Application des règles sur les contenus illicites et la désinformation en ligne

IRIS

Une publication
de l'Observatoire européen de l'audiovisuel

Observatoire européen de l'audiovisuel

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

IRIS-6
Application des règles sur les contenus illicites et la désinformation en ligne
Observatoire européen de l'audiovisuel, Strasbourg, 2025
ISSN 2079-1062

Directrice de publication – Pauline Durand-Vialle, Directrice exécutive
Supervision éditoriale – Maja Cappello, Responsable du Département Informations juridiques
Observatoire européen de l'audiovisuel

Équipe éditoriale – Sophie Valais et Diego de la Vega
Observatoire européen de l'audiovisuel

Auteur (en ordre alphabétique)
Irène Bouhadana, Mark D. Cole, Roderick Flynn, William Gilles, Giovanni de Gregorio, Mariette Jones, Mehmet Bedii Kaya, Dariia Opryshko, Roxana Radu, Clara Rauchegger, Sandra Schmitz-Berndt, Krzysztof Wojciechowski

Traduction
Erwin Rohwer, Marco Polo Sarl, Anne-Lise Weidmann, Ulrike Welsche

Relecture
Linda Byrne, Aurélie Courtinat, Catherine Koleda, Udo Lücke, Sonja Schmidt

Assistante éditoriale – Alexandra Ross
Presse et relations publiques – Alison Hindhaugh, alison.hindhaugh@coe.int
Observatoire européen de l'audiovisuel

Éditeur
Observatoire européen de l'audiovisuel
76, allée de la Robertsau, 67000 Strasbourg, France
Tél.: +33 (0)3 90 21 60 00
iris.obs@coe.int
www.obs.coe.int

Maquette de couverture – ALTRAN, France

Veuillez citer cette publication comme suit :
Cappello M. (ed.), *Application des règles sur les contenus illicites et la désinformation en ligne*, IRIS, Observatoire européen de l'audiovisuel, Strasbourg, décembre 2025

Application des règles sur les contenus illicites et la désinformation en ligne

Irène Bouhadana, Mark D. Cole, Roderick Flynn, William Gilles, Giovanni de Gregorio, Mariette Jones, Mehmet Bedii Kaya, Dariia Opryshko, Roxana Radu, Clara Rauchegger, Sandra Schmitz-Berndt et Krzysztof Wojciechowski

Observatoire européen de l'audiovisuel

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Avant-propos

« La liberté absolue raille la justice. La justice absolue nie la liberté. Pour être fécondes, les deux notions doivent trouver, l'une dans l'autre, leur limite[1]. » Albert Camus écrit ces mots dans *L'Homme révolté*, un essai publié en 1951, soit quelques années seulement après la Seconde Guerre mondiale et la Shoah. Ce faisant, il suscite bien des remous parmi ce qu'il est convenu d'appeler le milieu intellectuel de son temps, pour sa critique des mouvements révolutionnaires et de leurs excès.

Un demi-siècle plus tard, internet, une autre de ces révolutions prônant la liberté absolue, a immanquablement entraîné son lot d'excès, dont nous payons le prix aujourd'hui et que nous continuons de combattre.

Cependant, comme l'affirme Camus, il n'est pas possible de juxtaposer en opposition la justice absolue et la liberté absolue. Pour être fécondes, ces deux notions doivent au contraire atteindre un équilibre.

Celle de la liberté d'expression trouve ses limites dans les intérêts de la sécurité nationale, de l'intégrité territoriale ou de la sûreté publique, de la défense de l'ordre et de la prévention du crime, de la protection de la santé ou de la morale, de la protection de la réputation ou des droits d'autrui, ainsi que là où il faut empêcher la divulgation d'informations confidentielles, ou encore garantir l'autorité et l'impartialité du pouvoir judiciaire. Les restrictions en la matière doivent toutefois être prévues par la loi et constituer des mesures nécessaires dans une société démocratique.

