre familles de clauses se distinguent par leur fonction

[89] FRISON-ROCHE (M.-A.) (dir.), La juridictionnalisation de la Compliance, coll. « Régulations & Compliance », Journal of Regulation & Compliance (JoRC) et Dalloz, 2023, 489 p.
[90] Directive (UE) 2019/1937 du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union ; loi n° 2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte.
[91] Principes directeurs, préc., principe 31.

réelle. La déclaration d'usage final, la vérification, la suspension graduée, le traitement des demandes étatiques *(cf. annexe n° 4 p. 63)*.

La première mérite un mot, son utilité étant mal comprise. Son intérêt n'est pas informatif, un client de mauvaise foi déclarant ce qu'il faut, mais probatoire et pénal : la fausse déclaration caractérise un manquement contractuel et affecte l'élément intentionnel d'une mise en cause éventuelle *(infra, § 30)*.

Une pratique doit être écartée : celle des clauses miroir, par lesquelles l'entreprise se borne à répercuter sur son cocontractant les obligations qui lui incombent, en se réservant une action en garantie. Ce mécanisme transfère le risque juridique sans réduire le risque réel pour les personnes, et il est aujourd'hui critiqué comme tel, y compris dans les travaux préparatoires du droit européen de la vigilance. Une clause n'est un instrument de diligence que si elle est assortie d'une vérification et d'une conséquence effective ; à défaut, elle n'est qu'un instrument d'allocation de responsabilité entre professionnels.

§ 27. La réponse aux demandes étatiques

On aborde ici la situation la plus difficile, et celle où le droit positif est le plus démuni. Un État adresse à l'opérateur une demande d'interruption, de restriction ou d'accès. Elle émane d'une autorité, invoque une base légale, s'accompagne d'un délai bref. L'entreprise doit décider seule, et ni la loi de 2017, ni la directive européenne, ni le droit spatial ne lui indiquent comment.

Les Principes directeurs posent la règle : en cas de conflit entre le respect des droits humains et les prescriptions du droit national, l'entreprise doit chercher les moyens de respecter les principes internationaux et démontrer ses efforts[92]. Le seul référentiel sectoriel opérationnel, celui de la Global Network Initiative, organise la réponse aux demandes gouvernementales autour de quelques exigences : base légale écrite, interprétation la plus restrictive possible, contestation des demandes excessives, information des utilisateurs lorsque le droit le permet, publication du volume des demandes reçues[93]. Il présente une lacune décisive. Ses membres évalués dans les télécommunications sont des opérateurs terrestres, et aucun opérateur satellitaire n'y figure[94]. Le seul cadre crédible en matière de demandes étatiques ne couvre pas le secteur qui y est le plus exposé.

Au degré 1, la demande émane souvent d'une autorité dont le titre même est incertain, et c'est sa compétence qu'il faut d'abord vérifier. Au degré 2, la configuration est inverse et plus

[92] Ibid., principe 23, point b), et son commentaire.
[93] GLOBAL NETWORK INITIATIVE, Principles on Freedom of Expression and Privacy et Implementation Guidelines.
[94] Liste des entreprises évaluées lors des cycles d'évaluation indépendante conduits par la Global Network Initiative dans le secteur des télécommunications.

embarrassante. L'autorité est incontestablement compétente et sa demande régulière au regard du droit interne ; c'est son contenu qui pose difficulté. L'entreprise affronte un conflit entre légalité interne et droits fondamentaux qu'aucun texte ne l'habilite à trancher. Les seules ressources disponibles sont procédurales. Exiger la formalisation écrite, apprécier la nécessité et la proportionnalité, restreindre l'exécution à ce qui est strictement demandé, épuiser les voies de contestation locales, documenter chaque étape, alerter le cas échéant l'État d'établissement. C'est peu. C'est pourtant tout ce dont l'opérateur dispose.

Au degré 3, la demande émane d'une partie au conflit, parfois de l'État de nationalité de l'opérateur, et croise le régime des sanctions et du contrôle des exportations. Il ne s'agit plus d'apprécier la légitimité de la demande mais d'articuler des obligations concurrentes. C'est le seul degré où l'entreprise peut être tenue d'exécuter en vertu d'un texte contraignant, la diligence consistant alors à documenter la contrainte plutôt qu'à s'y opposer.

§ 28. La sortie responsable

Reste l'issue que l'on présente spontanément comme la plus prudente : cesser le service. Les Principes directeurs invitent à ne pas y recourir mécaniquement, demandant que soient prises en compte les conséquences du désengagement pour les personnes[95], et le guide du Programme des Nations unies pour le développement a développé cette exigence sous le nom de sortie responsable[96].

Cette réserve prend ici une portée qu'elle n'a nulle part ailleurs, puisque la privation du service est elle-même une atteinte potentielle. Interrompre un faisceau parce qu'un client en fait un usage contestable prive tous les autres utilisateurs de la même ressource. La suspension ne peut donc être tenue par principe pour l'option la moins risquée. Elle doit elle-même faire l'objet d'une appréciation de ses conséquences, au même titre que le maintien.

Il en résulte une hiérarchie des réponses que la procédure interne devrait consacrer, du moins au plus radical. La restriction ciblée vient en premier, puis le levier contractuel, puis le non-renouvellement à l'échéance. La suspension immédiate ne se justifie qu'en dernier rang, lorsque la gravité et l'imminence de l'atteinte l'imposent.

[95] Principes directeurs, préc., principe 19 et son commentaire.
[96] PNUD, Heightened Human Rights Due Diligence for Business in Conflict-Affected Contexts, préc., développements relatifs au responsible exit.

Chapitre 2. Les tempéraments : la mesure juste de la responsabilité

Section 1. Le refus du garant universel

§ 29. L’influence limitée et sa portée juridique

Tout ce qui précède décrit une exigence renforcée ; il faut maintenant en fixer les bornes, faute de quoi la proposition serait injuste et inapplicable. Le premier tempérament tient à ce que l’opérateur ne maîtrise pas la chaîne au bout de laquelle son service est employé.

Les Principes directeurs raisonnent en termes d’effet de levier, c’est-à-dire de capacité effective à modifier le comportement de l’entité qui cause l’atteinte[97]. Cette capacité varie considérablement selon la configuration commerciale. Elle est réelle lorsque l’opérateur contracte directement avec l’utilisateur final, et qu’il dispose d’une relation suivie, d’un contrat en cours et d’une prestation individualisable. Elle décroît lorsque la capacité est vendue à un distributeur qui la revend, puis à un intégrateur qui l’assemble à d’autres services. Elle devient parfois nulle lorsque le client est un État, qui n’acceptera ni audit, ni clause de suspension, ni déclaration d’usage final.

Cette limite n’est pas une donnée de fait. Le droit européen l’a consacrée. En recentrant la vigilance sur les partenaires commerciaux directs, la directive de février 2026 a reconnu qu’une surveillance illimitée le long de la chaîne excédait ce qu’une entreprise peut raisonnablement accomplir[98]. Il faut assumer ici un usage bilatéral du même texte : cette directive a servi à fonder l’intensification de la vigilance, en consacrant l’approche par les risques *(supra, § 15)* ; elle sert à présent à en limiter la portée, en consacrant la primauté du lien direct. La contradiction n’est qu’apparente : les deux mouvements procèdent du même principe, la vigilance se mesurant à ce que l’entreprise peut réellement connaître et influencer.

§ 30. La fausse déclaration du client

Le cas appelle un traitement propre, étant le plus fréquent en pratique et le plus mal traité en doctrine. Un client déclare un usage civil, obtient la capacité, l’emploie à d’autres fins. L’opérateur a-t-il manqué à ses obligations ? La réponse n’est ni un acquittement automatique ni une imputation mécanique ; elle se construit en trois temps.

Premier temps : la fausse déclaration n’exonère pas lorsque des indices contraires étaient accessibles. C’est la solution du contrôle des exportations, où l’exportateur ne peut se retrancher derrière l’attestation d’usage final s’il disposait d’éléments propres à éveiller ses soupçons. Le critère décisif est le degré du contexte : au degré 2 ou 3, le niveau de vérification attendu est plus

[97] Principes directeurs, préc., principe 19, commentaire relatif à l’effet de levier.
[98] Directive (UE) 2026/470, préc.

élevé, et des indices négligeables ailleurs deviennent des signaux d'alerte. L'échelle produit ici un effet direct sur l'imputation.

Deuxième temps : elle exonère lorsque la diligence correspondant au degré identifié a été régulièrement conduite. Si l'opérateur a qualifié le contexte, appliqué les vérifications prévues, examiné les signaux d'alerte et documenté ses constatations, la fausse déclaration du client est susceptible de peser de manière déterminante dans l'appréciation de l'imputation. C'est la contrepartie d'une obligation de moyens : la mise en œuvre sérieuse de la méthode doit être prise en compte dans l'appréciation de la responsabilité de l'opérateur.

