

Journal du Droit Transnational



Directeurs:
Ilias Bantekas
Catherine Maia
Tarcisio Gazzini
Francesco Seatzu

www.journaldudroittransnational.it

LE DEVOIR DE VIGILANCE NUMÉRIQUE LIÉ AUX COUPURES D'INTERNET POUR DES MOTIFS POLITIQUES: RÉFLEXIONS À PARTIR DU CAS DU GROUPE VIVENDI.

Bamidayé Komi Assogba

Résumé

Les coupures d'internet ordonnées pour des motifs politiques constituent désormais une pratique récurrente dans plusieurs régions du monde, notamment en Afrique de l'Ouest. Si la responsabilité des États au regard des instruments internationaux de protection des droits de l'homme est relativement bien identifiée, celle des entreprises numériques participant matériellement à ces restrictions demeure plus incertaine. À partir du cas du Groupe Vivendi et de ses activités de fourniture d'accès à internet en Afrique, le présent article interroge l'existence d'un devoir de vigilance numérique applicable aux fournisseurs d'accès à internet (FAI) et aux opérateurs de réseaux mobiles (ORM) confrontés à des demandes étatiques de coupure d'internet.

L'étude met en évidence l'existence d'un risque identifiable d'atteinte aux droits de l'homme lié aux coupures d'internet, à travers l'articulation entre les obligations internationales des États, les standards de diligence raisonnable applicables aux entreprises multinationales et les dynamiques contentieuses récentes. Après avoir analysé les fondements théoriques de ce risque, l'article examine les évolutions normatives internationales, régionales et privées relatives au droit d'accès à internet et à la responsabilité des entreprises numériques. Il montre ensuite que la jurisprudence de la Cour de justice de la CEDEAO contribue à structurer un véritable cadre de protection juridictionnelle contre les coupures d'internet, en consacrant progressivement un droit d'accès au réseau dérivé de la liberté d'expression.

L'article soutient que, sans consacrer encore une obligation autonome et pleinement stabilisée imposant aux entreprises de prévenir les coupures d'internet, les dynamiques normatives et jurisprudentielles actuelles suffisent néanmoins à objectiver un risque juridique sérieux que les entreprises soumises à la loi française sur le devoir de vigilance ne peuvent ignorer.

Mots clés

Devoir de vigilance – vigilance numérique – coupures d'internet – droits de l'homme – liberté d'expression – droit d'accès à internet – entreprises multinationales – diligence raisonnable.

Depuis 2011, année où les autorités égyptiennes y ont recouru pour la première fois¹, les coupures d'internet ou les restrictions d'accès à certains sites ou application sont devenues des pratiques récurrentes dans de nombreux États². Ces mesures visent

¹ *Internet Shutdowns*, An Internet Society Public Policy Briefing, Décembre 2029, p. 2.

² En 2024, on a recensé 296 restrictions d'accès à internet dans 54 pays, voir les statistiques sur le site de l'un des organismes dédiés à ces questions, <https://www.accessnow.org/campaign/keepiton/>, consulté le 27 octobre 2025.

généralement à contrôler l'opinion publique et à ralentir, voire paralyser, les manifestations citoyennes hostiles aux autorités publiques. Au début de l'année 2025, les dernières évolutions du conflit armé dans l'est de la République Démocratique du Congo ont conduit les autorités à restreindre l'accès à certains réseaux sociaux, notamment X et TikTok, dans le but affiché de lutter contre la désinformation³. De même, à partir du 26 juin 2025, des restrictions d'accès à internet ont été observées au Togo, dans le contexte des manifestations politiques contre les autorités en place⁴. Le Togo s'était déjà illustré en 2017 par des coupures d'internet pour les mêmes motifs, qui ont conduit à une décision de la Cour de justice de la Communauté économique des États de l'Afrique de l'Ouest, notamment l'arrêt *Amnesty International Togo & Others c. République togolaise*⁵.

Partant de cette dernière occurrence, la présente étude vise à éclairer la responsabilité des entreprises dans le cadre des coupures d'internet motivées par des considérations politiques à la lumière du devoir de vigilance des entreprises, qui est une notion émergente en droit international dans le sillage de la loi française sur le devoir de vigilance, à laquelle est soumise précisément l'une des entreprises numériques actives au Togo, le Groupe Vivendi. Ce dernier y commercialise le service d'accès à Internet sous la marque CanalBox à travers sa filiale Groupe Vivendi Africa (GVA)⁶.

Dans le contexte international de responsabilisation accrue des entreprises en matière de droits de l'homme, la loi française du 27 mars 2017 relative au devoir de vigilance des sociétés mères et entreprises donneuses d'ordre⁷ apparaît comme un phare. Cette loi impose aux grandes entreprises d'élaborer, publier et mettre en œuvre un plan de vigilance visant à identifier et prévenir les risques d'atteintes aux droits humains, à l'environnement, à la santé et à la sécurité dans l'ensemble de leur chaîne de valeur. Elle revêt, à cet égard, une dimension extraterritoriale, le législateur n'ayant pas entendu limiter le périmètre du plan aux seules entités de la chaîne localisées sur le territoire français. Aussi, depuis 2024, la directive européenne sur le devoir de vigilance des

³ « RDC: X et TikTok suspendus pour lutter contre la propagation de fausses nouvelles sur la situation dans l'Est du pays », en ligne <https://www.business-humanrights.org/fr/latest-news/rdc-x-et-tiktok-suspendus-dans-plusieurs-villes-congolaises-pour-lutter-contre-la-propagation-de-fausses-nouvelles-sur-la-situation-dans-lest-du-pays/>, consulté le 06 novembre 2025.

⁴ Chapitre Togolais de l'Internet Society, *Rapport technique sur les perturbations de l'accès à l'internet au Togo* (juin-juillet 2025), en ligne, <https://internetsociety.tg/2025/07/04/rapport-technique-sur-les-perturbations-de-lacces-a-internet-au-togo-juin-juillet-2025/>, consulté le 06 novembre 2025.

⁵ Cour de justice de la CEDEAO, arrêt du 25 juin 2020, *Amnesty International Togo & Others c. République togolaise* (N° ECW/CCJ/JUD/09/20).

⁶ Arrêté n°015 du 7 juin 2017 portant attribution de licence de fournisseur d'accès Internet (FAI) à la société GVA Togo.

⁷ Loi n° 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre ; Lucas D'AMBROSIO, « Le devoir de vigilance : une innovation juridique entre continuités et ruptures », *Droit et société*, 2020, pp. 633-647 ; Guillaume DELALIEUX, « La loi sur le devoir de vigilance des sociétés multinationales : parcours d'une loi improbable », *Droits et société*, 2019, pp. 649-665 ; Béatrice PARANCE, Elise GROULX, Victoire CHATELIN, « Regards croisés sur le devoir de vigilance et *duty of care* », *Journal du droit international*, 2018, pp. 21-52.

entreprises en matière de durabilité⁸ impose une obligation sensiblement similaire à certaines grandes entreprises européennes, ainsi qu'à certaines entreprises étrangères réalisant un chiffre d'affaires significatif dans l'Union européenne. Enfin, à l'initiative du Conseil des droits de l'homme, et depuis l'adoption de la résolution 26/9 en 2014, le projet d'instrument juridiquement contraignant visant à réglementer, dans le cadre du droit international des droits de l'homme, les activités des sociétés transnationales et autres entreprises envisage, au stade de son troisième projet révisé, d'instaurer une obligation de diligence raisonnable comparable pour les entreprises, exclusivement en matière de droits de l'homme⁹.

Ces dynamiques témoignent de l'ancrage progressif du devoir de vigilance ou de la diligence raisonnable dans l'ordre juridique international comme socle normatif de la responsabilité des entreprises¹⁰. La réception de la notion en doctrine a donné lieu à sa traduction en « *devoir de vigilance numérique* »¹¹, principalement envisagé sous l'angle des pollutions générées par les activités numériques des entreprises, qu'il s'agisse de la multiplication des infrastructures et équipements ou d'une consommation accrue d'énergie¹².

L'hypothèse défendue ici est que ce devoir de vigilance s'étend à d'autres risques numériques liés au développement des technologies de l'information et de la communication¹³. On songe, entre autres, à la privatisation de la liberté d'expression, l'amplification de la désinformation et des discours de haine, la modération biaisée ou insuffisante des contenus, la manipulation de l'opinion dans les contextes électoraux, ou encore l'automatisation opaque et discriminatoire de la diffusion de l'information¹⁴. Ces phénomènes représentent une menace pour la démocratie et pour des droits fondamentaux, notamment la liberté d'opinion et d'expression, le droit de participer à la vie publique, le droit à l'égalité et à la non-discrimination, ainsi que le droit au respect de

⁸ Directive (UE) 2024/1760 du Parlement européen et Conseil du 13 juin 2024 sur le devoir de vigilance des entreprises en matière de durabilité et modifiant la directive (UE) 2019/1937 et le règlement (UE) 2023/2859.

⁹ Anicet Rodrigue TAYO, « Le devoir de vigilance des entreprises dans les instruments juridiques africains », *Revue québécoise de droit international*, 2022, vol. 35, n° 2, pp. 94 et s.

¹⁰ Voir Rapport sur la neuvième session du Groupe de travail intergouvernemental à composition non limitée sur les sociétés transnationales et autres entreprises et les droits de l'homme, 26 décembre 2023, A/HRC/55/59.

¹¹ Caroline DEVAUX et Jean-Philippe NICOLAÏ, « vers un devoir de vigilance numérique (ou comment intégrer le problème de la pollution numérique dans la gouvernance des entreprises) », *Revue interdisciplinaire droit et organisations*, 2022, n°4, pp.13-32.

¹² *Ibid.*, p. 15.

¹³ Suzanne LEQUETTE, *op. cit.*, p. 33 ; Catherine PREBISSY-SCHNALL et Éric PEZET, « Faire évoluer le droit en fonction du risque numérique », *Cahiers Droit, Sciences & Technologies*, 2025, n°20, pp. 29-39.

¹⁴ Rapport de la Rapporteuse spéciale sur la promotion et la protection du droit à la liberté d'opinion et d'expression, *La liberté d'expression dans le contexte des élections à l'ère du numérique*, 11 juin 2025, A/HRC/59/50 ; Rapport de la Rapporteuse spéciale sur la promotion et la protection du droit à la liberté d'opinion et d'expression, *Menaces sur la liberté d'expression en ligne en temps de troubles*, 18 août 2025, A/80/341.

la vie privée¹⁵. Ils résultent de comportements problématiques imputables aux entreprises, tels que la modération des contenus, le traitement des informations sensibles, ou encore les coupures d'internet pour des motifs politiques, ces dernières constituant le point d'attention de la présente étude.

Internet recouvre une réalité protéiforme allant des couches fondamentales du réseau (les infrastructures physiques sous-tendant le réseau, l'intelligence du réseau permettant la communication entre les différents points du réseau) aux couches d'application du réseau comme le web¹⁶. Selon une définition classique, Internet est « *réseau télématique international, qui résulte de l'interconnexion des ordinateurs du monde entier utilisant un protocole commun d'échanges de données (baptisé TCP/IP ou Transport Control Protocol/Internet Protocol et spécifié par l'Internet Society, ou ISOC) afin de dialoguer entre eux via les lignes de télécommunication (lignes téléphoniques, liaisons numériques, câble)* »¹⁷. Ses usagers y ont accès par l'intermédiaire des fournisseurs d'accès à Internet (FAI) et, par extension, des opérateurs de réseaux mobiles (ORM). Il s'agit de prestataires techniques, qui offrent « *à leurs clients la possibilité de se connecter au réseau internet, en contrepartie d'un prix déterminé* »¹⁸.

Cette configuration permet de mieux saisir la portée des coupures d'Internet, définies comme une interruption intentionnelle des communications en ligne, rendant celles-ci inaccessibles ou inutilisables pour une population ou un territoire donné, souvent dans le but de contrôler le flux d'informations¹⁹. Plus précisément, on entend par « *coupures d'internet* », dans le cadre de cette étude, les restrictions ou limitations d'accès au réseau intervenant à la suite de « *mesures prises par un gouvernement, ou au nom d'un gouvernement* »²⁰, dans un but politique. Elles se distinguent des restrictions d'accès à certains contenus, ordonnées par un juge, conformément à la loi, à la demande de toute personne intéressée, par exemple pour prévenir ou faire cesser un dommage. Tel est également le cas, en France, des mesures destinées à faire cesser la diffusion illicite d'un événement sportif en ligne ou la circulation de fausses informations²¹.

Les coupures d'internet peuvent être mises en œuvre par divers procédés: blocage complet de la connexion, censures de certains mots-clés sur les moteurs de recherche, filtrage des sites contenant certains mots-clés, limitation de la bande passante, restrictions des services mobiles, ou encore manipulation du Domain Name System

¹⁵ Suzanne LEQUETTE, *op.cit.*, p. 33 ; Joël ANDRIANTSIMBAZOVINA, « Convention européenne des Droits de l'Homme », *Annuaire international de justice constitutionnelle*, 37-2021, 2022, p. 272 ; Nina LE BONNIEC, « La Cour européenne des droits de l'homme face aux nouvelles technologies de l'information et de communication numériques », *RDLF*, 2018, chr. n° 5., pp. 2-3.