Certains contenus en ligne peuvent être considérés comme illégaux en tant que tels et doivent par conséquent être retirés par l'auteur ou l'éditeur, soit volontairement, soit sous la contrainte d'une décision administrative ou judiciaire. Si les modalités pour ce faire sont parfois complexes, il s'agit simplement à ce stade de faire appliquer la loi. Le point épineux concerne plutôt les contenus préjudiciables. Ainsi que l'expliquent les auteurs de la présente publication, le terme désigne « les contenus qui ne sont pas nécessairement illicites mais qui sont néanmoins jugés préjudiciables pour les individus ou la société - par exemple, la désinformation, les informations sanitaires inexactes ou les contenus qui portent atteinte aux processus démocratiques ». La question est dès lors de savoir comment lutter contre des contenus qui, n'étant pas illégaux, ne sont donc pas limités par la loi. *Aïe, voilà bien le souci*.[2]

Ce rapport a été élaboré en collaboration avec l'Institut européen du droit des médias (EMR) et différents experts de ce domaine complexe. L'application des dispositions permettant de lutter contre les contenus illégaux et la désinformation en ligne y est abordée dans toutes ses dimensions. À partir du cadre général de l'Union européenne et du

[1] Camus, A., *L'Homme révolté*, Gallimard, Folio essais, 1951, p. 363.
[2] Shakespeare, W., « *Ay, there's the rub* », *Hamlet*. Traduction par Bill Kredenster, 2015.

Conseil de l'Europe, et de la réglementation de base concernant les plateformes, la présente publication analyse en détail des exemples nationaux provenant de toute l'Europe qui illustrent la situation actuelle en la matière.

Je tiens à remercier chaleureusement les autrices et auteurs qui ont participé à ce rapport pour leur engagement et la qualité de leur travail (par ordre des contributions) : Mark D. Cole, Sandra Schmitz-Berndt, Roxana Radu, William Gilles, Irène Bouhadana, Dariia Opryshko, Mehmet Bedii Kaya, Roderick Flynn, Clara Rauchegger, Giovanni de Gregorio, Krzysztof Wojciechowski et Mariette Jones.

Sans vouloir préjuger des conclusions de ce passionnant rapport, je conclurai par une réflexion personnelle. La réglementation de l'environnement en ligne peut parfois donner l'impression d'être une tâche surhumaine et, de fait, il reste tant à faire. Ne perdons pas espoir, cependant, car pour citer à nouveau Albert Camus, « on appelle surhumaines les tâches que les hommes mettent longtemps à accomplir, voilà tout[3] ».

Très bonne lecture !

Bonne lecture !

Maja Cappello

Coordinatrice IRIS

Responsable du Département Informations juridiques

Observatoire européen de l'audiovisuel

[3] Camus, A., *L'Été*, 1954, Quarto Gallimard, Œuvres, 2013.

Observatoire européen de l'audiovisuel

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Table des matières

Observatoire européen de l'audiovisuel

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Observatoire européen de l'audiovisuel

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Observatoire européen de l'audiovisuel
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Liste d'abréviations et acronymes

AEP	*Autoritatea Electorală Permanentă* (Autorité électorale permanente, Roumanie)
AGCOM	*Autorità per le Garanzie nelle Comunicazioni* (Autorité de régulation des communications, Italie)
ANCOM	*Autoritatea Națională pentru Administrare și Reglementare în Comunicații* (Autorité national pour l'administration et la régulation des communication, Roumanie)
APCE	Assemblée Parlementaire du Conseil de l'Europe
API	Interfaces de programmation d'applications
ARCOM	Autorité de régulation de la communication audiovisuelle et numérique (France)
AS	Systèmes autonomes
ASA	*Advertising Standard Authority* (Autorité des normes publicitaires, Royaume-Uni)
BAI	*Broadcasting Authority of Ireland*
BGH	*Bundesgerichsthof* (Cour fédérale de justice, Allemagne)
BKA	*Bundeskriminalamt* (Office fédéral de la police judiciaire. Allemagne)
BNetzA	*Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen* (Agence fédérale des réseaux pour l'électricité, le gaz, les télécommunications, la poste et les chemins de fer, Allemagne)BTK *Bilgi Teknolojileri ve İletişim Kurumu* (Autorité des technologies de l'information et de la communication, Türkiye)
CAP	*Committee of Advertising Practice* (Commission des pratiques publicitaires, Irlande)
CEPD	Comité européen de la protection des données
CJUE	Cour de Justice de l'Union Européenne
CM/Rec	Recommandation du Comité des Ministres
CNA	*Consiliul Național al Audiovizualului* (Conseil National de l'Audiovisuel, Roumanie)
CnaM	*Coimisiún na Meán* (Commission des médias, Irlande)
DDG	*Digitale-Dienste-Gesetz* (Loi sur les services numérique, Allemagne)
DMA	Règlement sur les marchés numériques
DSA	Règlement sur les services numériques