Troisième temps : la découverte fait naître une obligation nouvelle. Dès qu'il apprend l'usage réel, l'opérateur ne peut plus invoquer son ignorance et devient tenu d'agir, selon la hiérarchie des réponses exposée plus haut *(supra, § 28)*. C'est là que se joue l'appréciation de son comportement : l'inaction postérieure à la découverte, bien plus que la tromperie initiale, caractériserait une contribution au sens du principe 13.

§ 31. Entre responsabilité diluée et obligation paralysante

Les deux écueils sont symétriques. Une responsabilité diluée dans une chaîne d'intermédiaires ne protège personne, puisque nul n'en répond. Une obligation trop lourde produit l'effet inverse de celui recherché. L'opérateur prudent se retire des contextes à risque, et les populations perdent l'accès à un service dont elles dépendent, au profit d'acteurs moins scrupuleux. Cet effet d'éviction est documenté dans d'autres secteurs soumis à des obligations intenses ; quiconque propose un renforcement doit le prendre au sérieux.

Le critère d'équilibre proposé est celui de la prévisibilité raisonnable, apprécié ex ante. L'opérateur répond des atteintes qu'il pouvait prévoir au moment de sa décision, compte tenu des informations dont il disposait ou aurait dû disposer eu égard au degré du contexte, et des moyens dont il disposait pour agir. Il ne répond pas de ce qui n'était pas prévisible, ni de ce qu'il n'avait aucun moyen d'empêcher.

Ce critère présente trois avantages. Il est connu du droit français de la responsabilité, où il structure l'appréciation de la faute. Il est compatible avec l'office du juge de la vigilance, qui contrôle la méthode et refuse de fixer le résultat à la place de l'entreprise, comme l'illustre le jugement rendu contre TotalEnergies, le tribunal ayant enjoint de compléter le plan tout en refusant de déterminer la cible[99]. Il est enfin praticable, parce qu'il se prouve : ce que l'entreprise savait à un instant donné est établi par le dossier de décision *(supra, § 24)*.

[99] TJ Paris, 25 juin 2026, préc.

La doctrine fournit ici l'instrument de mesure qui manquait. Classant les obligations de compliance selon qu'elles relèvent de l'obligation de moyens ou de résultat, Marie-Anne Frison-Roche soutient que l'entreprise n'est pas tenue d'atteindre le but monumental, ce qui excéderait sa portée, mais de construire une structure produisant des effets crédibles au regard de ce but[100]. La formule livre le curseur recherché. Intensifier la vigilance de l'opérateur, c'est élever l'exigence pesant sur la structure : qualification du contexte, traçabilité de l'arbitrage, niveau hiérarchique de la décision, délai de réexamen. Ce n'est pas convertir l'obligation de moyens en obligation de résultat, ce qui ferait de l'opérateur le garant de l'usage final de sa capacité. Le renforcement porte sur le dispositif, non sur l'issue.

Section 2. La cartographie des risques encourus par l'opérateur

§ 32. Le risque pénal et ses qualifications

Le paradoxe le plus frappant du sujet apparaît ici. L'opérateur satellitaire n'est soumis à aucune obligation de diligence ; il encourt pourtant le risque juridique le plus lourd, celui de la complicité. L'absence de norme de comportement n'a pas fait disparaître le risque, elle a supprimé la méthode permettant de s'en prémunir.

Les affaires Amesys et Nexa Technologies en fournissent la démonstration. Des dirigeants de ces sociétés françaises, qui avaient fourni des systèmes de surveillance à la Libye puis à l'Égypte, ont été mis en examen en juin 2021 par le pôle spécialisé du tribunal judiciaire de Paris, pour complicité de tortures dans le premier volet et complicité de tortures et de disparitions forcées dans le second, à la suite de plaintes d'organisations de défense des droits humains. L'état des deux procédures a depuis divergé, la chambre de l'instruction ayant confirmé les mises en examen du volet libyen et annulé celles du volet égyptien, sans clôture de l'information[101]. Ce précédent établit qu'une fourniture technologique peut être saisie par le juge pénal français à raison d'usages commis à l'étranger par un État tiers.

L'application au secteur satellitaire suppose toutefois de traiter l'élément intentionnel. La complicité par fourniture de moyens exige la connaissance de la destination criminelle de l'aide[102]. Or la capacité de communication n'est pas conçue pour porter atteinte aux droits, à la différence d'un système d'interception *(supra, § 11)*. Cette différence protège l'opérateur, mais

[100] FRISON-ROCHE (M.-A.), « Concevoir l'Obligation de Compliance : faire usage de sa position pour participer à la réalisation des Buts Monumentaux de la Compliance », in L'Obligation de Compliance, préc., p. 3 à 44.

[101] Mises en examen prononcées les 16 et 17 juin 2021 par le pôle crimes contre l'humanité du tribunal judiciaire de Paris. Par arrêt du 21 novembre 2022, la chambre de l'instruction de la cour d'appel de Paris a confirmé celles de la société Amesys et de ses dirigeants dans le volet libyen tout en annulant celles de deux salariés ; par arrêt du 14 décembre 2022, elle a annulé celles de la société Nexa Technologies et de quatre dirigeants et salariés dans le volet égyptien. L'information judiciaire s'est poursuivie dans les deux cas.

[102] Art. 121-7 du code pénal ; sur l'exigence de connaissance, voir la jurisprudence relative à la complicité par fourniture de moyens.

seulement tant qu'il ignore. Dès lors que le contexte a été qualifié, que des signaux d'alerte ont été relevés et qu'aucune conséquence n'en a été tirée, la connaissance devient difficile à contester. Il en résulte un effet contre-intuitif qu'il faut nommer : une diligence sérieusement conduite ne crée pas le risque pénal, elle en fixe le périmètre, en permettant d'établir ce que l'entreprise savait et ce qu'elle a fait de ce savoir.

La gradation éclaire la nature du risque encouru. Le degré 2 correspond à la configuration de ces affaires : un État fonctionnel employant à des fins de répression une technologie fournie, avec pour qualifications possibles la complicité de tortures ou de disparitions forcées. Le degré 3 ouvre le registre de la complicité de crimes de guerre, dès lors que la capacité contribuerait à des opérations dirigées contre des civils. Ces qualifications n'ont rien de théorique : ce sont des qualifications qu'un juge d'instruction pourrait être conduit à envisager.

§ 33. Le risque civil après le renvoi aux droits nationaux

Le risque civil a connu en 2026 une transformation ambivalente, l'abandon du régime européen harmonisé renvoyant les victimes aux droits nationaux[103]. Présentée comme une simplification, cette évolution recrée une hétérogénéité dont il n'est pas certain qu'elle serve les entreprises.

L'effet pervers est rarement relevé. L'absence de régime harmonisé ne protège ni l'entreprise, exposée à autant de régimes que d'États membres, ni les victimes, tenues d'identifier une juridiction compétente et de surmonter des obstacles dissuasifs. Cette insécurité symétrique plaide pour une clarification sectorielle, un opérateur qui sait ce que l'on attend de lui étant mieux placé pour s'en acquitter.

La doctrine relève d'ailleurs que l'obligation de vigilance exerce une tension sur le concept même de responsabilité civile, en substituant à une logique de réparation d'un dommage causé une logique de prévention de risques systémiques[104]. La difficulté atteint ici son point extrême : le dommage allégué serait causé par un tiers, le plus souvent un État, sur un territoire étranger, et le manquement reproché à l'opérateur consisterait en une abstention de vigilance dont il faudrait établir qu'elle a rendu l'atteinte possible. Entre le fait générateur et le préjudice s'interposent une décision souveraine et un conflit armé. Aucun système de responsabilité civile n'a été conçu pour une telle chaîne causale, ce qui explique la prudence des juridictions saisies jusqu'à présent.

[103] Directive (UE) 2026/470, préc. ; art. 1240 du code civil ; règlement (CE) n° 864/2007 dit Rome II sur la loi applicable aux obligations non contractuelles.
[104] MEKKI (M.), « Peut-on repenser la responsabilité à l'aune du devoir de Vigilance, pointe avancée de la Compliance ? », in FRISON-ROCHE (M.-A.) (dir.), L'Obligation de Compliance, préc.

§ 34. Le risque réputationnel, actionnarial et de financement

En l'absence de contrainte juridique directe, la pression effective vient d'ailleurs, et trois canaux doivent être distingués.

Le canal associatif d'abord, illustré par l'affaire de l'automne 2022 : une organisation de défense de la liberté de l'information a saisi le régulateur, obtenu une décision du juge administratif et déclenché la mise en demeure. L'action associative supplée ainsi l'absence d'autorité dotée d'un pouvoir d'initiative, mais elle reste tributaire de l'attention médiatique.