¹⁶ Voir Suzanne LEQUETTE, *Droit du numérique*, Paris, LGDJ, Lextenso, 2024, pp. 61. et s.

¹⁷ *Dictionnaire Le Larousse*, en ligne, consulté le 13 novembre 2025.

¹⁸ Vincent FAUCHOUX, Pierre DEPREZ, Jean-Michel BRUGUIERE, *Le droit de l'internet*, 2^e éd, Paris, Lexisnexis, 2013, p. 379.

¹⁹ *Internet Shutdowns*, An Internet Society Public Policy Briefing, *op. cit.*, p. 1.

²⁰ *Coupures de l'accès à Internet : tendances, causes, implications juridiques et conséquences sur une série de droits de l'homme*, Rapport du Haut-Commissariat des Nations Unies aux droits de l'homme, 13 mai 2022, A/HRC/50/55, p. 2.

²¹ Emmanuel DREYER, *Droit de la communication*, Paris, LexisNexis, 2022, pp. 400 et s.

(DNS) consistant à rediriger les requêtes de noms de domaine vers des pages d'erreur ou des adresses bloquées²².

Quelle que soit la technique employée, Internet est devenu, depuis les années 1990, un instrument central de l'action collective²³. Il sert à diffuser des informations, coordonner des protestations, signer des pétitions ou encore mobiliser les citoyens, en complément ou en substitution des moyens traditionnels. Alors indispensable pour la mise en œuvre des droits garantis par la Charte internationale des droits de l'homme²⁴, Internet constitue ainsi un canal essentiel de l'exercice de la liberté d'expression.

Rappelons que le droit à la liberté d'expression est consacré par plusieurs instruments internationaux, dont l'article 19 §2 du Pacte international relatif aux droits civils et politiques (PIDCP). Ce droit occupe une place centrale dans la théorie des droits fondamentaux, parce qu'il est un pilier essentiel de la société démocratique²⁵. Pouvant toutefois entrer en conflit avec d'autres droits, tels que le droit à la vie privée, ou avec la protection de l'ordre public, il est admis que des restrictions lui soient apportées. S'ouvrent en conséquence des débats sur les limites légitimes à la liberté d'expression²⁶, lesquelles limites peuvent hypothétiquement couvrir ou justifier les coupures d'internet.

Il reste que la question doit faire l'objet d'une analyse sérieuse, d'autant plus que les coupures d'internet mettent en cause indirectement d'autres droits de l'homme comme la liberté de manifestation ou la liberté de réunion et d'associations pacifiques. Il convient de relever à cet égard que la liberté de manifestation trouve son ancrage en droit international des droits de l'homme à travers la liberté de réunion et d'associations pacifiques et la liberté d'expression²⁷. Quant à la liberté de réunion et d'association pacifiques, quand bien même elle est expressément revêtue d'une portée juridique

²² Olivier ALAIS, Erik DA SILVA, Gabriel FONLLADOSA, *Rapport sur les libertés numériques dans les pays francophones d'Afrique*, Paris, AFD, 2023, p. 4 ; *Coupures de l'accès à Internet : tendances, causes, implications juridiques et conséquences sur une série de droits de l'homme*, *ibid.*, p. 3 ; Christianne FERAL-SCHUHL, *Cyberdroit, Le droit à l'épreuve d'internet*, 8^e éd., Dalloz, Paris, 2020, p. 1527.

²³ Jean-Samuel BEUSCART, Sylvain PARASIE, *Sociologie d'internet*, Malakof, Armand Colin, 2016, pp. 106 et s.

²⁴ David TOURNIER, « Quand la toile porte l'étoile : internet au service de la charte internationale des droits de l'homme ? », *Revue québécoise de droit international*, 2005, vol 18, n°2, pp. 187-211.

²⁵ Charles GIRARD, « La liberté d'expression est-elle un droit absolu ? », *Revue de métaphysique et de morale*, 2022/4, N° 116, pp. 477-495 ; Michel HOTELLIER, Eleanor MCGREGOR, « La liberté d'expression : regards croisés sur ses sources, son contenu et ses fonctions », *Cahiers de la recherche sur les droits fondamentaux*, 2010, pp. 11-26.

²⁶ Xavier BIOY, « La protection renforcée de la liberté d'expression politique dans le contexte de la Convention européenne des droits de l'homme », *Les Cahiers de droit*, 2012, 53(4), pp. 739-760 ; David RIVIERE, « Les rapports entre liberté politique et liberté d'expression. Enjeu de l'introduction du principe de proportionnalité dans la mise en œuvre de l'ordre public immatériel », *Droit et société*, 2016/3, n° 94, pp. 581-602.

²⁷ Julie FERRERO, « La liberté de manifestation en droit international : illustration des limites de l'emprise du droit international sur les pratiques nationales », *Jus Politico : revue de droit politique*, 2017, n° 17, pp. 545-566.

contraignante à travers l'article 21 du PIDCP²⁸, elle est aussi généralement couplée à la liberté d'expression.

En tout état de cause, visant à garantir la participation pacifique des citoyens à la vie publique, la jouissance de ces libertés est menacée par les coupures d'Internet, ce qui engage non seulement la responsabilité des États, mais également celle des acteurs privés impliqués. En effet, les fournisseurs d'accès à internet (ci-après FAI) et des opérateurs de réseaux mobiles (ci-après ORM) jouent un rôle déterminant dans la mise en œuvre effective des coupures²⁹, qu'elles soient ordonnées par les autorités publiques, décidées par les juridictions, ou exécutées sur une base volontaire³⁰.

Dans ces conditions, l'étude s'attache à déterminer si le Groupe vivendi et, par extension, des entreprises françaises du secteur numérique, est tenue à un devoir de vigilance spécifique face au risque d'atteinte aux droits de l'homme découlant des coupures d'Internet à motivation politique. Cela revient à se demander si les coupures d'internet engendrent un risque d'atteinte aux droits de l'homme que les entreprises soumises à la loi sur le devoir de vigilance doivent prendre en compte.

L'analyse de cette question présente un intérêt théorique quant à la coexistence des obligations respectives des entreprises et des États en matière de droits de l'homme. Sur le plan pratique, elle invite également à examiner l'articulation des obligations d'une société mère avec celles de sa filiale locale.

En dépit de l'importance de la question cristallisée par ces intérêts identifiés, force est de constater que les entreprises sont globalement frileuses pour prendre en considération le risque associé aux coupures d'Internet, à l'exception de quelques-unes³¹. Ce risque s'accroît pourtant inexorablement du fait de l'emprise des technologies de l'information sur les sociétés, qui renforce la centralité du numérique dans l'exercice des libertés publiques, au point où il ne serait pas superfétatoire de soutenir l'émergence d'un droit d'accès à internet. Ce phénomène socio-juridique s'inscrit en décalage avec le retour de l'autoritarisme dans de nombreux pays. La mobilisation politique accrue de la « *génération Z* »³², dont les actions ont récemment contribué à des renversements de

²⁸ Sur les droits de l'homme potentiellement en jeu dans le cadre du développement des technologies numériques, voir Joël ANDRIANTSIMBAZOVINA, *op. cit.*, p. 272 ; Nina LE BONNIEC, *op. cit.*, pp. 2-3.

²⁹ *Coupures de l'accès à Internet : tendances, causes, implications juridiques et conséquences sur une série de droits de l'homme*, Rapport du Haut-Commissariat des Nations Unies aux droits de l'homme, 13 mai 2022, A/HRC/50/55, p. 13.

³⁰ Voir CommDH/IssuePaper, *La prééminence du droit sur internet et dans le monde numérique en général*, (2014)1.

³¹ Parmi les 11 entreprises évaluées dans le cadre d'initiative d'entreprises prenant en compte ce risque, on remarquera qu'Orange, société française probablement soumise à la loi sur le devoir de vigilance, traite des risques d'atteinte à la liberté d'expression dans son plan de vigilance, voir notamment le rapport de l'évaluation indépendante du Global Network Initiative du 23 octobre 2023 couvrant le cycle 2021/2022, en ligne, https://globalnetworkinitiative.org/wp-content/uploads/GNI_PAR23_102023_casestudies.pdf, consulté le 10 novembre 2025.

³² L'expression désigne l'individu hypermoderne en constante adaptation et évolution. La technologie est considérée comme une part entière de sa personne, voir Frederic TORDO, « Génération Z », in Pauline ESCANDE-GAUQUIE, Bertrand NAIVIN (coord.), *Comprendre la culture numérique*, Malakoff, Dunos, 2029, pp. 216-220.

gouvernement au Bangladesh, au Sri Lanka et à Madagascar, en constitue une illustration éloquente. A cet égard, le risque d'atteinte aux droits de l'homme du fait des coupures d'internet est aujourd'hui indéniablement d'actualité.

Pour appréhender ce risque, au-delà des considérations théoriques (I), deux approches de la vigilance peuvent être convoquées. Celles-ci consistent soit à s'appuyer sur une qualification juridique de la situation déjà effectuée par des juridictions ou législateurs, ce qui suppose une veille réglementaire et jurisprudentielle active, soit à procéder à un repérage rigoureux des « *situations nouvelles et un effort pour décrire et nommer le risque engendré* »³³. Les deux formes de vigilance, loin d'être exclusives, se complètent et convergent pour confirmer la réalité d'un risque numérique lié aux coupures d'Internet à motivation politique. Plus précisément, à travers les dynamiques normatives (II) et jurisprudentielles (III) mises en évidence par la présente étude, l'on peut identifier les linéaments d'un droit d'accès à internet, droit menacé à la fois par le comportement direct des acteurs politiques et par le comportement indirect des entreprises.

I-) LES FONDEMENTS THEORIQUES DU RISQUE D'ATTEINTE AU DROIT D'ACCÈS A INTERNET

L'ordre juridique international ne disposant pas de mécanismes efficaces pour sanctionner la violation des normes qu'il édicte, leur mise en œuvre repose largement sur des dispositifs internes faisant office de normes secondaires³⁴. Cette articulation révèle toutefois un risque structurel : celui de voir ces mécanismes internes se révéler inopérants ou insuffisants, laissant ainsi certaines violations du droit international dépourvues de sanction effective.

L'analyse du risque d'atteinte aux droits de l'homme lié aux coupures d'Internet doit, dans cette perspective, distinguer le droit positif applicable des évolutions normatives en cours, issues notamment de la *soft law* et des dynamiques jurisprudentielles. En l'absence de dispositions internes contraignant les destinataires des normes internationales à agir ou à s'abstenir, des atteintes aux droits de l'homme peuvent en effet demeurer sans sanction (A).

Ce risque est d'autant plus marqué que les États d'accueil peinent souvent à répondre aux attentes des victimes de violations commises par des entreprises multinationales. C'est précisément pour pallier ces lacunes inhérentes à la mondialisation³⁵ que les législations

³³ Catherine PREBISSY-SCHNALL et Éric PEZET, « Faire évoluer le droit en fonction du risque numérique », *op. cit.*, p. 29.

³⁴ Y. KERBRAT, « La responsabilité des entreprises peut-elle être engagée pour violation du droit international ? », in: (Dir) H. GHERARI et Y. KERBRAT, *L'entreprise dans la société internationale* (colloque des 11 et 12 décembre 2008), A. PEDONE, 2010, pp. 98-99; Bamidayé Komi ASSOGBA, « L'extraterritorialité comme outil de politique extérieure », in H. BUXBAUM, T. FLEURY GRAFF (dir.), *Extraterritoriality*, The Hague Academy of International Law, Brill Nijhoff, 2022, p. 265.

³⁵ Mahmood BAGHERI, Mohammad Jafar GHANBARI, « Globalization and extraterritorial application of economic regulation: crisis in international law and balancing interests », *European Journal of Law and Economics*, 2016, pp. 393-429.

de type « devoir de vigilance » ont été adoptées, en ouvrant aux victimes un accès à la justice dans l'État d'origine des entreprises.

Dans ce cadre, l'articulation entre responsabilité locale et responsabilité délocalisée des entreprises multinationales apparaît elle-même comme une source autonome de risque, notamment dans les situations de coupures d'Internet (B).

A-) LA COMPLEMENTARITE NECESSAIRE ENTRE DROIT INTERNE ET INTERNATIONAL

En droit international des droits de l'homme, les responsabilités étatiques et des acteurs privés sont étroitement imbriquées. En effet, les obligations des entreprises se définissent à la lumière de celles des États, lesquels peuvent être tenus responsables des violations commises par des acteurs privés relevant de leur juridiction ou de leur contrôle³⁶. Toutefois, en raison du caractère largement statocentrique du système international de protection des droits de l'homme³⁷, les mécanismes existants ne permettent de sanctionner que des États, y compris lorsque la violation résulte du comportement d'entreprises privées³⁸.

Il en découle que, dans le contexte des coupures d'Internet, seule la responsabilité de l'État peut être recherchée dans le cadre de ces mécanismes. Ceux-ci ne permettent donc pas, en l'état du droit positif, de mettre directement en cause les entreprises impliquées, notamment les fournisseurs d'accès à Internet (FAI) et les opérateurs de réseaux mobiles (ORM).