Observatoire européen de l'audiovisuel

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

DSC	Coordinateur pour les services numériques
EBDS	Comité européen des services numériques
EBMS	Comité européen des services de médias
EDMO	Observatoire européen des médias numériques
EEE	Espace Economique européen
EFCSN	Réseau européen des normes de vérification des faits
EMFA	Règlement européen sur la liberté des médias
EMR	Institut européen du droit des médias
ERGA	Groupe des régulateurs européens pour les services de médias audiovisuels
FIMI	Manipulation de l'information et d'ingérence menées depuis l'étranger
FIMI-ISAC	Centre de partage et d'analyse de l'information consacré aux activités de manipulation de l'information et d'ingérence menées depuis l'étranger
FSI	Fournisseurs de services internet
IA	Intelligence Artificielle
JMStV	*Jugendmedienschutz-Staatsvertrag* (Traité d'État sur la protection de la jeunesse dans les medias, Allemagne)
LUM	Loi sur les médias (Ukraine)
MStV	*Medienstaatsvertrag* (Traité d'État sur les media, Allemagne)
NCCC	Centre national de coordination de la cybersécurité (Ukraine)
NCU	Centre national de gestion opérationnelle et technique des réseaux de télécommunications (Ukraine)
NetzDG	*Netzwerkdurchsetzungsgesetz* (loi relative à l'application du droit sur les réseaux sociaux, Allemagne)
NSDC	Conseil national de sécurité et de défense (Ukraine)
OSA	*Online Safety Act* (Loi sur la sécurité en ligne, Royaume-Uni)
OSMR	*Online Safety and Media Regulation Act* (Loi sur la sécurité en ligne et la régulation des medias, Irelande)
PERCI	Plateforme Européenne de Retraits de Contenus illégaux sur Internet
PEReN	Pôle d'Expertise de la Régulation Numérique
PESC	Politique Étrangère et de Sécurité Commune
PIDCP	Pacte International relatif aux Droits Civils et Politiques
RGPD	Règlement Général sur la Protection des Données

Observatoire européen de l'audiovisuel

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

SEAE	Service Européen pour l'Action Extérieure
SMA	Services de Médias Audiovisuels
StGB	*Strafgesetzbuch* (Code pénal, Allemagne ou Autriche)
TERREG	Règlement sur les contenus à caractère terroristeTFUE Traité sur le Fonctionnement de l'Union européenne
TGMR	Très Grands Moteurs de Recherche
TGP	Très Grandes Plateformes
TTPA	Règlement relatif à la transparence et au ciblage de la publicité à caractère politique
TUE	Traité sur l'Union européenne
TUSMA	*Testo Unico sui Servizi di Media Audiovisivi* (Code consolidé des services de médias audiovisuels, Italie)
UE	Union EuropéenneUKE *Urząd Komunikacji Elektronicznej* (Office des communications électroniques, Pologne)
URL	Localisateur uniforme de resource
UŚUDE	*Ustawa o świadczeniu usług drogą elektroniczną* (Loi relative à la prestation de services par voie électronique, Pologne)
VIGINUM	Service de vigilance et de protection contre les ingérences numériques étrangères
VLOP	Très grandes plateformes en ligne
VLOSE	Très grands moteurs de recherche en ligne
VPN	Services de colocation et les réseaux privés virtuels
VPS	Serveurs privés virtuels
VSP	Service de vidéo à la demande
VwVG	*Verwaltungsvollstreckungsgesetz* (loi sur l'exécution administrative, Allemagne)
ZMI	Cellule centrale de signalement des contenus répréhensibles sur internet