Le canal financier ensuite : les investisseurs institutionnels ont leurs propres obligations de publication, et les informations issues du reporting alimentent leurs analyses[105]. Un opérateur dont la gestion des risques droits humains apparaîtrait défaillante s'exposerait à des interrogations lors des campagnes de vote, voire à des exclusions de portefeuille. Le canal actionnarial est enfin particulier dans ce secteur, en raison de la présence d'un actionnaire public, dont les attentes ne se réduisent pas à la rentabilité et qui peut porter des considérations d'intérêt général au sein des organes sociaux.

Ces pressions sont réelles, mais ne sauraient tenir lieu de norme. Elles sont asymétriques, s'exerçant sur les seuls théâtres médiatiquement exposés ; discontinues, suivant le cycle de l'actualité ; indifférentes au processus enfin, puisqu'elles sanctionnent une décision perçue comme mauvaise et non une méthode défaillante, et peuvent frapper une entreprise diligente en épargnant une entreprise négligente dont le cas n'a pas été révélé. Ces mécanismes réputationnels ne peuvent donc se substituer à une régulation fondée sur un processus de diligence identifiable et contrôlable.

Chez l'opérateur français, les sanctions frappant les chaînes russes diffusées par sa flotte, ajoutées à la résiliation d'accords de capacité, expliquent une part du recul de 13,1 % du chiffre d'affaires de l'activité vidéo sur l'exercice 2025-2026. De plus, l'absence d'impact supplémentaire de ces sanctions figure parmi les hypothèses sur lesquelles reposent les objectifs financiers communiqués au marché[106]. Un risque né du traitement de contenus en contexte de conflit est devenu une variable de la prévision financière, portée à la connaissance des investisseurs. La frontière entre risque de droits humains et risque financier, souvent tenue pour théorique, est ici franchie.

---

[105] Règlement (UE) 2019/2088 du 27 novembre 2019 sur la publication d'informations en matière de durabilité dans le secteur des services financiers.

[106] EUTELSAT COMMUNICATIONS, Résultats annuels de l'exercice 2025-26, communiqué de presse, 7 août 2026, préc., analyse du chiffre d'affaires de l'activité Vidéo et note relative aux hypothèses sous-tendant les objectifs financiers. Le communiqué mentionne par ailleurs, au titre des services aux gouvernements, des services fournis en Ukraine.

Section 3. Combler le vide : quatre voies

§ 35. La voie sectorielle spatiale

La première voie est la plus solide, parce qu'elle n'exige aucune construction nouvelle. Il a été établi que le régime français d'autorisation des opérations spatiales permet de refuser, de retirer ou de suspendre une autorisation lorsque l'opération est de nature à compromettre le respect par la France de ses engagements internationaux, et que les conventions relatives aux droits humains sont de tels engagements *(supra, § 18)*. La proposition consiste à expliciter cette condition et à en tirer les conséquences procédurales.

Elle se décline en trois éléments. Une condition d'octroi, d'abord : l'exploitant devrait justifier d'un dispositif de diligence comportant une méthode de qualification des contextes, une procédure de décision d'urgence et un dispositif de traçabilité. Une obligation d'information ensuite : il signalerait à l'autorité les demandes étatiques d'interruption reçues dans un contexte qualifié, selon des modalités préservant le secret des affaires et la sécurité des personnes. Un motif de suspension enfin, distinct de la sanction et soumis au contradictoire.

La même logique peut être portée au niveau européen, et le moment y est favorable. La proposition de règlement sur les activités spatiales repose sur trois piliers, dont aucun ne porte sur les droits humains *(supra, introduction)*, alors que les travaux préparatoires indiquent que le traitement des activités à double usage demeure une question ouverte entre les États membres[107]. Une contribution consisterait à proposer un considérant reconnaissant que les services de communication par satellite peuvent affecter les droits fondamentaux dans les contextes de conflit ou à haut risque, puis une disposition subordonnant l'autorisation à la démonstration d'un dispositif de diligence proportionné au degré du contexte. Elle ne crée aucune obligation de résultat et ne vise que les opérateurs déjà soumis à autorisation.

Il convient alors de se demander ce que font les autres États dont relèvent les grands opérateurs. Nous rapprocherons trois régimes : le régime français, le régime britannique, dont dépend l'essentiel de la constellation en orbite basse exploitée depuis Londres, et le régime des États-Unis, dont relève l'opérateur cité en introduction[108].

---

[107] Travaux préparatoires relatifs à la proposition COM(2025) 335 final, préc.

[108] Pour le Royaume-Uni : Outer Space Act 1986, section 4, paragraphe 2, aux termes duquel le Secrétaire d'État ne délivre la licence que s'il est convaincu que les activités autorisées ne mettront pas en danger la santé publique ou la sécurité des personnes et des biens, seront compatibles avec les engagements internationaux du Royaume-Uni et ne porteront pas atteinte à sa sécurité nationale ; Space Industry Act 2018 pour les activités conduites depuis le territoire britannique. Pour les États-Unis : Communications Act de 1934, titre III, et 47 CFR partie 25, la Commission délivrant l'autorisation lorsque le demandeur est juridiquement et techniquement qualifié et que l'opération sert l'intérêt public.

	France	Royaume-Uni	États-Unis
Texte applicable	Loi n° 2008-518 du 3 juin 2008	Outer Space Act 1986, complété par le Space Industry Act 2018	Communications Act de 1934, titre III ; 47 CFR partie 25
Autorité	Ministre chargé de l'espace, après avis du ministre de la défense	Secrétaire d'État, par l'intermédiaire de la Civil Aviation Authority	Federal Communications Commission
Critère d'octroi	Garanties morales, financières et professionnelles ; conformité technique	Absence de risque pour la santé et la sécurité ; compatibilité avec les engagements internationaux du Royaume-Uni ; préservation de la sécurité nationale	Qualification juridique et technique du demandeur ; conformité de l'opération à l'intérêt public
Référence aux engagements internationaux	Oui : prescriptions de l'article 5 et retrait de l'article 9	Oui : condition d'octroi expresse	Non
Critère de droits humains	Indirect, par le renvoi aux engagements internationaux	Indirect, par la même voie	Aucun
Retrait en cours d'exploitation	Oui, pour compromission des engagements internationaux	Oui, révocation ou modification des conditions de la licence	Oui, mais fondé sur le respect des règles techniques et de l'intérêt public

Deux enseignements s'en dégagent. Le premier rassure, car le levier proposé plus haut n'a rien d'une singularité française. Le droit britannique conditionne expressément l'octroi de la licence à la compatibilité de l'activité avec les engagements internationaux du Royaume-Uni, et permet d'en modifier les conditions en cours d'exploitation. Les deux principaux États d'immatriculation des opérateurs européens disposent donc du même point d'appui, sans l'avoir jamais employé sur ce terrain. Une proposition qui s'y adosse ne crée aucune catégorie nouvelle, elle active une clause existante.

Le second est plus embarrassant. Le régime américain, dont relève l'opérateur dont les décisions ont ouvert ce mémoire, ne comporte rien de tel. La Commission fédérale des communications délivre ses autorisations au vu de la qualification du demandeur et de la conformité de l'opération à l'intérêt public, notion large dont la pratique décisionnelle n'a jamais fait un instrument de droits humains. L'asymétrie doit être assumée. L'opérateur le plus susceptible de décider seul du sort d'une capacité en zone de conflit est celui que le droit de son État d'immatriculation encadre le moins. La voie européenne ne l'atteindra qu'indirectement, par la conditionnalité de l'accès au marché.

§ 36. La voie du contrôle des exportations

La deuxième voie repose sur un mécanisme éprouvé, dont on a montré qu'il constituait le modèle juridique le mieux adapté à la structure du risque *(supra, § 22)*. Il s'agirait d'étendre à la fourniture de capacité le mécanisme de l'article 5 du règlement de 2021 : lorsque l'opérateur a connaissance d'éléments indiquant que le service pourrait contribuer à la répression interne ou à

des violations graves des droits humains, il en informerait l'autorité compétente, à qui il reviendrait de soumettre ou non la fourniture à autorisation.

Deux difficultés doivent être reconnues : la capacité de communication n'est pas un bien exporté au sens classique, et l'extension supposerait d'adapter la notion ; un opérateur non européen n'étant pas soumis à la même contrainte, le risque de contournement subsiste, auquel seule répond la conditionnalité de l'accès au marché européen.

§ 37. La voie de la qualification officielle du contexte

Les deux voies précédentes supposent résolue une question qui ne l'est pas : qui décide qu'un contexte relève du degré 2 ? En faire porter l'appréciation à la seule entreprise, c'est lui demander un jugement politique sur des États avec lesquels elle est en relation contractuelle.