C'est précisément pour pallier cette limite que le troisième pilier des Principes directeurs des Nations unies relatifs aux entreprises et aux droits de l'homme (Principes de Ruggie) est consacré à l'accès aux voies de recours. Ce pilier invite les États à prévoir des mécanismes judiciaires et non judiciaires accessibles aux victimes de violations imputables aux entreprises. Toutefois, ces principes, en tant qu'instruments de *soft law*, ne créent pas en eux-mêmes d'obligations juridiquement contraignantes. Ils produisent néanmoins des effets normatifs indirects, en structurant les attentes à l'égard des entreprises et en influençant les pratiques ainsi que l'interprétation juridictionnelle.

Dans cette perspective, la loi française de 2017 relative au devoir de vigilance s'inscrit dans le prolongement de ces recommandations. Elle confirme, dans une certaine mesure,

³⁶ R. McCORQUODALE, P. SIMONS, « Responsibility beyond Borders: State responsibility for extraterritorial violations by corporations of international human right Law », *Modern Law Review* 2007, pp. 598-625 ; O. De SCHUTTER, « La responsabilité des États dans le contrôle des sociétés transnationales : vers une convention internationale sur la lutte contre les atteintes aux droits de l'homme commises par les sociétés transnationales », in E. DECAUX (dir.), *La responsabilité des entreprises multinationales en matière de droits de l'homme*, Bruxelles, Bruylant, 2010, pp. 20-100.

³⁷ Ludovic HENNEBEL, Hélène TIGROUDJA, *Traité de droit international des droits de l'homme*, Paris, A. Pedone, 2016, pp. 79 et s.

³⁸ Voir par exemple Commission africaine des droits de l'homme et des peuples, *Institute for Human Rights and Development in Africa et autres c. République Démocratique du Congo*, Communication n° 393/10, 20^{ème} Session extraordinaire, du 9 au 18 juin 2016.

l'effet horizontal des droits de l'homme à l'égard des entreprises multinationales³⁹. Toutefois, elle n'explicite pas de manière exhaustive les droits directement opposables aux entreprises. Il convient dès lors de distinguer l'obligation des États de protéger les droits de l'homme de l'obligation, distincte dans sa portée, des entreprises de respecter ces droits, telle que cela ressort des Principes de Ruggie⁴⁰.

La jurisprudence régionale, notamment celle de la Commission africaine des droits de l'homme et des peuples issue de *l'affaire SERAC*⁴¹, confirme cette dualité en soulignant la différence de teneur entre les obligations imposées aux États et celles pesant sur les entreprises. Ces dernières sont tenues, *a minima*, d'une obligation de diligence raisonnable. Cette obligation, au cœur des Principes de Ruggie comme d'autres instruments relatifs à la responsabilité des entreprises⁴², présente une proximité conceptuelle avec le devoir de vigilance⁴³.

Les droits de l'homme opposables aux entreprises au titre de la loi de 2017 ne diffèrent donc pas, en tant que tels, de ceux opposables aux États, même si la gradation de leurs obligations respectives est distincte. En conséquence, l'identification d'obligations pour les États en matière de coupures d'internet devra entraîner, dans une certaine mesure, l'opposabilité de ces obligations aux entreprises.

Les Principes de Ruggie apportent en outre une précision importante quant au contenu des droits matériels concernés. Ils visent les droits internationalement reconnus, notamment ceux figurant dans la Charte internationale des droits de l'homme constituée des deux pactes de 1966 ainsi que la Déclaration universelle des droits de l'homme (DUDH). Dès lors, s'il est démontré que les coupures d'Internet affectent des droits protégés par cette Charte, il est possible de soutenir que les entreprises doivent, dans le cadre de leur obligation de vigilance, prendre en compte les risques correspondants.

Il reste toutefois que, en l'état du droit positif, la mise en cause des entreprises pour de telles atteintes ne peut intervenir que par l'intermédiaire de mécanismes internes. Or, lorsque ces mécanismes relèvent du droit de l'État à l'origine des coupures, leur effectivité apparaît incertaine.

³⁹ Voir Observation n° 31 (Doc. ONU HRI/GEN/1Rev. 7 (2004), §8; Y. KERBRAT, « La responsabilité des entreprises peut – elle être engagée pour des violations de droit international? » in H. GHERARI et Y. KERBRAT (dir.), *L'entreprise dans la société internationale*, Paris, Pedone, 2010, p. 103.

⁴⁰ John RUGGIE, *Rapport du représentant spécial du Secrétaire spécial du Secrétaire Général chargé de la question des droits de l'homme et des sociétés transnationales et autres entreprises*, Doc off CDH NU, 17^e sess., 2011, Doc NU/A/HRC/17/31 (2011), p. 15.

⁴¹ Commission africaine des droits de l'homme et des peuples, *Social and Economic Rights Action Center (SERAC) and Center for Economic and Social Rights (CESR) c. Nigeria*, CADHP, 13 au 27 octobre 2001, 30^e session ordinaire, Communication 155/96.

⁴² Notamment dans les Principes directeurs de l'OCDE à l'intention des entreprises multinationales et la Déclaration de principes tripartite sur les entreprises multinationales et la politique sociale de l'OIT.

⁴³ Anicet Rodrigue TAYO, « Le devoir de vigilance des entreprises dans les instruments juridiques africains », *Revue québécoise de droit international*, vol. 35, n° 2, 2022, pp. 94 et s.

B-) LA COMPLEMENTARITE NECESSAIRE ENTRE RESPONSABILITE LOCALE ET DELOCALISEE

Le problème théorique précédemment identifié trouve une illustration particulièrement éclairante dans l'analyse des situations concrètes de la responsabilité des entreprises multinationales. C'est en effet à ce niveau que le risque d'atteinte aux droits de l'homme révèle toute sa portée, en mettant en évidence la nécessité d'une articulation entre les juridictions locales et celles des États d'origine des entreprises.

La loi sur le devoir de vigilance s'inscrit précisément dans cette logique, en visant à superposer au recours local un recours alternatif, voire complémentaire, dans l'État d'origine de l'entreprise. Elle tend ainsi à réduire le risque de déni de justice auquel sont confrontées les victimes, lorsqu'elles ne peuvent obtenir réparation ni devant les juridictions locales, ni, en pratique, devant celles de l'État d'origine.

Dans ce contexte, bien qu'il soit essentiel de distinguer les obligations des sociétés mères de celles de leurs filiales locales, certains éléments factuels permettent d'éclairer concrètement le rôle des opérateurs dans la mise en œuvre des coupures d'Internet.

À cet égard, dans l'affaire *Amnesty International Togo & Others c. République togolaise*, il ressort des éléments du dossier que certains opérateurs de réseaux mobiles, notamment MOOV et Togocel, avaient reçu instruction de maintenir exclusivement les services diplomatiques et gouvernementaux, tout en interrompant ou en restreignant l'accès pour les autres usagers⁴⁴. Les informations relayées par des représentants étatiques indiquent que ces instructions ont été exécutées⁴⁵, ce qui suggère une participation effective des opérateurs à la mise en œuvre matérielle des mesures de coupure.

Cet exemple met en évidence le rôle opérationnel des filiales locales dans l'exécution des décisions étatiques. Il éclaire les conditions concrètes dans lesquelles le risque d'atteinte aux droits de l'homme se réalise, et dans lesquelles les entreprises peuvent être impliquées.

L'intervention des filiales locales est, en outre, susceptible d'engager leur responsabilité au regard du droit interne applicable. Dans le cas togolais, le cadre normatif impose aux fournisseurs d'accès à Internet et aux opérateurs de réseaux mobiles une obligation de continuité du service, impliquant un accès permanent, régulier et de qualité⁴⁶. En cas de manquement, les opérateurs sont tenus d'indemniser les abonnés lésés, lesquels peuvent saisir l'autorité de régulation compétente ou les juridictions nationales⁴⁷. Ce cadre normatif a d'ailleurs déjà donné lieu à des sanctions: en 2022, l'opérateur Togo Cellulaire

⁴⁴ Cour de justice de la CEDEAO, arrêt du 25 juin 2020, *Amnesty International Togo & Others c. République togolaise* (N° ECW/CCJ/JUD/09/20), §8.

⁴⁵ *Ibid.*

⁴⁶ Togo, ARCEP, Décision N°185/ARCEP/DG/22 fixant les modalités de compensations des abonnés aux services d'accès à internet fixe du 24 octobre 2022.

⁴⁷ *Ibid.*

a été condamné à une amende de 2,361 milliards de francs CFA (soit environ 3,6 millions d'euros) pour manquements à ses obligations de qualité de service⁴⁸.

Ce dispositif témoigne de l'existence de mécanismes de responsabilité au niveau local. Toutefois, leur effectivité apparaît plus incertaine lorsque les coupures d'Internet sont motivées par des considérations politiques. Dans de telles hypothèses, les recours internes peuvent se révéler difficilement mobilisables, voire inopérants, ce qui contribue à renforcer le risque de violations des droits de l'homme demeurant sans sanction effective.

C'est précisément dans ce contexte que l'intervention de la société mère peut être interrogée au titre du devoir de vigilance. Sans préjuger de l'existence d'une obligation juridiquement stabilisée en la matière, il lui appartient, en principe, d'identifier les risques d'atteinte aux droits de l'homme liés aux activités de ses filiales, y compris lorsque celles-ci opèrent dans des environnements à risque.

L'identification et la consistance de ce risque ne peuvent toutefois être pleinement appréhendées qu'à la lumière des dynamiques normatives et jurisprudentielles encadrant les coupures d'Internet.

II-) LES FONDEMENTS NORMATIFS DU RISQUE D'ATTEINTE AU DROIT D'ACCÈS A INTERNET

Au regard du cadre international et du cadre régional spécifique aux entreprises françaises soumises à la loi sur le devoir de vigilance, un risque d'atteinte aux droits de l'homme du fait des coupures d'internet pour des motifs politiques peut être bien identifié, tant sous l'angle de l'activité normative non-contentieuse (A) que contentieuse (B). Cette activité contribue à faire émerger un droit d'accès à internet dont la juridicité apparaît encore variable et dont l'opposabilité aux entreprises FAI ou ORM demeure en construction.

A-) LES OBLIGATIONS ISSUES DES NORMES DESTINÉES AUX ETATS

La production normative à l'échelle internationale répond généralement à une difficulté ou un risque identifié dans l'ordre international. Elle intervient lorsque les États choisissent, ou se voient conduits, à ne plus laisser une situation à leur discrétion, voire à la soustraire de leur domaine réservé, dans une optique solidariste⁴⁹ plus ou moins contrainte. À l'instar du système des Nations unies ou des mécanismes de protection des droits de l'homme, ces dynamiques normatives internationales visent essentiellement à

⁴⁸ Togo, ARCEP, Décision N°2022-006/ARCEP/CD/22 du 24 juin 2022 du Comité de direction de l'Autorité de régulation des communications électroniques et des postes.

⁴⁹ Emmanuelle JOUANNET, *Le droit international Libéral-providence une histoire du droit international*, Bruxelles, Bruylant, 2011, p. 5.

endiguer des risques existants, s'inscrivant davantage dans une logique réactive que véritablement préventive⁵⁰.

Dans cette perspective, l'ordre juridique international a vu apparaître, dans le sillage du développement de la société numérique, des normes à faible juridicité, c'est-à-dire de *soft law*, principalement adressées aux États. À la lumière du cadre international des droits de l'homme existant, ces normes rappellent tant les obligations des États (1) que, de manière plus indirecte, celles des entreprises (2) en matière d'accès à internet.

1-) Les obligations des États

L'émergence d'un certain risque numérique pour les droits de l'homme peut être étayée à l'aune de plusieurs résolutions portant sur l'impact du numérique dans ce domaine. Dans cet ordre d'idées, par une résolution du 05 juillet 2012⁵¹, le Conseil des droits de l'homme a affirmé que « *les mêmes droits dont les personnes disposent hors ligne doivent être aussi protégés en ligne, en particulier la liberté d'expression, conformément au droit international* ». Par cette affirmation, il rappelle que les obligations des États en matière de droits de l'homme s'appliquent aussi dans l'espace numérique, lequel échappe pourtant par nature aux logiques territoriales de l'État-nation⁵².

Dans la même résolution, le Conseil des droits de l'homme souligne l'importance d'un internet ouvert et accessible pour garantir la jouissance des droits de l'homme. Cette reconnaissance implicite d'un droit d'accès à internet a été réitérée en 2016⁵³ et renforcée négativement par la condamnation des « *mesures visant à empêcher ou à perturber délibérément l'accès à l'information ou la diffusion d'informations en ligne* ». Invitant les États à s'abstenir de telles pratiques, le Conseil prend ainsi acte du recours croissant, par certains États, aux coupures d'Internet pour contenir des revendications politiques, qu'il considère comme attentatoires aux droits de l'homme.

Dans le même sens, l'Assemblée générale des Nations unies⁵⁴ a condamné en 2022 les coupures d'internet motivées par des considérations politiques, en réaffirmant l'importance de la liberté d'opinion et d'expression et du droit de rechercher, de recevoir et de diffuser des informations dans le contexte des technologies numériques. Quelle que soit leur teneur, il convient toutefois de rappeler que les résolutions des organes onusiens

⁵⁰ Voir notamment Laurence BOISON DE CHAZOURNES, « Préface », in M. M. MBENGUE, *Essai sur une théorie du risque en droit international public, L'anticipation du risque environnemental et sanitaire*, Paris, Pedone, 2009.