Résumé

Cette nouvelle publication *IRIS* propose une analyse complète de l'application actuelle des réglementations européennes relatives aux contenus illicites et à la désinformation en ligne. Douze éminents auteurs[4], experts dans leurs domaines respectifs, ont contribué à la rédaction de chacun de ces chapitres qui explorent, tant au niveau européen que national, la manière dont les cadres réglementaires peuvent permettre l'application des dispositions en vigueur.

Ce rapport présente non seulement le point de vue de l'Union européenne et du Conseil de l'Europe, mais offre également divers exemples nationaux qui permettent de mieux comprendre les mesures prises à l'heure actuelle en Europe pour répondre à cette question essentielle.

Le **chapitre 1**, rédigé par Mark D. Cole et Sandra Schmitz-Berndt, s'intéresse à la manière dont les plateformes numériques sont à la fois de puissants outils d'expression et une source particulière de risques du fait de leur pouvoir sur le marché, de leur portée et de l'absence de contrôle éditorial. Il examine également les différences entre les contenus illicites et la désinformation en ligne, en explorant les aspects juridiques de chaque notion, leur diffusion et les nuances qui peuvent être observées dans divers pays européens.

Le **chapitre 2** explore le cadre législatif relatif à la régulation des contenus et les mesures d'application prévues au niveau européen. La première partie, rédigée par Sandra Schmitz-Berndt, analyse les mesures d'application et le socle des droits fondamentaux du Conseil de l'Europe, en tenant compte non seulement des différentes recommandations formulées par l'institution et des résolutions de l'Assemblée parlementaire du Conseil de l'Europe, mais également de la jurisprudence de la Cour européenne des droits de l'homme.

En partant du principe selon lequel internet joue un rôle majeur dans l'exercice du droit à la liberté d'expression, l'auteure analyse la responsabilité des portails en ligne, ainsi que les devoirs et responsabilités des intermédiaires d'internet, des entités non professionnelles et des créateurs de liens hypertextes pour des contenus illicites publiés par des tiers. Elle examine également les différentes mesures coercitives prévues par la jurisprudence de la Cour, comme le blocage de l'accès à des sites web ou à des comptes sur les réseaux sociaux.

La deuxième partie présente le cadre réglementaire applicable aux contenus et les mesures coercitives prises au niveau de l'Union européenne, en particulier dans le droit primaire et au titre de la politique étrangère et de sécurité commune (PESC), ainsi qu'en

[4] Par ordre alphabétique : Irène Bouhadana, Mark D. Cole, Roderick Flynn, William Gilles, Giovanni de Gregorio, Mariette Jones, Mehmet Bedii Kaya, Dariia Opryshko, Roxana Radu, Clara Rauchegger, Sandra Schmitz-Berndt et Krzysztof Wojciechowski.

matière de manipulation de l'information et d'ingérence étrangères (FIMI). Ce chapitre passe également en revue d'autres outils élaborés par l'Union européenne pour lutter contre les contenus illicites et la désinformation.

Dans le **chapitre 3**, Mark D. Cole examine les mesures coercitives prises au niveau de l'UE pour lutter contre la désinformation et se concentre sur la désinformation orchestrée par des États, qui illustre l'intensification et l'ampleur des campagnes de désinformation au sein de l'Union européenne. L'auteur analyse également diverses initiatives européennes, telles que le Code de conduite sur la désinformation de l'UE et ses liens avec le Règlement sur les services numériques (DSA), et passe en revue des outils tels que la vérification des faits et le recours à des signaleurs de confiance dans l'environnement numérique.