Le modèle a été décrit au premier chapitre : la liste des zones de conflit ou à haut risque établie par la Commission avec le concours d'experts externes *(supra, § 5)*. Trois caractéristiques en font un instrument transposable : le caractère indicatif préserve l'appréciation de l'entreprise et évite de conférer à la liste une portée diplomatique ; le recours à des experts externes place la qualification hors de la négociation politique immédiate ; la mise à jour régulière permet de suivre des situations mouvantes.

La transposition consisterait à établir une liste des contextes à haut risque pour les services de communication, distinguant le haut risque par défaillance du haut risque par maîtrise. La seconde catégorie est la plus délicate, nommant des États dont l'appareil fonctionne, et sans doute la plus nécessaire, étant susceptible de recouvrir une part importante des demandes étatiques.

§ 38. La désignation d'une autorité compétente

Aucune autorité ne dispose aujourd'hui d'une compétence stable pour connaître de la diligence d'un opérateur satellitaire en contexte de conflit ou à haut risque *(supra, § 10)*. Seule une désignation expresse peut la combler. L'autorité chargée du régime des opérations spatiales est la mieux placée, détenant déjà le pouvoir d'autorisation et de suspension qui constitue le levier ; encore faudrait-il lui adjoindre une expertise dont elle ne dispose pas, la sienne étant technique et défensive.

S'y ajouterait un point de contact unique, vers lequel les opérateurs signaleraient les demandes reçues et auprès duquel ils solliciteraient une position en urgence. C'est la réponse la plus directe à la question posée par ce mémoire : un opérateur qui reçoit à minuit une demande d'interruption émanant d'un État étranger n'a aujourd'hui personne à appeler, et la décision reste assumée par lui seul, sans mécanisme institutionnel pour l'encadrer.

Conclusion

§ 39. Un vide qui tient à l'architecture

Le vide constaté n'est pas une lacune de rédaction que le relèvement d'un seuil suffirait à combler. Il procède de l'architecture même du droit de la vigilance.

Le premier décalage tient à la manière dont ce droit a été construit. Il regarde essentiellement vers l'amont de la chaîne, alors que, pour un opérateur satellitaire, le risque apparaît surtout dans l'usage qui est fait du service. Le critère d'assujettissement le confirme : en mesurant l'effectif, le législateur a retenu un indicateur pertinent pour une activité de main-d'œuvre, qui rend mal compte de la portée d'une infrastructure exploitée par quelques centaines de personnes.

À cette première difficulté s'en ajoute une autre. Les catégories existantes appréhendent mal certains contextes dans lesquels l'État, loin d'être défaillant, exerce au contraire un contrôle très étroit sur les communications. La seule catégorie contextuelle dont dispose le droit de l'Union, conçue pour l'extraction minière, ne connaît que la défaillance ; elle laisse hors de son champ la configuration qui paraît la plus fréquente dans le secteur étudié. Or les deux situations n'appellent pas la même diligence, l'une posant un problème de connaissance et l'autre un problème d'arbitrage.

Il en résulte une situation singulière. Les entreprises qui exploitent les infrastructures de communication les plus critiques d'Europe, dont l'État est à la fois actionnaire, client et concédant, ne sont soumises à aucune obligation juridique de diligence en matière de droits humains, tout en encourant, pour les mêmes faits, un risque pénal de complicité. Le vide de la norme de comportement n'est pas un vide de risque : c'est un vide de méthode.

§ 40. Fonder l'exigence, désigner celui qui décide

Au terme de cette analyse, trois éléments paraissent converger en faveur d'une exigence renforcée de diligence : la nature du service fourni, le contexte dans lequel il est délivré et la position particulière de l'opérateur à l'égard de la puissance publique. La première interdit tout filtrage par le produit et fait de la privation elle-même une atteinte possible ; le deuxième module déjà, en droit positif, l'intensité de la vigilance ; la troisième procède d'une position que l'entreprise n'a pas acquise sur un marché. Pris ensemble, ces éléments fournissent un fondement solide à l'intervention du législateur ou de l'autorité compétente, d'autant que le véhicule normatif existe : le régime d'autorisation des opérations spatiales permet de retirer une autorisation compromettant le respect par la France de ses engagements internationaux.

Cette question se pose avec une acuité particulière au moment où l'Union européenne construit sa propre infrastructure satellitaire souveraine. La constellation IRIS² doit entrer en service à la fin de la décennie, tandis que le futur cadre européen applicable aux activités spatiales est encore en discussion, et qu'aucun de ses piliers ne traite directement des droits humains. Les travaux préparatoires montrent d'ailleurs que le traitement du double usage y demeure débattu. Le moment paraît donc propice pour intégrer cette dimension avant que le cadre ne soit définitivement fixé, faute de quoi l'Europe disposera d'une infrastructure souveraine, d'un régime d'autorisation unifié et d'aucun mécanisme permettant de dire qui, un soir de crise, aura le droit de couper.

L'opérateur satellitaire occupe, à cet égard, une position singulière. Il peut être rapproché de l'opérateur crucial décrit par la doctrine de la compliance, puisqu'il détient une capacité que l'État ne peut entièrement reproduire par ses propres moyens[109]. Le secteur ajoute toutefois une difficulté que cette catégorie n'avait pas envisagée : les attentes adressées à l'opérateur peuvent émaner d'États dont les intérêts ne coïncident pas. C'est précisément pour cette raison que la diligence renforcée ne saurait se limiter à accroître les obligations pesant sur l'entreprise. Elle doit aussi déterminer plus clairement qui est légitime pour décider, selon quelle procédure et dans quelles limites.

[109] FRISON-ROCHE (M.-A.), « Les Buts Monumentaux, cœur battant du Droit de la Compliance », préc. ; « La Vigilance, pointe avancée et part totale de l'Obligation de Compliance », préc.

Bibliographie

I. Textes

A. Droit international

Conventions de Genève du 12 août 1949, articles 2 et 3 communs.

Convention de sauvegarde des droits de l'homme et des libertés fondamentales, Rome, 4 novembre 1950.

Pacte international relatif aux droits civils et politiques, New York, 16 décembre 1966.

Traité sur les principes régissant les activités des États en matière d'exploration et d'utilisation de l'espace extra-atmosphérique, y compris la Lune et les autres corps célestes, Londres, Moscou et Washington, 27 janvier 1967.

Protocole additionnel I aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux, Genève, 8 juin 1977.

Convention européenne sur la télévision transfrontière, Conseil de l'Europe, STE n° 132, Strasbourg, 5 mai 1989, entrée en vigueur le 1er mai 1993 ; état des signatures et ratifications consulté le 28 août 2026. L'Ukraine a signé le 14 juin 1996 et ratifié le 26 mars 2009, la Convention entrant en vigueur à son égard le 1er juillet 2009 ; la Fédération de Russie l'a signée sans la ratifier.

UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS, Constitution et Convention de l'Union internationale des télécommunications, Genève, 1992, telles qu'amendées par les Conférences de plénipotentiaires, in Recueil des textes fondamentaux adoptés par la Conférence de plénipotentiaires, UIT, éd. 2023 ; Règlement des radiocommunications, éd. 2024, UIT, Genève, 2024, incorporant les révisions issues de la CMR-23.

B. Droit de l'Union européenne

Règlement (CE) n° 864/2007 du Parlement européen et du Conseil du 11 juillet 2007 sur la loi applicable aux obligations non contractuelles, dit Rome II.

Règlement (UE) 2017/821 du Parlement européen et du Conseil du 17 mai 2017 fixant des obligations liées au devoir de diligence à l'égard de la chaîne d'approvisionnement pour les importateurs de l'Union qui importent de l'étain, du tantale et du tungstène, leurs minerais et de l'or provenant de zones de conflit ou à haut risque.

Directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union.

Règlement (UE) 2019/2088 du Parlement européen et du Conseil du 27 novembre 2019 sur la publication d'informations en matière de durabilité dans le secteur des services financiers.

Règlement (UE) 2021/821 du Parlement européen et du Conseil du 20 mai 2021 instituant un régime de l'Union de contrôle des exportations, du courtage, de l'assistance technique, du transit et des transferts en ce qui concerne les biens à double usage.

Directive (UE) 2022/2464 du Parlement européen et du Conseil du 14 décembre 2022 en ce qui concerne la publication d'informations en matière de durabilité par les entreprises.

Règlement délégué (UE) 2023/2772 de la Commission du 31 juillet 2023 complétant la directive 2013/34/UE en ce qui concerne les normes d'information en matière de durabilité.

Directive (UE) 2024/1760 du Parlement européen et du Conseil du 13 juin 2024 sur le devoir de vigilance des entreprises en matière de durabilité.

Directive (UE) 2025/794 du Parlement européen et du Conseil du 14 avril 2025 modifiant les directives (UE) 2022/2464 et (UE) 2024/1760 en ce qui concerne les dates à partir desquelles les États membres appliquent certaines exigences.