⁵¹ Résolution 20/8 du Conseil des droits de l'homme, *La promotion, la protection et l'exercice des droits de l'homme sur l'Internet*, 5 juillet 2012.

⁵² Voir Hélène RUIZ-FABRI, « Immatériel, territorialité et État », *Archives de philosophie du droit*, t. 43, 1999, pp. 187-212.

⁵³ Résolution A/HRC/RES/32/13 du Conseil des droits de l'homme (1er juillet 2016): "La promotion, la protection et l'exercice des droits de l'homme sur l'Internet".

⁵⁴ Résolution 76/227 de l'Assemblée générale, *La promotion et la protection des droits de l'homme dans le contexte des technologies numériques nouvelles et émergentes*, 10 janvier 2022.

ne sont pas juridiquement contraignantes pour les États⁵⁵, même si elles peuvent contribuer à l'émergence d'une *opinio juris* en faveur d'une norme coutumière prohibant les coupures d'Internet pour des motifs politiques⁵⁶. Elles témoignent ainsi du consensus croissant selon lequel de telles pratiques constituent une menace pour les droits de l'homme, sans pour autant consacrer un droit autonome d'accès à Internet.

Cette limite peut toutefois être nuancée à la lumière de l'observation générale n° 34 du Comité des droits de l'homme. Faisant sans doute œuvre normative en interprétant du PIDCP à la lumière des réalités nouvelles⁵⁷, le comité affirme que les interdictions générales de fonctionnement de certains sites et systèmes ne sont pas compatibles avec l'article 19 §3 du Pacte⁵⁸. Ce paragraphe n'autorise des restrictions à la liberté d'expression que si elles sont prévues par la loi, nécessaires et proportionnées à un objectif légitime, tels que la protection des droits ou de la réputation d'autrui et la sauvegarde de la sécurité nationale, l'ordre public, la santé ou la moralité publique. Le comité précise en outre que les restrictions au titre de ce paragraphe « *doivent constituer le moyen le moins perturbateur parmi ceux qui pourraient permettre d'obtenir le résultat recherché et elles doivent être proportionnées à l'intérêt protégé* »⁵⁹.

S'agissant plus spécifiquement de l'accès à internet, il estime que seules les restrictions visant un contenu déterminé peuvent être admises, à l'exclusion des interdictions fondées sur des opinions critiques à l'égard du gouvernement ou du système politique⁶⁰. Les Principes de Johannesburg sur la « *Sécurité Nationale, Liberté d'Expression et Accès à l'Information* », vont dans le même sens en excluant les restrictions visant à protéger un gouvernement de l'embarras, à dissimuler des fautes ou à imposer une idéologie⁶¹. Dans cette perspective, les coupures d'Internet à motivation politiques apparaissent, à tout le moins, difficilement conciliables avec les exigences du droit international des droits de l'homme.

Au niveau européen, si le Conseil de l'Europe a adopté des instruments contraignants en matière de protection des données personnelles (la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel entrée en vigueur le 1^{er} octobre 1985 et son protocole additionnel) ou de lutte contre la cybercriminalité (la Convention sur la cybercriminalité du 23 novembre 2001 et son protocole additionnel), le droit d'accès à internet demeure abordé dans des recommandations dépourvues de force obligatoire⁶². On retrouve néanmoins, en

⁵⁵ Michel VIRALLY, « La valeur juridique des recommandations des organisations internationales », *AFDI*, volume 2, 1956, pp. 66-96.

⁵⁶ Julien CAZALA, « Le *soft law* international entre inspiration et aspiration », *Revue interdisciplinaire d'études juridiques*, 2011, vol. 66., pp. 41-84.

⁵⁷ Laurent BASSAH, *Le pouvoir de décision du Comité des droits de l'homme des Nations Unies : Entre légitimité, autorité et effectivité*, Paris, L'harmattan, 2023, pp. 271 et s.

⁵⁸ Comité des droits de l'homme, observation générale n° 34 (2011), par. 43.

⁵⁹ *Ibid.*, par. 34.

⁶⁰ *Ibid.*, par. 43.

⁶¹ *Les Principes de Johannesburg, Sécurité Nationale, Liberté d'Expression et Accès à l'Information* (U.N. Doc. E/CN.4/1996/39).

⁶² Voir notamment la *Recommandation du Comité des ministres aux États membres sur la liberté d'internet*, 16 avril 2016 (CM/Rec (2016)5).

filigrane, dans ces instruments, l'idée d'un lien étroit entre accès à Internet et exercice effectif de la liberté d'expression, constituant ainsi les linéaments d'un droit d'accès à internet.

2-) Les obligations des entreprises

Malgré la réalité du risque d'atteinte aux droits de l'homme que constituent les coupures d'Internet, la responsabilité des entreprises possédant ou exploitant les infrastructures numériques n'est pas consacrée, en tant que telle, par des instruments interétatiques spécifiquement dédiés à ce risque. Les instruments existants se bornent principalement à rappeler aux États les obligations qui leur incombent du fait des actes commis par des acteurs privés. On peut le constater à la lumière de la Déclaration de principes sur la liberté d'expression et l'accès à l'information en Afrique, adoptée en 2019 par la Commission africaine des droits de l'homme et des peuples, qui invite les États parties à garantir la liberté d'expression « *contre les actes d'acteurs non étatiques qui entravent la jouissance de la liberté d'expression et de l'accès à l'information* »⁶³.

Ce constat doit toutefois être nuancé. Certains instruments adressent également, de manière indirecte ou partielle, des exigences aux entreprises. Ainsi, la Recommandation du Comité des ministres du Conseil de l'Europe de 2016, notamment en son annexe, précise que toute mesure prise par les autorités publiques ou par des acteurs privés visant à bloquer ou restreindre l'accès à une plateforme ou à des outils de communication numérique doit satisfaire aux exigences de légalité, de légitimité et de proportionnalité découlant de l'article 10 de la Convention européenne des droits de l'homme⁶⁴. Elle souligne également que les acteurs privés, notamment les fournisseurs de services d'internet, doivent traiter le trafic de manière transparente et non discriminatoire. Il s'agit toutefois d'indicateurs dont la portée normative demeure limitée.

Sur un plan plus global, deux rapports publiés en 2025 par la Rapporteuse spéciale sur la liberté d'opinion et d'expression concernant les incidences du numérique sur la liberté d'expression encouragent expressément les entreprises à « *faire preuve d'une diligence accrue en matière de droits de l'homme en cas de conflits, d'élections ou d'autres situations à haut risque* »⁶⁵ et à « *résister aux ordres des gouvernements visant à couper l'accès à Internet ou à restreindre l'accès aux services numériques* »⁶⁶.

Cela fait écho au rapport du Haut-Commissariat aux droits de l'homme de 2022, qui recommande aux entreprises d'employer tous les moyens juridiques à leur disposition pour empêcher la mise en œuvre d'une coupure ordonnée par les autorités et, si celle-ci devait néanmoins se produire, d'en atténuer autant que possible les effets négatifs sur les droits de l'homme. Elles sont en outre invitées à épuiser les voies de recours internes, à

⁶³ Voir le Principe 1 de la Déclaration.

⁶⁴ Voir annexe à la Recommandation CM/Rec (2016) 5.

⁶⁵ Rapport de la Rapporteuse spéciale sur la promotion et la protection du droit à la liberté d'opinion et d'expression, *La liberté d'expression dans le contexte des élections à l'ère du numérique*, op. cit., p. 24.

⁶⁶ Rapport de la Rapporteuse spéciale sur la promotion et la protection du droit à la liberté d'opinion et d'expression, *Menaces sur la liberté d'expression en ligne en temps de troubles*, op. cit., p. 21.

procéder de manière aussi restrictive que possible en préservant autant que possible les canaux de communication, et à permettre la divulgation complète des informations relatives aux interférences⁶⁷. Il est enfin préconisé aux entreprises d'exercer une diligence raisonnable pour identifier les impacts des coupures d'internet sur les droits de l'homme, d'affirmer publiquement leur engagement en faveur du droit d'accès à internet et d'instaurer un dialogue avec les parties prenantes afin de prévenir la survenance de telles coupures.

Quoi qu'il en soit, il s'agit de simples recommandations sans valeur juridique contraignante, dont la portée est toutefois amplifiée par leur reprise dans des instruments spécifiquement dédiés à la responsabilité des entreprises en matière de droits de l'homme.

B-) LES OBLIGATIONS ISSUES DES NORMES DÉDIÉES AUX ENTREPRISES

La responsabilité des entreprises en matière de droits de l'homme est abordée de manière croissante dans des instruments spécifiques, qui se caractérisent généralement par leur caractère volontaire. La logique de ces normes est d'inciter les entreprises à s'autoréguler. La problématique des coupures d'internet s'inscrit dans leur champ d'application. Il convient toutefois de distinguer les normes d'origine étatique (1) de celles d'origine privée (2).

1-) Les normes d'origine étatique

Les Principes directeurs relatifs aux entreprises et aux droits de l'homme instituent des standards de comportement pour leurs destinataires, notamment pour les FAI et ORM dans le contexte des coupures d'internet. Certes, leur juridicité, c'est-à-dire leur caractère contraignant, demeure discutée en doctrine⁶⁸. Il n'en reste pas moins que les Principes de Ruggie constituent un instrument de référence en matière de la responsabilité des entreprises, auquel se réfèrent tant les juges saisis du contentieux du devoir de vigilance⁶⁹ que les différents rapports onusiens relatifs aux coupures d'internet⁷⁰.

Dans le premier cas, les juridictions ont déjà pu rappeler, conformément aux arguments développés par la société civile, que les Principes de Ruggie constituent des sources matérielles de la loi sur le devoir de vigilance. Dans le second cas, la responsabilité des

⁶⁷ *Coupures de l'accès à Internet: tendances, causes, implications juridiques et conséquences sur une série de droits de l'homme*, Rapport du Haut-Commissariat des Nations Unies aux droits de l'homme, *op. cit.*, p. 18.

⁶⁸ Justine NOLAN, « The corporate responsibility to respect human rights: soft law or not law? », in *Human Rights obligations of Business*, Cambridge, Cambridge Press university, 2013, pp.141-143.

⁶⁹ TJ de Paris, 28 février 2023, n° RG 22/53943.

⁷⁰ *Coupures de l'accès à Internet : tendances, causes, implications juridiques et conséquences sur une série de droits de l'homme*, Rapport du Haut-Commissariat des Nations Unies aux droits de l'homme, *op. cit.*, p. 13 ; *La liberté d'expression dans le contexte des élections à l'ère du numérique*, Rapport de la Rapporteuse spéciale sur la promotion et la protection du droit à la liberté d'opinion et d'expression, *op. cit.*, p. 13 ; *Menaces sur la liberté d'expression en ligne en temps de troubles*, Rapport de la Rapporteuse spéciale sur la promotion et la protection du droit à la liberté d'opinion et d'expression, *op. cit.*, p. 11.

entreprises en matière de violations des droits de l'homme liées aux coupures d'internet est appréciée à l'aune de ces Principes : les entreprises doivent, *a minima*, exercer une diligence raisonnable afin d'identifier leurs incidences sur les droits de l'homme, prendre des mesures destinées à prévenir et atténuer ces incidences, et rendre compte de la manière dont elles y remédient.

De *lege lata* toutefois, les Principes demeurent silencieux quant à l'existence d'obligations spécifiques relatives aux coupures d'internet eu égard à la perspective généraliste originellement adoptée. Leur portée généraliste vise en effet à garantir leur applicabilité à l'ensemble des domaines dans lesquels les activités des entreprises peuvent affecter les droits de l'homme.

A la différence des Principes de Ruggie, les Principes directeurs de l'OCDE à l'intention des entreprises multinationales⁷¹ articulent les recommandations autour de thématiques spécifiques (droits humains, droit du travail, environnement, corruption, intérêts des consommateurs, publication d'informations, science et technologie, concurrence et fiscalité). La question de l'accès à internet y est abordée sous l'angle des « *sciences, technologie et innovation* » dans le cadre du chapitre IX des Principes directeurs.

Il y est recommandé aux entreprises de contribuer au développement technologique, en respectant les Principes directeurs et les exigences légales applicables, notamment en matière de protection de la vie privée et des données⁷². Plus précisément, ces Principes invitent les entreprises à exercer un devoir de diligence fondé sur les risques à l'égard des impacts négatifs réels ou potentiels liés à la science, à la technologie et à l'innovation⁷³. Les commentaires précisent que les entreprises devraient « *soutenir, lorsque cela est approprié en fonction de leurs circonstances, les efforts de coopération menés dans les forums adéquats pour promouvoir un internet ouvert, libre, mondial, interopérable, fiable, accessible, abordable, sûr et résilient, y compris par le respect des libertés d'expression, de réunion pacifique et d'association en ligne, et conformément aux sujets couverts par les Principes directeurs* »⁷⁴.