Ce chapitre comporte une partie rédigée par Roxana Radu et consacrée à la Roumanie, qui analyse le cadre national applicable aux plateformes, les dispositions spécifiques en matière de désinformation et le cas particulier de l'annulation de l'élection présidentielle roumaine de 2024, où la désinformation a joué un rôle déterminant dans la manipulation du processus électoral, en tirant parti des profondes vulnérabilités structurelles du pays, notamment l'instabilité politique, l'incertitude économique et la polarisation de la société. William Gilles et Irène Bouhadana s'intéressent à l'exemple français, depuis le cadre législatif national applicable aux plateformes, défini par la jurisprudence constitutionnelle, jusqu'aux dispositions spécifiques en matière de désinformation et leur application au cas des récentes élections.

Dans ce même chapitre, Dariia Opryshko dresse un état des lieux de la situation en Ukraine, et examine le cadre législatif national applicable aux plateformes ainsi que la nouvelle loi ukrainienne relative aux médias. Elle étudie les dispositions spécifiques instaurées par cette loi en matière de désinformation et leur application en cas d'ingérence étrangère sous forme de désinformation dans un contexte de guerre. Le chapitre explore également la manière dont l'absence de mécanismes efficaces pour lutter contre l'influence des plateformes en ligne étrangères et protéger les intérêts nationaux a conduit à un blocage généralisé des sites web et des plateformes en ligne.

Dans le **chapitre 4,** Mark D. Cole se concentre sur l'accessibilité des contenus terroristes et les mesures prises pour lutter contre ce phénomène sous l'angle du règlement relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne (TCOR), qui prévoit des « injonctions de retrait » et habilite les autorités compétentes à émettre de telles injonctions qui exigent des fournisseurs d'hébergement qu'ils retirent les contenus à caractère terroriste ou en bloquent l'accès dans tous les États membres de l'UE.

Dans ce même chapitre, Sandra Schmitz-Berndt présente le dispositif allemand en vigueur applicable aux plateformes, tout en mentionnant la *Netzwerkdurchsetzungsgesetz* (loi relative à l'application du droit sur les réseaux sociaux – NetzDG), désormais abrogée, et ses principes qui ont inspiré le DSA. La NetzDG établissait déjà une liste des infractions pénales qui constituaient des « contenus illicites » et imposait aux fournisseurs de réseaux sociaux l'obligation de mettre en place une procédure efficace et transparente pour le traitement des plaintes relatives à ces contenus illicites. Le chapitre examine également les dispositions allemandes spécifiquement applicables aux contenus à caractère terroriste.

Mehmet Bedii Kaya analyse la situation en Türkiye, en présentant une vue d'ensemble du cadre législatif national applicable aux plateformes dans le contexte de l'adhésion de la Türkiye au Conseil de l'Europe et de sa candidature à l'Union européenne. Comme l'explique l'auteur, les autorités turques ont mis en place une infrastructure réglementaire complète qui vise à préserver l'ordre public dans les domaines physique et numérique, ainsi que certaines dispositions spécifiquement applicables aux contenus à caractère terroriste.

Dans le **chapitre 5**, Mark D. Cole met l'accent sur la lutte contre les propos diffamatoires, les discours de haine et l'incitation à la violence, sous l'angle de l'application de la réglementation au niveau de l'UE. Parallèlement à cette analyse, Roderick Flynn examine le régime irlandais applicable aux plateformes en ligne et le rôle de la nouvelle autorité de régulation des médias, la *Coimisiún na Meán* (CnaM). L'auteur analyse le processus d'application du DSA dans ce domaine et les dispositions spécifiques en matière de propos diffamatoires, de discours de haine et d'incitation à la violence, ainsi que le code irlandais de sécurité en ligne.