Directive (UE) 2026/470 du Parlement européen et du Conseil du 24 février 2026, JOUE L, 2026/470, 26 février 2026.

C. Recommandations, propositions et travaux préparatoires

Recommandation (UE) 2018/1149 de la Commission du 10 août 2018 relative aux lignes directrices non contraignantes pour l'identification des zones de conflit ou à haut risque et d'autres risques liés à la chaîne d'approvisionnement.

Recommandation (UE) 2024/2659 de la Commission du 11 octobre 2024 concernant des orientations pour l'exportation de biens de cybersurveillance au titre de l'article 5 du règlement (UE) 2021/821 du Parlement européen et du Conseil, JOUE L, 2024/2659, 16 octobre 2024.

Proposition de règlement du Parlement européen et du Conseil relatif à la sécurité, à la résilience et à la durabilité des activités spatiales dans l'Union, COM(2025) 335 final, 25 juin 2025.

DONAZZAN (E.), projet de rapport de la commission de l'industrie, de la recherche et de l'énergie du Parlement européen, PE784.432v01-00, 3 mars 2026.

D. Droit français

Code civil, article 1240.

Code de commerce, articles L. 225-102-4, L. 225-102-5 et L. 442-1.

Code monétaire et financier, articles L. 561-1 et suivants.

Code pénal, article 121-7.

Loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication.

Loi n° 2008-518 du 3 juin 2008 relative aux opérations spatiales, JORF n° 0129 du 4 juin 2008, notamment art. 4, 5 et 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.

Loi n° 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre.

Loi n° 2021-1729 du 22 décembre 2021 pour la confiance dans l'institution judiciaire, art. 56.

Loi n° 2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte.

II. Rapports et documents institutionnels

A. Nations unies

SOUS-COMMISSION DE LA PROMOTION ET DE LA PROTECTION DES DROITS DE L'HOMME, Normes sur la responsabilité en matière de droits de l'homme des sociétés transnationales et autres entreprises, E/CN.4/Sub.2/2003/12/Rev.2, 26 août 2003.

COMMISSION DES DROITS DE L'HOMME, décision 2004/116 du 20 avril 2004.

RUGGIE (J.), Protéger, respecter et réparer : un cadre pour les entreprises et les droits de l'homme, rapport du Représentant spécial du Secrétaire général, A/HRC/8/5, 7 avril 2008.

CONSEIL DES DROITS DE L'HOMME, résolution 17/4 du 16 juin 2011.

HAUT-COMMISSARIAT DES NATIONS UNIES AUX DROITS DE L'HOMME, *Principes directeurs relatifs aux entreprises et aux droits de l'homme : mise en œuvre du cadre de référence « protéger, respecter et réparer » des Nations unies*, Nations unies, New York et Genève, 2011.

HAUT-COMMISSARIAT DES NATIONS UNIES AUX DROITS DE L'HOMME, projet B-

Tech, *Applying the UN Guiding Principles on Business and Human Rights to Digital Technologies*, notes de cadrage, Genève, 2020 et suivantes.

GROUPE DE TRAVAIL DES NATIONS UNIES SUR LA QUESTION DES DROITS DE L'HOMME ET DES SOCIÉTÉS TRANSNATIONALES ET AUTRES ENTREPRISES, *Entreprises, droits de l'homme et régions touchées par un conflit : vers une action renforcée*, A/75/212, 21 juillet 2020.

HAUT-COMMISSARIAT DES NATIONS UNIES AUX DROITS DE L'HOMME, *Internet shutdowns : trends, causes, legal implications and impacts on a range of human rights*, A/HRC/50/55, 13 mai 2022.

PROGRAMME DES NATIONS UNIES POUR LE DÉVELOPPEMENT, *Heightened Human Rights Due Diligence for Business in Conflict-Affected Contexts : A Guide*, PNUD, New York, 2022.

B. Autres organisations internationales

COMITÉ INTERNATIONAL DE LA CROIX-ROUGE, *Guide interprétatif sur la notion de participation directe aux hostilités en droit international humanitaire*, CICR, Genève, 2009.

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, *Guide OCDE sur le devoir de diligence pour des chaînes d'approvisionnement responsables en minerais provenant de zones de conflit ou à haut risque*, 3e éd., Éditions OCDE, Paris, 2016.

GLOBAL NETWORK INITIATIVE, *Principles on Freedom of Expression and Privacy* et *Implementation Guidelines*, versions révisées le 20 mars 2017, consultées le 28 août 2026.

C. Autorités françaises et européennes

AGENCE FRANÇAISE ANTICORRUPTION, recommandations destinées à aider les personnes morales de droit public et de droit privé à prévenir et à détecter les faits de corruption, JORF, 12 janvier 2021.

MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES, réponse à la question écrite n° 3485 de M. Benjamin Haddad, « Eutelsat S.A. – Lutte contre la propagande russe », Assemblée nationale, XVIe législature, question publiée au Journal officiel du 29 novembre 2022, p. 5728, réponse publiée au Journal officiel du 3 janvier 2023, p. 96.

AUTORITÉ DE RÉGULATION DE LA COMMUNICATION AUDIOVISUELLE ET NUMÉRIQUE, mise en demeure du 14 décembre 2022.

COMMISSION EUROPÉENNE, « Commission takes next step to deploy the IRIS² secure satellite system », direction générale de l'industrie de la défense et de l'espace, 16 décembre 2024, relatif à la signature du contrat de concession IRIS² avec le consortium SpaceRISE.

MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA SOUVERAINETÉ INDUSTRIELLE, ÉNERGÉTIQUE ET NUMÉRIQUE, « Souveraineté industrielle et numérique : l'État devient le premier actionnaire d'Eutelsat », communiqué de presse n° 199, 12 décembre 2025.

AGENCE DE L'UNION EUROPÉENNE POUR LE PROGRAMME SPATIAL, « Commission accelerates IRIS² deployment with enhanced security and expanded satellites network », 7 août 2026, relatif à l'accord de mise en œuvre conclu entre la Commission européenne et le consortium SpaceRISE.

D. Documents d'entreprise et information réglementée

EUTELSAT COMMUNICATIONS, communiqué relatif à la cessation de la diffusion de certaines chaînes en Russie et en Iran, 21 décembre 2022.

EUTELSAT COMMUNICATIONS, Document d'enregistrement universel 2024-25, déposé auprès de l'Autorité des marchés financiers le 30 octobre 2025 sous le numéro D.25-0693, 404 p.

EUTELSAT COMMUNICATIONS, Amendement au document d'enregistrement universel 2024-25, déposé auprès de l'Autorité des marchés financiers le 24 novembre 2025.

EUTELSAT COMMUNICATIONS, Résultats annuels de l'exercice 2025-26, communiqué de presse, 7 août 2026.

SES S.A., Annual Report 2025, Luxembourg, 2026.

HISPASAT, Informe Anual 2025, Madrid, 2026.

VIASAT, INC., Annual Report on Form 10-K for the fiscal year ended March 31, 2026, déposé auprès de la Securities and Exchange Commission le 29 mai 2026.

III. Ouvrages généraux et manuels

BREEN (E.), GAUDEMET (A.), ROUSSILLE (M.) et RÉDACTION DES ÉDITIONS

FRANCIS LEFEBVRE, *Mémento Compliance 2025-2026*, coll. « Mémento pratique Francis Lefebvre », Éditions Francis Lefebvre, 2024, 1 188 p.

SUDRE (F.), *Droit européen et international des droits de l'homme*, 17e éd., PUF, coll. « Droit fondamental », Paris, 2025, 1 049 p.

BALMOND (L.), *Le droit international humanitaire*, 2e éd., Bréal, coll. « Lexifac Droit », 2025, 208 p.

ACHILLEAS (P.) (dir.), *Droit de l'espace : télécommunication, observation, navigation, défense, exploration*, Larcier, Bruxelles, 2009, 384 p.

IV. Ouvrages spéciaux, monographies et thèses

Collection « Régulations & Compliance », Journal of Regulation & Compliance (JoRC)

FRISON-ROCHE (M.-A.) (dir.), *Régulation, supervision, compliance*, Dalloz, Paris, 2017.

FRISON-ROCHE (M.-A.) (dir.), *Les outils de la Compliance*, coll. « Régulations & Compliance », Journal of Regulation & Compliance (JoRC) et Dalloz, Paris, 2021, 323 p.

FRISON-ROCHE (M.-A.) (dir.), *Les Buts Monumentaux de la Compliance*, coll. « Régulations & Compliance », Journal of Regulation & Compliance (JoRC) et Dalloz, Paris, 2022, 520 p.

FRISON-ROCHE (M.-A.) (dir.), *La juridictionnalisation de la Compliance*, coll. « Régulations & Compliance », Journal of Regulation & Compliance (JoRC) et Dalloz, Paris, 2023, 489 p.