Dans une perspective de *lege ferenda*, certaines initiatives institutionnelles ont cherché à préciser davantage les responsabilités des entreprises. Ainsi, le Commissaire aux droits de l'homme du Conseil de l'Europe proposait en 2014 de s'appuyer sur les Principes de Ruggie afin de définir de nouvelles orientations sur les responsabilités des entreprises

⁷¹ Sur des considérations doctrinales concernant ces principes, voir Laurence DUBIN, « L'élaboration des principes à l'intention des entreprises multinationales par l'OCDE ou comment globaliser la régulation du comportement d'un acteur global ? », in SFDI, *Le pouvoir normatif de l'OCDE*, Paris, Pedone, 2013, pp. 113-128 ; Rainer GEIGER, « Instruments internationaux de responsabilité de l'entreprise : le rôle de l'OCDE », in DAUGAREILH I. (dir.), *La responsabilité sociale de l'entreprise transnationale et globalisation de l'économie*, Bruxelles, Bruylant, 2010, pp. 413-428 ; Isabelle DAUGAREILH, « La dimension sociale des Principes directeurs de l'OCDE à l'intention des entreprises multinationales », *Revue générale de droit international public*, 2008, pp. 567-602.

⁷² Voir OCDE (2023), *Principes directeurs de l'OCDE à l'intention des entreprises multinationales sur la conduite responsable des entreprises*, Éditions OCDE, Paris, p. 53.

⁷³ Voir *ibid.*, Chapitre IX, paragraphe 1.

⁷⁴ *Ibid.*, p. 54.

privées en matière de droits de l'homme lorsqu'elles procèdent d'elles-mêmes, ou à la demande des autorités publiques, à des coupures internet⁷⁵.

Dans ce prolongement, la Déclaration de Windhoek +30, a appelé les entreprises technologiques à évaluer de manière transparente les risques pour les droits de l'homme et à prendre des mesures pour les atténuer⁷⁶. Elle a notamment inspiré l'adoption des Principes pour la gouvernance des plateformes numériques, qui imposent aux entreprises des exigences en matière de diligence raisonnable, de transparence et de responsabilité⁷⁷.

Toutefois, ces instruments visent principalement les plateformes numériques. Leur extension aux FAI et ORM nécessite donc des précisions. La plateforme numérique se définit comme un espace virtuel, reposant sur des logiciels et des technologies permettant d'organiser les interactions entre différents utilisateurs. Elle permet notamment la création la diffusion et la commercialisation des contenus ou des services en ligne et constitue, ce faisant, une interface de mise en relation entre des offreurs et des demandeurs d'un bien ou d'un service⁷⁸. Facebook, LinkedIn, AirBnB et Uber en sont des exemples caractéristiques. Ils se distinguent nettement des FAI et ORM, qui relèvent d'entreprises spécialisées dans les technologies de l'information et de la communication⁷⁹ et fournissent principalement les infrastructures et réseaux de télécommunications nécessaires à la transmission et le traitement des informations numériques⁸⁰.

Si une distinction doit être maintenue entre ces catégories d'acteurs, il peut néanmoins être soutenu que, compte tenu de la finalité de ces instruments, certaines de leurs exigences pourraient être transposées, avec prudence, aux fournisseurs d'accès et opérateurs de réseaux.

Ainsi, sans consacrer une obligation juridique pleinement autonome, ces normes contribuent à structurer des attentes croissantes à l'égard des entreprises en matière de prise en compte du risque lié aux coupures d'internet.

⁷⁵ Voir *La prééminence du droit sur internet et dans le monde numérique en général*, CommDH/IssuePaper (2014)1.

⁷⁶ Elle a été adoptée en 2021 à l'issue de la conférence internationale de la journée mondiale de la liberté de la presse organisée par l'UNESCO en Namibie, voir UNESCO, 2021, Déclaration de Windhoek +30 : l'information comme bien commun https://unesdoc.unesco.org/ark:/48223/pf0000378158_fre, consulté le 06 août 2025.

⁷⁷ UNESCO, Paris, 2023, Principes pour la gouvernance des plateformes numériques: préserver la liberté d'expression et l'accès à l'information - une approche multipartite, <https://unesdoc.unesco.org/ark:/48223/pf0000387359>, consulté le 06 août 2025.

⁷⁸ Voir Rapport du Cigref, *Nouvelles stratégies de plateformes*, décembre 2029, pp. 8 et s., en ligne <https://www.cigref.fr/wp/wp-content/uploads/2019/12/cigref-nouvelles-strategies-plateformes-business-conception-mise-en-oeuvre-decembre-2019.pdf>, consulté le 6 août 2025.

⁷⁹ Voir CNUCED, 2017, *Rapport sur l'investissement dans le monde: l'investissement et l'économie numérique*, Nations Unies, Genève.

⁸⁰ Voir entrée Serge Braudo, « Nouvelles technologies de l'information et de la communication », in *Dictionnaire du droit privé*, en ligne, <https://www.dictionnaire-juridique.com/definition/ntic-nouvelles-technologies-de-l-information-et-de-la-communication.php>.

2-) Les normes d'origine privée

En complément des instruments interétatiques et des standards internationaux, diverses initiatives normatives issues du secteur privé contribuent à structurer les obligations des acteurs privés en matière d'accès à internet. Face à la généralisation des coupures ordonnées par les autorités publiques, les entreprises technologiques ont progressivement élaboré des engagements volontaires destinés à encadrer leur conduite.

Ces engagements relèvent de la *soft law* et sont, en principe, dépourvus de force obligatoire⁸¹. Ils nourrissent les critiques relatives à la privatisation des droits de l'homme et aux limites de l'autorégulation⁸². Toutefois, leur portée juridique ne saurait être négligée. Selon leur formulation, leur incorporation dans des instruments juridiques contraignants ou la manière dont elles sont mobilisées dans les relations interentreprises ou pour l'information des tiers, ils peuvent produire des effets juridiques indirects et être prises en compte par les juridictions⁸³.

Dans ce cadre, les initiatives multipartites jouent un rôle structurant. Les Principes sur la liberté d'expression et la vie privée du Global Network Initiative (GNI)⁸⁴ renvoient explicitement aux normes universellement reconnues relatives aux droits de l'homme. Ils imposent aux entreprises membres de mettre en place des procédures décisionnelles responsables, impliquant l'examen rigoureux des demandes gouvernementales susceptibles de restreindre l'accès au réseau, fondées sur les lois et les normes internationales.

L'intérêt de ce dispositif réside notamment dans l'existence de mécanismes de transparence et d'évaluation indépendante. Les rapports publiés dans ce cadre permettent de documenter les pratiques de restriction de l'accès à internet et instaurent

⁸¹ Pour approfondir, voir Gérard FARJAT, « Réflexions sur les codes de conduite privés », in *Le droit des relations économiques internationales*, Études offertes à Berthold Goldman, Paris, Litec, pp. 47-66 ; Marion LAROUER, « Codes de conduites », *LEX ELECTRONICA*, vol 23-9, 2024, en ligne, [https://lexelectronica.openum.ca/files/sites/103/Codes-de-conduite LAROUER.pdf](https://lexelectronica.openum.ca/files/sites/103/Codes-de-conduite%20LAROUER.pdf) consulté le 9 novembre 2025 ; Brigitte PEREIRA, « Chartes et codes de conduite : le paradoxe éthique », *Management & Avenir*, 2009, 21(1), pp. 26-43 ; Jean-Baptiste RACINE, « La valeur juridique des codes de conduite privés dans le domaine de l'environnement », *Revue Juridique de l'Environnement*, n°4, 1996. pp. 409-424 ; G. MARAIN, *La juridicisation de la responsabilité sociétale des entreprises*, Marseille, P.U.A.M., 2016 ; M. LAROUER, *Les codes de conduite, sources du droit*, Paris, Dalloz, 2018, 554 p.

⁸² Alexandre CURCHOD, *Liberté d'expression, Guide juridique pratique et perspectives*, Favre, Paris, 2019, pp. 132 et s.

⁸³ Sur ces dynamiques, voir Cour d'appel de Versailles, 17^e chambre, 26 novembre 2015, n° 14/01071 ; Cass. Crim., 25 septembre 2012, n° 10-82938 ? Erika, D. 2012, 2711, note Delebecque, *JCP* 2012, 1243, note Le Couvior, Bull. Joly 2013, 69, note Trébulle ; voir également M.-P. CAMPROUX-DUFFRENE, D. GUIHAL, « Pollution maritime. Naufrage de l'Erika. Responsabilité pénale. Loi du 5 juillet 1973. Convention MARPOL. ZEE. Responsabilité civile pour dommages causés à l'environnement par des hydrocarbures en mer. Réparation du préjudice écologique pur. Cour de cassation, Chambre criminelle, 25 septembre 2012, SA Total et s., n° 3439, avec note », *RJE* 2013, pp. 457-480 ; Cour suprême de la Californie, *Kasky v. Nike*, 2 mars 2002.

⁸⁴ Sur cette organisation fondée par un consortium d'entreprises, d'universitaires et d'organisations de la société civile, voir <https://globalnetworkinitiative.org/gni-principles/>.

une forme de pression réputationnelle sur les entreprises et les États⁸⁵. Ainsi, le GNI œuvre sur le plan normatif pour garantir notamment l'accès au réseau pour les usagers dans le prolongement du rôle de l'*Internet Corporation for Assigned Names and Numbers*, société à but non lucratif œuvrant pour l'attribution des noms de domaine et des adresses IP afin d'ordonner sur le plan technique l'accès à internet⁸⁶.

Au-delà du dispositif du GNI, les entreprises subissent la pression d'une myriade d'organisations de la société civile, à l'instar de l'*Internet Society* ou encore d'*Accessnow*, qui participent à la documentation des coupures d'internet et à la mise en visibilité des pratiques étatiques et privées, contribuant ainsi à l'identification et à la prévention du risque.

Parallèlement, certaines entreprises ont développé des politiques internes encadrant leur réponse aux demandes de coupure. Ces politiques, souvent inspirées des standards internationaux, prévoient des procédures d'examen juridique des demandes étatiques et des engagements à limiter leur coopération lorsque celles-ci apparaissent contraires aux droits de l'homme.

L'exemple du groupe Vodafone est à cet égard significatif : ses politiques internes imposent un contrôle juridique systématique et prévoient des mécanismes de contestation des demandes jugées disproportionnées⁸⁷.

Si ces initiatives demeurent volontaires, elles participent à la structuration d'un ordre normatif privé qui complète les insuffisances du droit positif⁸⁸, pour ainsi étendre le champ du droit administratif global⁸⁹. Elles contribuent à diffuser des standards internationaux et à renforcer, de manière indirecte, les exigences pesant sur les entreprises, notamment afin de promouvoir la transparence, renforcer la participation et instaurer des dispositifs de responsabilisation à l'échelle globale.

Le droit d'accès à internet est en conséquence promu non seulement par les entreprises technologiques à travers les normes privées, mais également par la société civile qui mobilise par ailleurs les recours juridictionnels.

III-) LES FONDEMENTS JURISPRUDENTIELS DU RISQUE D'ATTEINTE AU DROIT D'ACCÈS A INTERNET

⁸⁵ Voir notamment le rapport de l'évaluation indépendante du 23 octobre 2023 couvrant le cycle 2021/2022, en ligne, https://globalnetworkinitiative.org/wp-content/uploads/GNI_PAR23_102023_casestudies.pdf, consulté le 10 novembre 2025.

⁸⁶ *Ibid.*, pp. 94 et s. ; Michèle RIOUX, Olivier DAGENAIS, *op. cit.*, p. 361.

⁸⁷ Voir https://www.vodafone.com/network-shutdowns?utm_source=chatgpt.com, consulté le 10 novembre 2025.

⁸⁸ Michèle RIOUX, Olivier DAGENAIS, « Le rôle des organisations internationales dans la gouvernance d'Internet et des secteurs numériques », *Revue québécoise de droit international*, 2021, hors-série, pp. 357-371 ; Patrick JACOB « La gouvernance de l'Internet du point de vue du droit international public », *Annuaire français de droit international*, vol. 56, 2010, pp. 543-563.

⁸⁹ Raphaël MAUREL, *Les sources du droit administratif global*, Thèse, Université Clermont Auvergne, 2019, 687 p.

Des facteurs contextuels, tels que ceux liés à la situation géographique ou l'existence de précédents avérés, sont également déterminants pour étayer l'existence d'un risque. Dans cette perspective, le risque d'atteinte grave aux droits de l'homme découlant des coupures d'internet apparaît particulièrement prégnant dans le contexte sous-régional ouest-africain, où opèrent des entreprises soumises à la loi sur le devoir de vigilance.

La jurisprudence de la Cour de justice de la Communauté économique des États de l'Afrique de l'Ouest (ci-après Cour de justice de la CEDEAO) le montre à suffisance. Elle a en effet consacré un droit d'accès à internet (B) de manière plus explicite que la Cour européenne des droits de l'homme (CEDH) (A). Sans préjuger d'une transposition automatique de ces solutions à l'ordre juridique international général ou aux obligations directes des entreprises, ces décisions contribuent néanmoins à objectiver l'existence d'un risque juridique identifiable.

Par ailleurs, ce risque est conforté par des précédents mettant directement en cause des opérateurs privés dans des mécanismes quasi-contentieux. La saisine d'un point de contact national dans le cadre des Principes directeurs de l'OCDE illustre à cet égard la possibilité concrète de mobilisation de la responsabilité des FAI et ORM (C).