Clara Rauchegger présente la situation en Autriche, et plus particulièrement la loi autrichienne relative aux plateformes de communication et la jurisprudence de la Cour de justice de l'Union européenne qui en découle, ainsi que son influence sur l'interprétation du DSA. Elle examine également l'application du dispositif autrichien dans les affaires de cyberharcèlement et d'abus sexuels par le biais d'images.

Giovanni de Gregorio cite l'exemple de l'Italie, et décrit les mécanismes nationaux mis en place pour faire respecter les dispositions du DSA, les mesures spécifiques relatives aux propos diffamatoires, aux discours de haine et à l'incitation à la violence, ainsi que le rôle joué par le *Codice Penale* (code pénal italien). L'auteur présente également les mécanismes d'application judiciaire en vigueur et analyse les défis qui restent à relever dans ce domaine.

Dans le **chapitre 6**, Mark D. Cole aborde d'autres catégories de contenus préjudiciables, et plus particulièrement les contenus qui ne sont pas nécessairement illicites, mais qui peuvent néanmoins faire l'objet de restrictions d'accès pour certains publics, comme les mineurs, dans la mesure où ces contenus peuvent leur être préjudiciables, surtout s'ils sont diffusés au moyen de supports audiovisuels.

Dans ce chapitre, Krzysztof Wojciechowski analyse en détail le cas de la Pologne et ses récentes réformes en matière de contenus préjudiciables, ainsi que les difficultés rencontrées sur le plan législatif et judiciaire pour traiter cette question complexe.

Mariette Jones dresse un état des lieux de la situation au Royaume-Uni, notamment en ce qui concerne la loi britannique relative à la sécurité en ligne (*Online Safety Act* – OSA), entrée en vigueur en septembre 2023, qui oblige les entreprises privées à surveiller, évaluer et supprimer systématiquement les contenus préjudiciables créés par des tiers et à prendre des mesures pour protéger les mineurs contre ces contenus, par exemple en améliorant les systèmes de vérification de l'âge. Cette partie aborde également la question des jeux d'argent et de hasard en ligne.

Enfin, dans le **chapitre 7**, Mark D. Cole et Sandra Schmitz-Berndt dressent une analyse comparative des études de cas présentées dans les rapports nationaux, et mettent en évidence les disparités dans l'application de la réglementation aux intermédiaires

d'internet en Europe. Bien que la législation européenne ait permis une forte harmonisation directement contraignante pour ses États membres, des divergences persistent dans l'application de la réglementation aux intermédiaires d'internet à travers l'Europe.

1. Introduction et vue d'ensemble

Dr Mark Cole, directeur des affaires académiques de l'Institut européen du droit des médias (EMR) et professeur en droit des médias et des télécommunications à l'Université du Luxembourg, et Dr Sandra Schmitz-Berndt, chercheuse associée à l'Institut européen du droit des médias (EMR)

À l'ère du numérique, internet constitue un « outil sans précédent d'exercice de la liberté d'expression »[5] et est devenu un « outil essentiel pour la participation à des activités et des discussions concernant des questions politiques et des débats d'intérêt général »[6]. Il joue par conséquent un rôle majeur dans l'amélioration de l'accès du public à l'actualité et, plus généralement, facilite la diffusion de l'information en temps réel et à l'échelle mondiale[7]. L'évolution du réseau internet a notamment été caractérisée par un profond basculement d'un outil statique de recherche d'informations à un espace participatif dynamique qui permet à chacun de créer, de partager et d'interagir avec des contenus à une nouvelle échelle et avec une potentielle couverture mondiale.