FRISON-ROCHE (M.-A.) (dir.), *L'Obligation de Compliance*, coll. « Régulations & Compliance », Journal of Regulation & Compliance (JoRC) et Éditions Lefebvre-Dalloz, Paris, 2025, 816 p.

MONNERIE (N.), *La compliance. De son apparition américaine à son appréhension européenne*, coll. « Nouvelle Bibliothèque de Thèses », vol. 237, Dalloz, Paris, 2024, 420 p.

MAUBERNARD (C.) et BRÈS (A.) (dir.), *Le devoir de vigilance des entreprises : l'âge de la maturité ?*, coll. « Droit & économie », Bruylant, Bruxelles, 2024.

BEAUCILLON (C.) et GALLO (C.) (dir.), *Vigilance et diligence en droit public*, Bruylant, Bruxelles, 2025, 260 p.

CAILLET (M.-C.), *Le droit à l'épreuve de la responsabilité sociétale des entreprises : étude à partir des entreprises transnationales*, thèse de doctorat en droit, Université de Bordeaux,

2014, 663 p.

DONGAR (O.), *L'évolution de la finalité des activités spatiales : un défi pour le droit de l'espace*, Pedone, Paris, 2020.

ACHILLEAS (P.) et HOBE (S.) (dir.), *Fifty Years of Space Law – Cinquante ans de droit de l'espace*, Brill Nijhoff, Leyde et Boston, 2020, 890 p.

V. Articles, chroniques et presse

FRISON-ROCHE (M.-A.), « La dynamique des Buts Monumentaux du Droit de la Compliance », in FRISON-ROCHE (M.-A.) (dir.), *Les Buts Monumentaux de la Compliance*, préc., 2022, p. 1 à 19.

FRISON-ROCHE (M.-A.), « Les Buts Monumentaux, cœur battant du Droit de la Compliance », in FRISON-ROCHE (M.-A.) (dir.), *Les Buts Monumentaux de la Compliance*, préc., 2022, p. 21 à 44.

FRISON-ROCHE (M.-A.), « Concevoir l'Obligation de Compliance : faire usage de sa position pour participer à la réalisation des Buts Monumentaux de la Compliance », in FRISON-ROCHE (M.-A.) (dir.), *L'Obligation de Compliance*, préc., 2025, p. 3 à 44.

FRISON-ROCHE (M.-A.), « La Vigilance, pointe avancée et part totale de l'Obligation de Compliance », in FRISON-ROCHE (M.-A.) (dir.), *L'Obligation de Compliance*, préc., 2025, p. 511 à 536.

ROUAUD (A.-C.), « L'intensité de l'obligation de vigilance selon les secteurs : le cas des opérateurs financiers », in FRISON-ROCHE (M.-A.) (dir.), *L'Obligation de Compliance*, préc., 2025, p. 539 à 550.

FRANÇON (M.), « L'intensité du devoir de vigilance dans le secteur bancaire », in FRISON-ROCHE (M.-A.) (dir.), *L'Obligation de Compliance*, préc., 2025, p. 551 à 557.

LOISEAU (G.), « L'intensité de l'obligation de vigilance selon les secteurs : le cas des opérateurs numériques », in FRISON-ROCHE (M.-A.) (dir.), *L'Obligation de Compliance*, préc., 2025, p. 559 à 569.

LAMOUREUX (M.), « L'obligation de vigilance des opérateurs énergétiques », in FRISON-ROCHE (M.-A.) (dir.), *L'Obligation de Compliance*, préc., 2025, p. 571 à 585.

MEKKI (M.), « Peut-on repenser la responsabilité à l'aune du devoir de Vigilance, pointe avancée de la Compliance ? », in FRISON-ROCHE (M.-A.) (dir.), *L'Obligation de*

Compliance, préc., 2025, p. 599 à 615.

MICHON (C.), « Devoir de vigilance : les premiers arrêts de la chambre spécialisée », *Revue internationale de la compliance et de l'éthique des affaires*, n° 4, juillet 2024, commentaire n° 146.

ABADIE (P.) et LERAY (G.), « Après la forme, le fond ! Premiers enseignements relatifs au contrôle judiciaire du devoir de vigilance », *Revue des sociétés*, n° 6, juin 2024, p. 383 à 389.

DANIS-FATÔME (A.) et HOFFSCHIR (N.), « La loi sur le devoir de vigilance rendue ineffective par le juge », *Revue des sociétés*, n° 12, décembre 2023, p. 793.

LECOURT (A.), « Premières décisions au fond sur le devoir de vigilance : des précisions importantes et une ouverture », *RTD com.*, n° 3, 2024, p. 686.

IDA (N.), « Contrat et devoir de vigilance des sociétés », *JCP E*, n° 28, 13 juillet 2023, p. 17 à 26.

CORDIER (L.), « Les biens à double usage », *TVA Douane Environnement*, n° 2-2026, juin 2026, art. 02.8.

BALMFORTH (T.), « Ukraine says Starlink terminals used by Russia deactivated in blow to Moscow », Reuters, 5 février 2026.

ROULETTE (J.), BRYAN-LOW (C.) et BALMFORTH (T.), « Musk ordered shutdown of Starlink satellite service as Ukraine retook territory from Russia », Reuters, 25 juillet 2025.

VI. Sites internet

EUR-Lex, portail du droit de l'Union européenne, https://eur-lex.europa.eu.

Légifrance, service public de la diffusion du droit, https://www.legifrance.gouv.fr.

Conseil d'État, base de jurisprudence ArianeWeb, https://www.conseil-etat.fr/arianeweb.

Autorité de régulation de la communication audiovisuelle et numérique, https://www.arcom.fr.

Autorité des marchés financiers, base des documents d'enregistrement universel, https://www.amf-france.org.

Haut-Commissariat des Nations unies aux droits de l'homme, https://www.ohchr.org.

Programme des Nations unies pour le développement, https://www.undp.org.

Global Network Initiative, https://globalnetworkinitiative.org.

Business and Human Rights Resource Centre, https://www.business-humanrights.org.

Reporters sans frontières, https://rsf.org.

Commission européenne, programme IRIS², https://defence-industry-space.ec.europa.eu.

Eutelsat Group, espace investisseurs, https://www.eutelsat.com/investors.

Agence des participations de l'État, https://www.economie.gouv.fr/agence-participations-etat.

Journal of Regulation & Compliance, https://mafr.fr.

Toutes les ressources en ligne mentionnées ci-dessus ont été consultées le 28 août 2026.

VII. Jurisprudence

Par ordre chronologique inverse

Tribunal judiciaire de Paris, 25 juin 2026, n° RG 22/03403, Notre affaire à tous et autres c/ TotalEnergies SE ; appel annoncé par communiqué de la société du 27 juillet 2026.

Cour d'appel de Paris, pôle 5, chambre 12, 17 juin 2025, n° RG 24/05193, S.A. La Poste c/ Fédération SUD PTT.

Tribunal judiciaire de Paris, 5 décembre 2023, n° RG 21/15827, Sud PTT c/ La Poste.

Cour d'appel de Paris, chambre de l'instruction, 14 décembre 2022, affaire Nexa Technologies (volet égyptien) : annulation des mises en examen de la société et de quatre dirigeants et salariés pour complicité de tortures et de disparitions forcées, poursuite de l'information judiciaire.

Conseil d'État, ordonnance de référé, 9 décembre 2022, Association Reporters sans frontières, n° 468969.

Cour d'appel de Paris, chambre de l'instruction, 21 novembre 2022, affaire Amesys (volet libyen) : confirmation des mises en examen de la société et de ses dirigeants pour complicité d'actes de torture, annulation des mises en examen de deux salariés, poursuite de l'information judiciaire.

Conseil constitutionnel, décision n° 2017-750 DC du 23 mars 2017.

Tribunal pénal international pour l'ex-Yougoslavie, chambre d'appel, Le Procureur c/ Tadić, arrêt relatif à l'exception préjudicielle d'incompétence, 2 octobre 1995.

Annexes

Annexe n° 1. Échelle graduée de vigilance : matrice de qualification et de conséquences

Cette matrice constitue la formalisation opérationnelle de l'échelle proposée au § 14. Elle est conçue pour être insérée telle quelle dans une procédure interne. Les délais indiqués sont des ordres de grandeur, à ajuster selon la taille de l'opérateur et l'architecture de sa fonction conformité.