A-) L'INCIDENCE DES DÉCISIONS DE LA COUR EUROPÉENNE DES DROITS DE L'HOMME

Dans le cadre des États européens d'origine des FAI ou ORM soumis à la loi sur le devoir de vigilance, un droit d'accès à internet est indirectement garanti par la Cour européenne des droits de l'homme (CEDH), à travers les droits de l'homme préexistants⁹⁰, notamment la liberté d'expression consacrée à l'article 10 de la Convention européenne des droits de l'homme et de sauvegarde des libertés fondamentales (Conv. EDH).

Cette protection résulte de la méthode d'interprétation dynamique adoptée de longue date par la Cour, qui conçoit la Convention comme « *un instrument vivant* »⁹¹. Ainsi, dans l'affaire *Yildirim c. Turquie*, la Cour a jugé contraire à l'article 10 le blocage de l'hébergeur Google Sites ordonné pour empêcher l'accès à un site diffusant des propos outrageant la mémoire d'Atatürk. Pour la CEDH, la base légale invoquée par la Turquie ne répondait pas à l'exigence de prévisibilité, condition indispensable à la conformité d'une ingérence à la Conv. EDH⁹².

La jurisprudence de la CEDH repose toutefois sur l'articulation étroite entre liberté d'expression et limitations autorisées par l'article 10 § 2. La liberté d'expression, bien que centrale en régime démocratique⁹³, n'est pas absolue. Elle peut être restreinte sous réserve des conditions cumulatives de légalité, de nécessité et de proportionnalité. Des restrictions peuvent ainsi être jugées nécessaires, notamment pour la protection de la réputation d'autrui au titre de l'article 8 de la Conv. EDH relatif au droit au respect de la

⁹⁰ Marie Bastian, « La fragmentation d'un droit préexistant ou la fondamentalité par analogie : le cas du droit d'accès à Internet », *La Revue des droits de l'homme*, 2019, n° 15, mis en ligne le 10 décembre 2018.

⁹¹ CEDH, 25 février 1978, *Tyrer c/ Royaume-Uni*, série A n° 26, req. n°5856/72, §31.

⁹² CEDH, arrêt du 18 décembre 2012, *Yildirim c. Turquie*, req. n° 3111/10.

⁹³ Christianne FERAL-SCHUHL, *op. cit.*, p. 1524 et s.

vie privée et familiale⁹⁴, comme l'illustre, par exemple, la condamnation d'une ONG pour avoir qualifié des propos d'un universitaire d'« antisémites »⁹⁵.

À cet égard, les motifs généralement invoqués pour justifier les coupures d'internet, tels que la sécurité nationale et la sûreté nationale, ne sont pas, en tant que tels, exclus du champ des restrictions admissibles⁹⁶, au regard de l'article 10 §2 de la Conv. EDH⁹⁷. Par exemple, dans l'affaire *Zana c. Turquie*⁹⁸, des déclarations publiques susceptibles d'encourager la violence ont légitimé une ingérence étatique.

Il en résulte une position nuancée : si la Cour encadre strictement les mesures de blocage d'internet, elle n'exclut pas en principe leur possibilité. Dans sa jurisprudence récente relative au blocage de plateformes numériques, elle adopte une approche exigeante, en sanctionnant notamment les mesures générales et indiscriminées⁹⁹. Ainsi, dans une affaire concernant le blocage de l'intégralité du site internet YouTube pour atteinte à la mémoire d'Atatürk sur quelques pages de la plateforme¹⁰⁰, la CEDH a estimé que les mesures de blocages constituaient une ingérence en ce qu'elles rendaient inaccessibles un site contenant des informations spécifiques pour les requérants et les privaient d'une source importante de communication. L'ingérence caractérisée, la CEDH devait vérifier si elle était justifiée, et est arrivée à la conclusion que l'État défendeur a violé l'article 10 de la conv. EDH, parce que la loi ne prévoyait pas le blocage intégral d'un site internet. Autrement dit, l'État défendeur était fondé en vertu de la loi à bloquer uniquement des contenus spécifiques du site internet. Ainsi, le blocage intégral d'un site internet est possible si la loi l'a prévu.

Dans une autre affaire¹⁰¹, un site internet partageant la même adresse IP qu'un autre site visé par une ordonnance a été bloqué par les autorités. La CEDH a estimé que la loi invoquée pour fonder l'ingérence ne répondait pas à la condition de prévisibilité, eu égard au fait que ladite loi donnait une trop grande latitude à l'organe compétent de bloquer un site internet sans tenir compte des incidents de cette coupure sur les autres sites internet connexes. Elle a conclu à la violation de l'article 13 combiné à l'article 10 de la Conv. EDH en se basant par ailleurs sur le fait que les mesures de blocage n'aient pas été prises par un organe juridictionnel susceptible de faire valoir le droit du requérant à se faire entendre, alors même que les juridictions saisies par la suite par le requérant n'ont pas

⁹⁴ CEDH, arrêt du 5 février 2009, *Brunet-Lecomte et autres c. France*, req. n°42117/04 ; CEDH, arrêt du 27 juin 2017, *Medžlis Islamske Zajednice Brčko et autres c. Bosnie-Herzégovine*, G.C., req. n°17224/11 ; CEDH, arrêt du 22 octobre 2007, *Lindon, Otchakovsky-Laurens et July c. France*, G.C., 22 octobre 2007, req. n°21279/02 et 36448/02 ; CEDH, arrêt du 14 janvier 2014, *Ojala et Etukeno Oy c. Finlande*, req. n°69939/10.

⁹⁵ CEDH, arrêt du 7 juin 2016, *Cicad c. Suisse*, req. n°17676/09.

⁹⁶ *Coupures de l'accès à Internet : tendances, causes, implications juridiques et conséquences sur une série de droits de l'homme*, Rapport du Haut-Commissariat des Nations Unies aux droits de l'homme, *op. cit.*, p. 9.

⁹⁷ CEDH, arrêt du 8 juillet 1999 (GC), *Sürek (n°1) c. Turquie*, req. n° 26682/95.

⁹⁸ Voir par exemple CEDH, arrêt du 25 novembre 1997, *Zana c. Turquie*, req. n° 18954/91 ; CEDH, arrêt du 2 octobre 2008, *Leroy c. France*, req. n°36109/03.

⁹⁹ Voir notamment CEDH, arrêt du 23 juin 2020, *000 Flavus et autres c. Russie*, req. n° 12468/15, 23489/15, et 19074/16 ; CEDH, *Bulgakov c. Russie (n° 20159/15) et Engels c. Russie*, req. n° 61919/16 ; CEDH, arrêt du 7 juin 2022, *Taganrog LRO et autres c. Russie*, req. n° 32401/10.

¹⁰⁰ CEDH, arrêt du 1^{er} décembre 2015, *Cengiz et autres c. Turquie*, req. n°48226/10 et 14027/11.

¹⁰¹ CEDH, arrêt du 23 juin 2020, *Vladimir Kharitonov c. Russie*, req. n° 10795/14.

été en mesure d'apprécier les intérêts en jeu en tenant compte des principes de nécessité et de proportionnalité.

A l'analyse de cette jurisprudence, l'existence d'un droit autonome d'accès à internet dans le système de la Conv. EDH demeure débattu¹⁰², ce qui est en phase avec la dynamique interne de certains États. En effet, en droit français, le Conseil d'État français l'a envisagé dans un rapport comme « *un droit fondamental à part entière* »¹⁰³, tandis que le Conseil constitutionnel a rattaché dans une décision l'accès au réseau à la liberté d'expression, « *eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique* »¹⁰⁴. On peut à tout le moins s'accorder avec les auteurs qui estiment que ce droit demeure principalement « *un droit à l'accès au réseau comme structure, mais pas entièrement comme contenu* »¹⁰⁵. Une reconnaissance plus marquée de ce droit est toutefois à l'œuvre dans la jurisprudence de la cour de justice de la CEDEAO, renforçant ainsi la vigilance dont devrait faire preuve les FAI et ORM.

B-) L'INCIDENCE DES DÉCISIONS DE LA COUR DE JUSTICE DE LA CEDEAO

L'émergence d'un devoir de vigilance numérique s'inscrit dans un contexte ouest-africain marqué par une multiplication des contentieux relatifs aux coupures d'internet pour des motifs politiques. La Cour de justice de la CEDEAO a ainsi successivement condamné plusieurs États, notamment dans les affaires *Amnesty International Togo & Others c. République togolaise*¹⁰⁶, *(SERAP) & Others v. Federal Republic of Nigeria*¹⁰⁷, *Association des Blogueurs de Guinée (ABLOGUI) & Others c. État de Guinée*¹⁰⁸ ou encore *Association des Utilisateurs des Technologies de l'Information et de la Communication (ASUTIC) et Monsieur Ndiaga Gueye contre la République du Sénégal*¹⁰⁹.

Ce corpus jurisprudentiel contribue à la fois à renforcer la protection juridictionnelle (1) et à en structurer le contenu normatif d'un droit d'accès à internet (2).

1-) La protection maximale d'un droit d'accès à internet

¹⁰² Christianne FERAL-SCHUHL, *op. cit.*, p. 1526 et s.

¹⁰³ Conseil d'État, *Le numérique et les droits fondamentaux*, documentation française, étude annuelle, sept. 2014, p. 90.

¹⁰⁴ DC 2009-580 du 10 juin 2009, *Loi favorisant la diffusion et la protection de la création sur internet*.

¹⁰⁵ Voir Berangère TAXIL, « Internet et l'exercice des droits fondamentaux », in SFDI, *Internet et le Droit International*, 2014, Paris, Pedone, p. 126

¹⁰⁶ Cour de justice de la CEDEAO, arrêt du 25 juin 2020, *Amnesty International Togo & Others c. République togolaise* (N° ECW/CCJ/JUD/09/20).

¹⁰⁷ Cour de justice de la CEDEAO, arrêt du 14 juillet 2022, *The registered trustees of the Socio-economic Rights and Accountability Project (SERAP) & Others v. Federal Republic of Nigeria*, (N° ECW/CCJ/JUD/40/22).

¹⁰⁸ Cour de justice de la CEDEAO, arrêt du 31 octobre 2023, *Association Des Blogueurs De Guinée (ABLOGUI) & Others c. État de Guinée* (N° ECW/CCJ/JUD/38/23).

¹⁰⁹ Cour de justice de la CEDEAO, arrêt du 14 mai 2025, *Association des Utilisateurs des Technologies de l'Information et de la Communication (ASUTIC) et Monsieur Ndiaga Gueye contre la République du Sénégal* (N° ECW/CCJ/JUD/29/25).

Les recours relatifs aux coupures d'internet mettent en lumière le caractère maximal de la protection accordée par la Cour de justice de la CEDEAO, tant du point de vue procédural que matériel¹¹⁰. L'adoption du Protocole additionnel de 2005¹¹¹, qui autorise la saisine directe de la Cour par les victimes alléguant une violation des droits de l'homme, constitue une innovation majeure en comparaison d'autres juridictions régionales, notamment la Cour africaine des droits de l'homme et des peuples (CADHP), soumise au principe du double consentement des États aux juridictions internationales¹¹².

De même, la juridiction communautaire n'exige pas l'épuisement préalable des voies de recours internes¹¹³. Par cette suppression d'un filtre traditionnel en contentieux international des droits de l'homme, la Cour offre aux victimes une garantie procédurale de premier ordre, qui affranchit la protection de leurs droits du consentement ou de l'inaction des États. Ainsi, le droit d'accès à internet bénéficie d'une protection procédurale maximale.

Aussi, la compétence matérielle de la Cour est fondée sur l'ensemble des instruments internationaux relatifs aux droits de l'homme, ce qui lui permet d'appliquer simultanément des normes issues du PIDCP, de la Charte africaine des droits de l'homme et des peuples (Ch. ADHP) et, dans certaines hypothèses, du Traité révisé de la CEDEAO. Dans l'affaire *Amnesty International Togo & Others c. République togolaise*, elle devait déterminer si la coupure d'internet constituait une violation du droit à la liberté d'expression garanti par l'article 19 § 2 du PIDCP et le droit de chercher et de recevoir des informations, d'exprimer et diffuser ses opinions qui est garanti par l'article 9 §1 et §2 de la Charte africaine des droits de l'homme et des peuples. La double base normative renforce objectivement le champ de protection, car il est bien établi que la formulation du droit à la liberté d'expression dans le cadre de la Charte africaine des droits de l'homme et des peuples est plus restrictive que dans le cadre du PIDCP¹¹⁴. Par exemple, contrairement au PIDCP qui est très explicite, la Ch. ADHP n'explicite pas les conditions auxquelles des restrictions peuvent être apportées au droit à la liberté d'expression, car l'article 9 §2 précise simplement que ce droit s'exerce « dans le cadre des lois et règlements ».

¹¹⁰ Alioune SALL, *Le contentieux de la violation des droits de l'homme devant la Cour de justice de la CEDEAO*, Paris, L'Harmattan, 2019 ; Cette protection est étendue également aux investisseurs, voir M. HAPPOLD, « Investor-state dispute settlement using the ECOWAS Court of Justice : an analysis and some Proposals », *ICSID Review*, vol. 34, N° 2 (2019).