Critère	**Degré 0** **Contexte ordinaire**	**Degré 1** **Haut risque par défaillance**	**Degré 2** **Haut risque par maîtrise**	**Degré 3** **Conflit armé**
Nature du risque dominant	Risque résiduel de droit commun.	L'État ne contrôle plus le territoire ; l'atteinte vient d'acteurs non étatiques.	L'État contrôle le territoire et se sert du réseau contre sa population.	Deux parties au moins s'affrontent ; la capacité devient un enjeu militaire.
Problème posé à l'opérateur	Aucun problème spécifique.	Un problème de connaissance : savoir qui utilise réellement la capacité.	Un problème d'arbitrage : choisir entre obéir à l'État et protéger les usagers.	Un problème de qualification : déterminer si la capacité devient un objectif militaire.
Indices de basculement	Absence des indices ci-contre.	Effondrement de l'autorité, sanctions internationales, alerte d'une organisation internationale, présence d'un groupe armé.	Coupure ordonnée, demande de filtrage ou d'interception, restriction récurrente, condamnation par une juridiction régionale.	Franchissement des seuils du droit international humanitaire, mobilisation, revendication de la capacité par une partie.
Niveau de décision	Opérationnel.	Direction de la conformité.	Comité mixte conformité, juridique et direction générale.	Direction générale, information du conseil d'administration.
Diligence exigée	Diligence standard : connaissance du client, contrôle des sanctions.	Diligence renforcée sur l'identité de l'utilisateur final et la chaîne de revente.	Diligence renforcée sur la demande étatique : base légale, proportionnalité, voie de recours.	Diligence maximale : qualification du bien, effets sur les usagers civils, consultation externe.
Documentation obligatoire	Dossier client.	Note de qualification datée et motivée.	Note de qualification et dossier de décision complet (cf. annexe n° 2).	Dossier de décision, avis juridique externe, procès-verbal de l'organe ayant tranché.
Délai de réexamen	Annuel.	Semestriel.	Trimestriel, et à chaque nouvelle demande.	Mensuel, et à chaque évolution significative de la situation.

Annexe n° 2. Trame du dossier de décision de maintien ou de suspension

Support de la traçabilité de l'arbitrage décrite au § 24. Le dossier n'a pas pour objet d'établir que la décision était juste, mais qu'elle a été prise selon un processus identifiable, au vu d'éléments datés. Il est constitué au moment de la décision et non reconstitué après coup.

I. Identification

1. Référence interne du dossier, date et heure d'ouverture, auteur de la saisine.
2. Service, zone géographique et clients concernés ; volume de capacité en cause.
3. Degré de l'échelle retenu et référence de la note de qualification applicable.

II. Éléments déclencheurs

4. Nature de la demande ou du signalement : demande étatique, alerte interne, saisine d'un tiers, information publique.
5. Auteur de la demande, qualité invoquée, base légale citée, forme de la demande et date de réception.
6. Pièces reçues, avec mention de celles qui ont été refusées ou qui n'ont pas été produites.

III. Analyse

7. Droits susceptibles d'être affectés par le maintien du service, et par sa suspension.
8. Usagers civils identifiés partageant la même ressource, et conséquences prévisibles pour eux.
9. Appréciation de la base légale invoquée : existence, accessibilité, proportionnalité, voie de recours ouverte.
10. Options envisagées, de la moins à la plus radicale, et motif d'écartement de chacune.
11. Avis recueillis : direction juridique, direction de la conformité, conseil externe, le cas échéant partie prenante extérieure.

IV. Décision

12. Sens de la décision, organe qui l'a prise, date et heure, identité des personnes présentes.
13. Motivation, y compris les éléments qui n'ont pas emporté la conviction.
14. Mesures d'atténuation retenues au bénéfice des usagers civils.
15. Date du réexamen programmé et événements qui le déclencheraient par anticipation.

V. Suites

16. Information des organes sociaux et, le cas échéant, de l'autorité de tutelle.
17. Communication externe éventuelle et date.
18. Conservation : durée, support, personnes habilitées à consulter le dossier.

Annexe n° 3. Circuit de traitement d’une demande étatique de suspension

Application des § 23 et 27. Le tableau répond à la question qui traverse le mémoire : qui décide, à quel moment, et qui répond. Les délais courent à compter de la réception de la demande.

Étape	Déclencheur	Acteur compétent	Délai indicatif	Trace produite
1. Réception et horodatage	Toute demande de suspension, de filtrage ou de remise de données, quelle qu’en soit la forme.	Point de contact unique désigné.	Immédiat.	Accusé de réception et enregistrement au registre des demandes.
2. Vérification de recevabilité formelle	Demande enregistrée.	Direction juridique.	Quatre heures.	Fiche de recevabilité mentionnant la base légale invoquée.
3. Qualification du contexte	Demande recevable en la forme.	Direction de la conformité.	Douze heures.	Note de qualification indiquant le degré retenu.
4. Analyse d’incidence	Degré 1 ou supérieur.	Conformité, avec appui opérationnel.	Vingt-quatre heures.	Section III du dossier de décision.
5. Arbitrage	Analyse achevée.	Selon le degré : conformité, comité mixte ou direction générale.	Quarante-huit heures, réduites en cas d’urgence caractérisée.	Section IV du dossier de décision.
6. Exécution ou refus motivé	Décision rendue.	Direction des opérations.	Immédiat.	Ordre d’exécution horodaté et notification à l’auteur de la demande.
7. Information des organes sociaux	Décision de degré 3.	Direction générale.	Prochaine séance, ou sans délai si l’enjeu le justifie.	Procès-verbal.
8. Réexamen	Échéance programmée ou fait nouveau.	Organe ayant rendu la décision.	Selon l’annexe n° 1.	Note de réexamen versée au dossier.

Annexe n° 4. Connaissance de l’usage : déclaration, signaux d’alerte, clausier et mécanisme d’alerte

Outils opérationnels correspondant aux § 22, 25 et 26. Ils transposent au service satellitaire des mécanismes déjà éprouvés en matière de contrôle des exportations et de lutte contre le blanchiment.

I. Déclaration d’usage final : mentions à recueillir

1. Destination du service et finalité déclarée.
2. Catégories d’utilisateurs finals, y compris en cas de revente ou de mise à disposition d’un tiers.
3. Zone géographique effective d’exploitation, distincte de la zone de couverture technique.
4. Engagement de notifier toute modification substantielle de l’un de ces éléments.
5. Identité de l’intermédiaire éventuel et date de sa constitution.

II. Signaux d’alerte à définir par avance

6. Incohérence entre la capacité souscrite et l’activité déclarée.
7. Demande de faisceau couvrant une zone sans rapport avec l’implantation du client.
8. Recours à un intermédiaire nouvellement constitué ou dépourvu d’antériorité dans le secteur.
9. Refus de toute clause d’audit ou de vérification.
10. Exigence de confidentialité excédant les usages du marché.
11. Variation soudaine du volume souscrit dans un contexte qualifié au degré 1 ou supérieur.
12. Demande de désactivation de fonctions de journalisation ou de géolocalisation.

III. Familles de clauses contractuelles

13. Déclaration d’usage final : obligation de déclarer la destination et de signaler tout changement. Fonction probatoire et pénale plus qu’informative.
14. Vérification : droit d’audit documentaire, accès aux informations d’usage, faculté de demander des justificatifs en cas de signal d’alerte. Sans vérification, la déclaration n’est qu’une formalité.
15. Suspension graduée : mise en demeure, exigence d’engagements vérifiables, suspension partielle ciblée, non-renouvellement, résiliation. Chaque échelon doit être contractuellement disponible pour que l’opérateur ne soit pas réduit au choix entre tout maintenir et tout couper.
16. Traitement des demandes étatiques : obligation réciproque d’information, faculté de contester, engagement de transparence agrégée sur le volume et la nature des demandes reçues.
17. À écarter : les clauses miroir, qui répercutent l’obligation sur le cocontractant sans vérification ni conséquence effective. Elles allouent la responsabilité entre professionnels sans réduire le risque pour les personnes.

IV. Mécanisme d’alerte adapté aux contextes à haut risque

18. Accessibilité linguistique : canal disponible dans les langues des zones desservies, et non dans les seules langues de travail de l’entreprise.
19. Sécurité de l’alertant : un formulaire hébergé sur un site identifiable n’offre aucune protection lorsque l’alerte vise une demande de l’État où réside cette personne.
20. Médiation par des tiers de confiance : organisations humanitaires ou de défense de la liberté de l’information, habilitées à relayer une alerte.
21. Délai compatible avec l’objet : un accusé de réception sous trois mois n’a aucun sens lorsque l’atteinte est en cours. Prévoir une voie d’urgence.

Annexe n° 5. La chaîne d’usage : ce que l’opérateur sait, ce qu’il peut vérifier, où s’arrête son influence

Représentation de la chaîne décrite aux § 4, 22 et 29. Elle se lit de gauche à droite, dans le sens de la mise à disposition de la capacité. Le trait épais situé entre les colonnes 3 et 4 marque la frontière au-delà de laquelle l’opérateur ne dispose plus de lien contractuel direct : c’est là que la connaissance du client cesse d’opérer et que doit prendre le relais la connaissance de l’usage.