¹¹¹ Protocole additionnel (A/SP.1/01/05) portant amendement du préambule, des articles 1er, 2, 9, 22 et 30 du Protocole A/P1/7/91 relatif à la Cour de justice de la Communauté, ainsi que de l'article 4 paragraphe 1 de la version anglaise dudit protocole, 19 janvier 2005.

¹¹² Art. 34 §6 du Protocole relatif à la Charte africaine des droits de l'homme et des peuples portant création d'une Cour africaine des droits de l'homme et des peuples de 1998 ; M. KAMTO, « La volonté de l'État en droit international », *RCADI*, vol. 310, 2007, pp. 256 et s.

¹¹³ Ludovic HENNEBEL, Hélène TIGROUDJA, *Traité de droit international des droits de l'homme*, Paris, A. Pedone, 2016, p. 401.

¹¹⁴ Mihaela Anca AILINCAI, « Le droit à la liberté d'expression dans la jurisprudence de la Cour africaine des droits de l'homme et des peuples », in Guillaume Le Floch (dir.) *La Cour africaine des droits de l'homme et des peuples*, Paris, Pedone, 2023, pp. 306 et s.

La diversité des sources offre donc aux juges communautaires une latitude interprétative substantielle, encore illustrée dans l'affaire *ASUTIC et Monsieur Ndiaga Gueye c. la République du Sénégal*¹¹⁵, où les requérants invoquaient également l'Acte additionnel de la CEDEAO sur l'harmonisation des politiques et du cadre réglementaire du secteur de l'information et des télécommunications et la Directive de l'UEMOA sur l'harmonisation des politiques de supervision et de régulation du secteur des télécommunications. La cour de justice de la CEDEAO, conformément au test issu de sa jurisprudence *Digital Rights Lawyers Initiative*¹¹⁶, s'est toutefois déclarée incompétente pour connaître de la violation de ces derniers instruments¹¹⁷. Selon ce test, sa compétence matérielle est subordonnée aux allégations de violation d'un droit subjectif consacré par un instrument auquel est partie l'État défendeur. La Cour a néanmoins admis dans l'affaire *ABLOGUI & Others c. État de Guinée*, la justiciabilité de l'article 66 §2 c) du Traité révisé garantissant les droits des journalistes¹¹⁸, tout en rejetant les prétentions au fond faute de qualité de journalistes des requérants¹¹⁹.

Pour finir, il convient de relever la diversité substantielle des droits affectés par les coupures d'internet. En effet, dans les affaires *SERAP & Others v. Federal Republic of Nigeria* et *ASUTIC et Monsieur Ndiaga Gueye c. la République du Sénégal*, les requérants ont invoqué un éventail très large de droits : liberté d'expression, liberté d'accès à l'information, liberté de réunion, droit au travail et droit à un procès équitable. Concernant le droit au travail par exemple, la Cour de justice de la CEDEAO a reconnu qu'internet et les réseaux sociaux « *alimentent des aspects essentiels du travail dans pratiquement toutes les institutions ou organisations modernes* »¹²⁰. Partant dès lors du caractère fondamental d'internet pour les professionnels du domaine des Technologies de l'information et de la communication, elle a estimé que l'État du Sénégal avait violé le droit au travail de l'un des requérants¹²¹. Le juge communautaire acte ainsi une réalité juridique fondamentale : « *tout droit de l'homme fondamental dont l'exercice ou la jouissance dépend de, ou est facilité par, l'accès à internet peut être violé par un État par le biais d'une coupure illégale ou arbitraire d'Internet* »¹²². Les coupures d'internet étant analysées comme une ingérence susceptible d'affecter une pluralité de droits, le droit d'accès à internet bénéficie d'une protection normative étendue devant la Cour de justice de la CEDEAO, qui éclaire le contenu de ce droit de manière prétorienne.

¹¹⁵ Cour de justice de la CEDEAO, arrêt du 14 mai 2025, *Association des Utilisateurs des Technologies de l'Information et de la Communication (ASUTIC) et Monsieur Ndiaga Gueye contre la République du Sénégal* (N° ECW/CCJ/JUD/29/25).

¹¹⁶ Cour de justice de la CEDEAO, arrêt du 13 mars 2023, *Digital Rights Lawyers Initiative v. Federal Republic of Nigeria* (No. ECW/CCJ/JUD/02/23).

¹¹⁷ *Association des Utilisateurs des Technologies de l'Information et de la Communication (ASUTIC) et Monsieur Ndiaga Gueye contre la République du Sénégal*, op. cit., §30.

¹¹⁸ *Association Des Blogueurs De Guinée (ABLOGUI) & Others c. État de Guinée*, op. cit., §74.

¹¹⁹ *Ibid.*, §75.

¹²⁰ *Association des Utilisateurs des Technologies de l'Information et de la Communication (ASUTIC) et Monsieur Ndiaga Gueye contre la République du Sénégal*, op. cit., §74.

¹²¹ *Ibid.*, §76.

¹²² *Ibid.*, §74.

2-) La construction prétorienne d'un droit d'accès à internet

La jurisprudence de la juridiction communautaire ouest-africaine contribue de manière déterminante à l'affirmation d'un véritable droit d'accès à internet. Ce droit, bien que dérivé de la liberté d'expression, acquiert progressivement un statut autonome au regard de son rôle fonctionnel dans l'ordre numérique contemporain. Il convient de distinguer méthodiquement les différents aspects du droit d'accès à internet, tels qu'ils ressortent des arrêts rendus par cette Cour.

.

a-) La prohibition des coupures d'internet pour des motifs politiques

Dans l'affaire *ABLOGUI c. Guinée*, la Cour énonce, par un *obiter dictum* explicite, qu'interdire un site ou un système d'information au seul motif qu'il critique le gouvernement constitue une violation de l'article 19 (3) du PIDCP¹²³. Cet *obiter dictum* s'apparente à un principe cardinal du droit d'accès à internet : la coupure ou la restriction du réseau pour des considérations politiques est intrinsèquement illicite. Par-là, les juges communautaires abordent la question des restrictions de manière négative, dans le sens où les instruments relatifs aux droits de l'homme affirment positivement les motifs pour lesquels des restrictions peuvent être apportées à la liberté d'expression. Si le motif politique est donc de nature à rendre illicite toute restriction de l'accès à internet, ce motif est généralement dissimulé par d'autres motifs, comme celui de la sécurité. Il va sans dire que les requérants auront à convaincre les juges du détournement des motifs légitimes par des États à des fins politiques.

b-) La prohibition des coupures d'internet d'ordre général

Dans l'affaire *ASUTIC et Monsieur Ndiaga Gueye c. la République du Sénégal*, s'appuyant notamment sur l'Observation générale n° 34 du Comité des droits de l'homme relative à l'article 19 du PIDCP ainsi que sur la Déclaration de principes de la Commission africaine (2019), la Cour de justice de la CEDEAO a jugé que « la fermeture générale de l'internet et des plateformes de réseaux sociaux (...) ne saurait constituer une réponse nécessaire ou proportionnée »¹²⁴, quels que soient les messages haineux et subversifs sur les réseaux sociaux.

La Cour adopte ainsi une position plus ferme que celle de la CEDH, qui admet encore en théorie la possibilité de restrictions intégrales¹²⁵, pourvu qu'elles satisfassent aux conditions de légalité, de nécessité et de proportionnalité. Cette approche, qui va au-delà des exigences intrinsèques des instruments internationaux relatifs aux droits de l'homme pertinents, va nécessairement créer un conflit avec les dispositions internes, adoptées par certains États à la suite des saisines de la juridiction communautaire. Dans ce sens, l'article 50 de la loi togolaise de 2019 sur la sécurité intérieure confère au ministre chargé

¹²³ *Association Des Blogueurs De Guinée (ABLOGUI) & Others c. État de Guinée*, op. cit., §65.

¹²⁴ *Association des Utilisateurs des Technologies de l'Information et de la Communication (ASUTIC) et Monsieur Ndiaga Gueye contre la République du Sénégal*, op. cit., §63.

¹²⁵ Voir notamment CEDH, arrêt du 1er décembre 2015, *Cengiz et autres c. Turquie*, op. cit.

de l'administration territoriale le pouvoir de demander « *l'interruption de tout service de communication au public qui constitue un risque grave à l'ordre public* ». La disposition est pour le moins ambiguë, mais elle peut être mobilisée sans doute pour justifier une coupure totale de l'accès à internet. Sans doute, la Cour aura à se prononcer de nouveau sur cet aspect à l'aune de cette disposition si jamais elle est saisie de nouveau. Quant aux FAI et ORM, ils auront à faire face à des obligations contradictoires, d'autant que la primauté du droit de la CEDAO n'est clairement pas consacrée et les décisions de la Cour de justice sont contestées par les juridictions suprêmes des États membres et faiblement exécutées par les États membres¹²⁶.

c-) La reconnaissance d'un droit d'accès à internet et aux plateformes numériques

Bien que la Cour ait rappelé dans l'affaire *Amnesty International Togo & Others c. République togolaise* que « *l'accès à internet n'est pas à proprement parler un droit de l'homme fondamental* »¹²⁷, elle reconnaît que l'accès à internet est un droit dérivé, composante fonctionnelle du droit à la liberté d'expression. Elle précise à ce titre que le droit d'accès à internet est lié à la liberté d'expression et que le premier englobe le second. Elle affirme l'interconnexion, sans doute irréductible, entre droit d'accès à internet et liberté d'expression. Autrement dit, la Cour consacre explicitement l'existence d'un droit d'accès à internet, tout en précisant que ce droit ne possède pas d'autonomie propre et s'inscrit seulement comme une modalité de la liberté d'expression.

Cette approche est confirmée par la Cour de justice de la CEDEAO dans l'affaire *SERAP & Others v. Federal Republic of Nigeria*, qui affirme que l'accès à Twitter constitue un droit dérivé protégé par les articles 9 de la Ch. ADHP et 19 du PIDCP, jouissant à ce titre d'une protection juridictionnelle. Interrogée sur l'existence d'un droit d'accès à cette plateforme, la Cour répond sans ambiguïté par l'affirmative, pour ainsi consacrer un droit d'accès aux plateformes numériques contemporaines de communications comme Facebook ou encore TikTok. Pour elle, l'usage de Twitter constitue un élément complémentaire de la jouissance du droit à la liberté d'expression¹²⁸, en raison de la place centrale qu'occupent les réseaux sociaux dans la diffusion et la réception des idées¹²⁹. Elle considère que twitter revêt une importance capitale dans l'atteinte des objectifs visés à travers la jouissance du droit à la liberté d'expression¹³⁰. Autrement dit, la Cour de justice

¹²⁶ Voir Abdoul Kader ABOU KOÏNI, « L'influence des décisions de la cour de justice de la CEDEAO en matière de protection des droits de l'homme sur les juridictions des États membres », Communication à la demi-journée des jeunes chercheurs de la SFDI du 17 mars 2023 à l'Université Sorbonne, Paris Nord, en ligne <https://sfdi.org/wp-content/uploads/2024/03/ABOU-KOINI-Abdoul-Kader-Linfluence-des-decisions-de-la-Cour-de-justice-de-la-CEDEAO-en-matiere-de-protection-des-droits-des-droits-de-lhomme-sur-les-juridictions-des-Etats-membres.pdf>, consulté le 10 novembre 2025.

¹²⁷ *Amnesty International Togo & Others c. République togolaise*, op. cit., §38.

¹²⁸ *The registered trustees of the Socio-economic Rights and Accountability Project (SERAP) & Others v. Federal Republic of Nigeria*, op. cit., §67.

¹²⁹ *Ibid.*, §70.

¹³⁰ *Ibid.*, §71.

de la CEDEAO fonde un droit d'accès aux plateformes numériques sur leur fonction, en tant qu'instrument incontournable d'exercice de la liberté d'expression.

d-) L'exigence de la légalité des restrictions

Dans l'affaire *Amnesty International Togo & Others c. République togolaise*, la Cour de justice de la CEDEAO a estimé que l'accès à internet doit être protégé par une loi, qui prévoit l'éventualité d'une ingérence des autorités publiques et les motifs pouvant justifier cette ingérence¹³¹. Cette cour affirme ainsi une obligation positive pour les États d'encadrer, et surtout de protéger l'accès à internet. Dans le même sens, dans l'affaire *ABLOGUI & Others c. État de Guinée*, elle souligne que la liberté d'expression implique pour les États des obligations d'abstention, mais aussi des obligations positives¹³².