	1. Opérateur satellitaire	**2. Distributeur ou intégrateur**	**3. Client contractuel**	**4. Utilisateur final déclaré**	**5. Usage réel**
Lien juridique avec l’opérateur	Sans objet	Contrat de distribution	Contrat de fourniture de capacité	Mentionné dans la déclaration d’usage final, sans lien direct	Aucun
Ce que l’opérateur sait	Tout : ressource, faisceau, volume	Identité, antériorité, portefeuille	Identité, secteur déclaré, zone souscrite	Ce que le client a déclaré	Rien, sauf signal extérieur
Ce qu’il peut vérifier	Sans objet	Solvabilité, sanctions, antécédents publics	Cohérence entre capacité souscrite et activité déclarée	Rien directement ; par audit contractuel seulement	Rien
Levier dont il dispose	Total	Résiliation, non-renouvellement, restriction	Mise en demeure, suspension ciblée, résiliation	Aucun en propre ; passe par le client	Aucun
Nature de la diligence attendue	Gouvernance interne et qualification du contexte	Connaissance du client renforcée	Connaissance du client et déclaration d’usage	Connaissance de l’usage : signaux d’alerte et clausier	Réaction : hiérarchie des réponses
Degré à partir duquel la vigilance s’intensifie	Degré 1	Degré 1	Degré 1	Degré 2	Degré 2 et 3

Trois enseignements se lisent directement sur ce tableau. La connaissance décroît de gauche à droite tandis que le risque d’atteinte croît dans le même sens : l’opérateur en sait le moins là où l’enjeu est le plus fort. Le levier contractuel s’éteint à la colonne 4, alors que la diligence, elle, doit se poursuivre au-delà. Enfin, aucune colonne n’est vide dans la ligne relative à la diligence attendue : le fait que l’influence s’arrête ne signifie pas que l’obligation s’arrête, mais qu’elle change de nature, passant de la vérification à la réaction.

Annexe n° 6. Déploiement de l’échelle graduée dans l’entreprise : feuille de route

Prolongement opérationnel des § 13, 20 et 23. Cette feuille de route est indicative et générique : elle ne décrit le dispositif d’aucun opérateur déterminé. Le calendrier donne un ordre de grandeur, à ajuster selon la taille de l’opérateur. Une même fonction peut cumuler plusieurs rôles, pourvu que leur attribution soit écrite.

Étape	Contenu	Pilote	Calendrier indicatif	Livrable
1. Gouvernance	Désigner le responsable de l’échelle et le point de contact unique ; fixer par écrit le niveau de décision attaché à chaque degré.	Direction générale.	Mois 1.	Note d’organisation et délégations.
2. Qualification initiale	Classer chaque zone desservie du degré 0 au degré 3, à partir de sources publiques.	Conformité, sur avis des directions commerciale et technique.	Mois 1 à 3.	Notes de qualification datées et motivées.
3. Intégration aux procédures	Inscrire le degré dans la fiche client ; intégrer la déclaration d’usage final, les signaux d’alerte et le clausier aux modèles de contrat (cf. annexe n° 4).	Conformité, juridique et commercial.	Mois 3 à 6.	Procédures et modèles de contrat mis à jour.
4. Formation	Former chaque public à son rôle dans le circuit de décision (détail ci-dessous).	Conformité.	Mois 3 à 9, puis chaque année.	Supports et attestations de suivi.
5. Exercice de simulation	Dérouler en temps réel une demande étatique reçue de nuit et constituer le dossier de décision (cf. annexes n° 2 et 3).	Conformité, opérations et direction générale.	Mois 9, puis chaque année.	Compte rendu et plan de correction.
6. Suivi	Tenir un tableau de bord : contextes par degré, demandes reçues, délais de traitement, signaux relevés et suites données.	Conformité.	Chaque semestre.	Tableau de bord présenté aux organes sociaux.
7. Revue	Tirer le retour d’expérience de chaque décision de degré 2 ou 3 ; réviser l’échelle et les procédures.	Conformité et audit interne.	Chaque année.	Rapport de revue.

Détail de l’étape 4 : une formation propre à chaque public

a) Équipes commerciales : reconnaître les signaux d’alerte, recueillir la déclaration d’usage final, savoir à qui transmettre.

b) Centre de contrôle et opérations : ne jamais exécuter une demande d’interruption hors circuit, horodater toute demande, saisir le point de contact unique.

c) Directions juridique et de la conformité : qualifier le contexte, apprécier la base légale et la proportionnalité, tenir le dossier de décision.

d) Direction générale et administrateurs : arbitrer en connaissance des risques encourus (§ 32 à 34) et, au degré 3, des repères du droit international humanitaire (§ 16).

La formation des opérationnels est l’étape la plus accessible : elle ne suppose ni texte nouveau ni outil nouveau. Elle est aussi la plus déterminante, puisqu’une demande d’interruption parvient d’abord à ceux qui sont en mesure de l’exécuter (§ 23).

Table des matières

Introduction.....6

Partie 1. L'inadaptation du cadre ordinaire et les fondements d'une diligence renforcée et graduée.....12

Chapitre 1. Un cadre normatif conçu pour la chaîne d'approvisionnement, et moins pour une infrastructure critique.....12

Section 1. De l'engagement volontaire à l'obligation de moyens.....12

§ 1. Les Principes directeurs de 2011 et la structure de la diligence.....12

§ 2. La juridicisation française et son office judiciaire.....14

§ 3. L'européanisation et son reflux.....15

Section 2. L'angle mort des contextes à haut risque.....16

§ 4. Un droit de l'amont appliqué à un risque de l'aval.....16

§ 5. La catégorie existante : les zones de conflit ou à haut risque.....17

§ 6. L'inadaptation de cette catégorie aux services de communication.....18

§ 7. Le comblement par la soft law et ses limites.....20

Section 3. La démonstration empirique du vide.....20

§ 8. L'exclusion par les seuils : l'application chiffrée.....20

§ 9. Le reliquat : rendre compte sans avoir à se comporter.....22

§ 10. La carence institutionnelle : l'enseignement de l'affaire Arcom.....24

Chapitre 2. Les fondements d'une diligence renforcée et graduée.....25

Section 1. Le fondement tiré de la nature du service.....25

§ 11. La dualité structurelle de la capacité.....25

§ 12. La criticité : la privation comme atteinte.....26

§ 13. L'irréversibilité et la temporalité de la décision.....26

Section 2. Le fondement tiré du contexte : construction d'une échelle.....27

§ 14. Proposition d'une échelle graduée de vigilance.....27

§ 15. La gravité comme facteur d'intensification et son fondement en droit positif.....29

§ 16. Le degré supérieur : l'articulation avec le droit international humanitaire.....30

Section 3. Le fondement tiré du statut de l'opérateur.....31

§ 17. L'opérateur adossé à la puissance publique.....31

§ 18. Le rattachement par le droit spatial.....32

§ 19. La diligence renforcée comme contrepartie de la puissance conférée.....33

Partie 2. Le contenu opérationnel de la diligence graduée et ses tempéraments.....35

Chapitre 1. Le contenu : construire une diligence calibrée sur le degré du contexte...35

Section 1. L'évaluation contextualisée.....35

§ 20. La qualification préalable du contexte.....35

§ 21. La cartographie des risques appliquée à un portefeuille de capacité.....35

§ 22. Du Know Your Customer au Know Your Use.....36

Section 2. La gouvernance de la décision d'urgence.....37

§ 23. L'architecture décisionnelle de crise.....37

§ 24. La traçabilité de l'arbitrage : le dossier de décision comme objet juridique.....37

§ 25. Le mécanisme d'alerte calibré sur le contexte.....38

Section 3. Les leviers d'action et leur mise en œuvre.....38

§ 26. L'outillage contractuel.....38

§ 27. La réponse aux demandes étatiques.....39

§ 28. La sortie responsable.....40

Chapitre 2. Les tempéraments : la mesure juste de la responsabilité.....41

Section 1. Le refus du garant universel.....41

§ 29. L'influence limitée et sa portée juridique.....41

§ 30. La fausse déclaration du client.....41

§ 31. Entre responsabilité diluée et obligation paralysante....42
Section 2. La cartographie des risques encourus par l'opérateur....43
§ 32. Le risque pénal et ses qualifications....43
§ 33. Le risque civil après le renvoi aux droits nationaux....44
§ 34. Le risque réputationnel, actionnarial et de financement....45
Section 3. Combler le vide : quatre voies....46
§ 35. La voie sectorielle spatiale....46
§ 36. La voie du contrôle des exportations....47
§ 37. La voie de la qualification officielle du contexte....48
§ 38. La désignation d'une autorité compétente....48
Conclusion....49
§ 39. Un vide qui tient à l'architecture....49
§ 40. Fonder l'exigence, désigner celui qui décide....49
Bibliographie....51
Annexes.... 60