Ainsi, toute restriction d'accès à internet ne peut être tolérée qu'en vertu des motifs prévus par une loi¹³³. C'est à cet égard que la Cour de justice de la CEDEAO a constaté que le premier critère du fondement légal de la restriction n'était pas rempli en l'espèce¹³⁴, alors même que l'État de Guinée n'a pas pu l'éclairer sur la justification et le caractère proportionnel de la mesure. Cette dernière précision est importante, parce qu'elle permet de souligner que la condition de la légalité des mesures de restrictions d'accès à internet ne serait pas remplie par la simple existence d'une loi fondant l'État à couper internet. Dans l'hypothèse où il y aurait une loi fondant la restriction, il faudrait encore que la mise en œuvre de la loi satisfasse au test de nécessité et de proportionnalité.

e-) L'exigence de dispositions législatives spécifiques, claires et antérieures

La Cour de justice de la CEDEAO rejette systématiquement les références à des dispositions constitutionnelles ou législatives générales pour justifier une coupure d'internet. Dans l'affaire *SERAP & Others v. Federal Republic of Nigeria*, elle rappelle que la légitimité de l'autorité à exercer le pouvoir de couper Internet¹³⁵ ne peut provenir d'une habilitation générale à légiférer, mais d'une disposition spécifique¹³⁶. Dans la décision *ASUTIC et Monsieur Ndiaga Gueye contre la République du Sénégal*¹³⁷, elle a ainsi estimé que les textes invoqués par l'État du Sénégal pour fonder la coupure d'internet « ne prescrivent ni n'autorisent aucune mesure restrictive spécifique, et encore moins une coupure d'internet et des réseaux »¹³⁸. Faute de base juridique « claire et spécifique »¹³⁹, l'État du Sénégal a violé l'article 15 de la Ch. ADHP et de l'article 6 du PIDESC.

¹³¹ *Amnesty International Togo & Others c. République togolaise*, op. cit., §38.

¹³² *Association Des Blogueurs De Guinée (ABLOGUI) & Others c. État de Guinée*, op. cit., §48.

¹³³ *Ibid.*, §53.

¹³⁴ *Association Des Blogueurs De Guinée (ABLOGUI) & Others c. État de Guinée*, op. cit., §55.

¹³⁵ *Ibid.*, §81.

¹³⁶ *Ibid.*

¹³⁷ *Association des Utilisateurs des Technologies de l'Information et de la Communication (ASUTIC) et Monsieur Ndiaga Gueye contre la République du Sénégal*, op. cit.

¹³⁸ *Ibid.*, §54.

¹³⁹ *Ibid.*, §59.

Dans l'affaire *Amnesty International Togo & Others c. République togolaise*, une précision importante avait déjà été faite par la juridiction communautaire : la loi servant de fondement à une coupure d'internet doit être antérieure à la mesure ¹⁴⁰. Une loi postérieure ne peut ainsi rétroactivement valider une ingérence.

Cette exigence d'antériorité et de spécificité ainsi que les autres exigences posées par la cour pourraient, en outre, engager la responsabilité des fournisseurs d'accès lorsqu'ils n'ont pas pris de mesures conformes à ces exigences.

C-) L'INCIDENCE DE LA SAISINE DU POINT DE CONTACT NATIONAL POUR LES PRINCIPES DIRECTEURS DE L'OCDE

L'analyse concrète des plans de vigilance du groupe Vivendi permet d'éclairer la manière dont ce risque est appréhendé par les entreprises. Le plan de vigilance 2024 du groupe n'évoque aucun risque lié aux coupures d'Internet, alors même que certaines de ses activités concernent directement la fourniture de services d'accès au réseau. Plus significatif encore, ce plan ne mentionne pas la filiale Groupe Vivendi Africa (GVA), pourtant chargée de la gestion des services Internet du groupe sur le continent africain, et se limite à un périmètre centré sur Vivendi SE et certaines de ses entités, telles que Gameloft¹⁴¹.

Une telle limitation du périmètre interroge au regard des exigences de la loi du 27 mars 2017, qui impose que le plan de vigilance couvre l'ensemble des activités de la société mère ainsi que celles des filiales directes et indirectes qu'elle contrôle, au sens de l'article L. 233-16 II du code de commerce¹⁴². À cet égard, la prise en compte effective des activités de GVA dans le dispositif de vigilance apparaît incertaine. Le plan de vigilance 2023 mentionnait certes cette filiale dans son périmètre, mais les risques identifiés en matière de droits humains se limitaient essentiellement à des problématiques internes, telles que la discrimination, le harcèlement des collaborateurs ou encore l'information des consommateurs, sans référence aux risques systémiques liés aux restrictions d'accès au réseau¹⁴³.

Si l'exemple de Vivendi illustre la prise en compte encore limitée du risque d'atteinte aux droits de l'homme lié aux coupures d'Internet par certaines multinationales du numérique¹⁴⁴, la responsabilité de ces dernières à ce titre n'apparaît plus purement théorique. En effet, le 16 mars 2022, l'*Open Society Justice Initiative* (ci-après OSJI) a saisi le Point de contact national autrichien pour les Principes directeurs de l'OCDE à

¹⁴⁰ *Ibid.*, §§39 et s.

¹⁴¹ Extrait du Document d'Enregistrement universel de Vivendi (2024), en ligne <https://www.vivendi.com/wp-content/uploads/2025/05/PLAN-DE-VIGILANCE-2024.pdf>, consulté le 06 novembre 2025.

¹⁴² Larios MAVOUNGOU, « Les pouvoirs privés économiques à l'épreuve de la loi française sur le devoir de vigilance », *Revue internationale de droit économique*, t. XXXIII (1), 2019, p. 55.

¹⁴³ Extrait du Document d'Enregistrement universel de Vivendi (2023), pp. 102-105, en ligne https://www.vivendi.com/wp-content/uploads/2024/03/20240322_VIV_Plan-de-vigilance-VIVENDI DEU FR 2023 .pdf, consulté le 06 novembre 2025.

¹⁴⁴ *Coupures de l'accès à Internet : tendances, causes, implications juridiques et conséquences sur une série de droits de l'homme*, Rapport du Haut-Commissariat des Nations Unies aux droits de l'homme, *op. cit.*, p. 14.

l'intention des entreprises multinationales¹⁴⁵ d'une plainte dirigée contre *Telekom Austria AG* et sa filiale *A1 Belarus*, au motif que l'entreprise aurait participé à plusieurs coupures de l'internet mobile en Biélorussie entre le 9 août et le 29 novembre 2020¹⁴⁶. Les griefs invoqués portaient notamment sur les atteintes aux droits humains (liberté d'expression, de réunion et d'association), l'insuffisance des mesures de diligence raisonnable ainsi que l'absence de mécanismes destinés à prévenir ou atténuer les effets des coupures. Le PCN ayant jugé la circonstance spécifique recevable, les entreprises mises en cause ont finalement accepté de coopérer avec l'OSJI pour la mise en œuvre des Principes directeurs de l'OCDE¹⁴⁷. Sans constituer une reconnaissance juridictionnelle de responsabilité, cette affaire témoigne néanmoins de l'importance croissante accordée par les parties prenantes aux risques numériques liés aux coupures d'internet et de leur intégration progressive dans le champ des obligations de vigilance. Elle montre surtout que les FAI et ORM peuvent être directement mis en cause en raison de leur participation à des mesures de restriction d'accès au réseau.

En tout état de cause, dans le cadre de la loi sur le devoir de vigilance, l'article L.225-102-5 du code de commerce prévoit qu'en cas de manquement aux exigences de vigilance établies à l'article L.225-102-4, la société engage sa responsabilité délictuelle pour la réparation du préjudice qu'une mise en conformité aurait permis d'éviter. Or, l'existence d'un dommage causé par des coupures d'internet à motifs politiques paraît difficilement contestable, compte tenu de leurs effets sur les activités économiques, l'accès aux services essentiels, les investissements ou encore les capacités de travail¹⁴⁸. L'impact préjudiciable des coupures est mis en exergue en particulier dans les affaires *Association des Utilisateurs des Technologies de l'Information et de la Communication (ASUTIC) et Monsieur Ndiaga Gueye contre la République du Sénégal*¹⁴⁹ et *Association Des Blogueurs De Guinée (ABLOGUI) & Others c. État de Guinée*¹⁵⁰ devant la Cour de justice de la CEDEAO. Si la Cour a, dans ces affaires, réduit ou rejeté les demandes d'indemnisation faute de

¹⁴⁵ Les Principes directeurs s'appuient sur les Points de contact nationaux (PCN), chargés d'en renforcer l'effectivité par des actions de promotion, la réponse aux demandes d'information et la résolution des difficultés liées à leur mise en œuvre, conformément aux Lignes directrices de procédure. Ils sont en outre complétés par des commentaires et divers guides d'interprétation.

¹⁴⁶ Point de Contact National de l'Autriche pour les Principes directeurs de l'OCDE à l'intention des entreprises multinationales, *The Open Society Justice Initiative & Telekom Austria AG*, Initial Assessment, 1^{er} août 2023, en ligne, <https://www.oecd.org/en/networks/national-contact-points-for-responsible-business-conduct/database/at0006.html>, consulté le 07 août 2025.

¹⁴⁷ Point de Contact National de l'Autriche pour les Principes directeurs de l'OCDE à l'intention des entreprises multinationales, *The Open Society Justice Initiative & Telekom Austria AG*, Final Statement, 25 juillet 2024, en ligne, <https://www.oecd.org/en/networks/national-contact-points-for-responsible-business-conduct/database/at0006.html>, consulté le 07 août 2025.

¹⁴⁸ *Coupures de l'accès à Internet : tendances, causes, implications juridiques et conséquences sur une série de droits de l'homme*, Rapport du Haut-Commissariat des Nations Unies aux droits de l'homme, *op. cit.*, pp. 10 et s.

¹⁴⁹ *Association des Utilisateurs des Technologies de l'Information et de la Communication (ASUTIC) et Monsieur Ndiaga Gueye contre la République du Sénégal*, *op. cit.*, §76.

¹⁵⁰ Cour de justice de la CEDEAO, arrêt du 31 octobre 2023, *Association Des Blogueurs De Guinée (ABLOGUI) & Others c. État de Guinée*, *op. cit.*, §85.

justification suffisante, elle a néanmoins reconnu l'existence d'un préjudice résultant des restrictions litigieuses.

La mise en œuvre de la responsabilité civile des entreprises demeure toutefois incertaine, notamment au regard de la caractérisation de la faute. Celle-ci pourrait néanmoins résulter d'un plan de vigilance lacunaire, insuffisamment mis en œuvre ou ne prévoyant pas de mesures raisonnables¹⁵¹ de mitigation du risque de coupure d'internet, notamment lorsqu'il ne tient pas compte du contexte local ou des standards dégagés par les juridictions régionales compétentes. À cet égard, certaines pratiques d'entreprises témoignent déjà de formes de vigilance accrues. Ainsi, la SONATEL a contesté en référé devant les juridictions sénégalaises des réquisitions administratives imposant des restrictions d'accès à internet en 2024¹⁵².

Par ailleurs, le principal défi soulevé par les coupures d'internet réside dans les situations d'obligations contradictoires auxquelles sont confrontées les entreprises multinationales, placées devant le dilemme de rester ou de quitter des États à risque. Dans ce sens, *Telekom Austria AG* soutenait devant le PCN autrichien qu'elle respectait les droits humains dans la mesure du possible et s'efforçait d'atténuer les effets négatifs lorsque la législation nationale l'empêchait d'agir autrement. L'entreprise invoquait également les contraintes politiques locales auxquelles elle était confrontée. Ces arguments traduisent les tensions auxquelles sont exposés les FAI et ORM opérant dans des environnements où les autorités publiques recourent fréquemment aux restrictions d'accès au réseau. Quoi qu'il en soit, le Principe 4 de la Déclaration africaine sur la liberté d'expression et l'accès à l'information rappelle que le droit le plus favorable à l'exercice des libertés fondamentales doit prévaloir en cas de conflit de normes.

La réalité du risque d'atteinte aux droits de l'homme du fait des coupures d'internet apparaît aujourd'hui difficilement contestable. En revanche, l'existence d'une obligation juridiquement stabilisée imposant aux entreprises une vigilance spécifique en la matière doit être appréhendée avec davantage de nuance.

D'une part, le droit d'accès à internet demeure principalement garanti de manière indirecte, à travers des droits préexistants, en particulier la liberté d'expression. D'autre part, malgré les avancées notables de certaines juridictions régionales, notamment la Cour de justice de la CEDEAO, ce droit ne bénéficie pas encore d'une autonomie pleinement consacrée en droit international positif.

Pour autant, les dynamiques normatives et jurisprudentielles étudiées révèlent une évolution significative du cadre applicable aux entreprises numériques. Les instruments internationaux, les standards de diligence raisonnable, les initiatives privées, ainsi que les jurisprudences régionales convergent progressivement vers une prise en compte accrue des risques liés aux coupures d'internet. À cet égard, la jurisprudence de la Cour de justice

¹⁵¹ Voir Lucas D'AMBROSIO, « Le devoir de vigilance : une innovation juridique entre continuités et ruptures », *Droit et société*, 106 (3), p. 645.

¹⁵² Cour suprême Sénégal, ordonnance n° 5 du 22 février 2024, *SONATEL SA*, n° J/044/RG/24.

de la CEDEAO joue un rôle structurant, en raison notamment du contexte ouest-africain marqué par la récurrence des restrictions d'accès au réseau pour des motifs politiques.

Sans permettre encore d'affirmer l'existence d'une obligation autonome et générale de prévention des coupures d'internet pesant sur les entreprises, ces évolutions suffisent néanmoins à objectiver un risque identifiable d'atteinte grave aux droits de l'homme. Dans ce contexte, les entreprises soumises à une obligation de vigilance, en particulier les FAI et ORM intervenant dans des États exposés à ce type de pratiques, ne peuvent raisonnablement ignorer ce risque dans l'élaboration et la mise en œuvre de leurs dispositifs de vigilance.