À ses débuts, internet se caractérisait principalement par une communication unidirectionnelle (Web 1.0), où les utilisateurs consommaient des informations fournies par un nombre limité de sources. Cette situation signifiait également que la source d'un contenu illicite, c'est-à-dire la personne à l'origine du contenu litigieux ou au moins celle responsable d'un site web bien précis, pouvait être identifiée et, en principe, être tenue pour responsable de l'infraction. Bien évidemment, la dimension « sans frontières » d'internet posait déjà à cette époque un certain nombre de défis qui subsistent aujourd'hui : l'identification de la personne ou de l'entité contre laquelle on souhaite faire appliquer la loi, les questions de compétence juridictionnelle, l'applicabilité du droit national et, pour finir, l'application de la législation dans les affaires transfrontalières[8]. Au fil du temps, le développement des technologies Web 2.0 dans le secteur des communications

[5] *Delfi As c. Estonie [GC]*, requête n° 64569/09 (CEDH, 16 juin 2015), paragraphe 110 ; *Times Newspapers Ltd (nos 1 et 2) c. Royaume-Uni*, requêtes n° 3002/03 et n° 23676/03 (CEDH, 10 mars 2009), paragraphe 27 ; et *Ahmet Yildirim c. Turquie*, requête n° 3111/10 (CEDH, 18 décembre 2012), paragraphe 48.

[6] *Sanchez c. France [GC]*, requête n° 45581/15 (CEDH, 15 mai 2023), paragraphe 158, qui renvoie à l'arrêt *Vladimir Kharitonov c. Russie*, requête n° 10795/14 (CEDH, 23 juin 2020), paragraphe 33, et à l'arrêt *Melike c. Turquie*, requête n° 35786/19 (CEDH, 15 juin 2021), paragraphe 44.

[7] *Sanchez c. France [GC]*, *op. cit*, paragraphe 159 ; *Delfi As c. Estonie [GC]*, *op. cit.*, paragraphe 133.

[8] Voir C. Reed, *Making Laws for Cyberspace*, Oxford University Press, Oxford, 2012, p. 49 et suiv. ; M. D. Cole, C. Etteldorf et C. Ullrich, *Cross-Border Dissemination of Online Content*, *Bd. 81 Schriftenreihe Medienforschung*, Nomos, Baden-Baden, 2021, p. 221 et suiv. ; M. D. Cole et C. Etteldorf, *Future Regulation of Cross-Border Audiovisual Content Dissemination*, *Bd. 83 Schriftenreihe Medienforschung*, Nomos, Baden-Baden, 2023, p. 85 et suiv. ; J. Ukrow, « Le cadre d'application de la loi à l'encontre des fournisseurs de contenu en ligne et étrangers » in M. Cappello (sous la direction de), L'application du droit des médias sans frontières, *IRIS Spécial*, Observatoire européen de l'audiovisuel, Strasbourg, 2018, p. 9 et suiv.

bidirectionnelles et des plateformes de médias sociaux au début des années 2000 a transformé internet en un environnement interactif qui permet aux simples utilisateurs de devenir des créateurs de contenus, des commentateurs et des fondateurs de communautés. Ce tournant vers la vie participative a démocratisé le discours public[9], en permettant à des voix diverses de contribuer aux débats politiques, culturels et sociaux qui étaient autrefois largement dominés par les médias traditionnels et les acteurs institutionnels[10]. Cette évolution a également favorisé de nouvelles formes d'engagement civique, de militantisme et d'échange d'informations, ce qui a renforcé le rôle fondamental que tient internet dans la vie démocratique moderne.

Bien que la philosophie du Web 2.0 reposait en principe sur l'ouverture, la participation et l'innovation décentralisée, cette structure participative a été largement dominée par quelques grandes plateformes en ligne. En effet, l'émergence des plateformes comme acteurs majeurs de l'écosystème numérique a radicalement transformé la manière dont l'information est produite, distribuée et consommée, leur conférant ainsi un véritable rôle de contrôleur d'accès de la sphère publique en ligne. Tout en continuant à faciliter la participation, les plateformes, en tant que modèles commerciaux fondés sur les données, se lancent de plus en plus dans la curation algorithmique des contenus et déterminent ainsi lesquels seront vus, partagés, voire supprimés. Par conséquent, leur ancien statut de simples intermédiaires passifs qui hébergent des contenus de tiers devient de plus en plus flou et, dans certains cas, elles assument un rôle bien plus actif, ce qui implique que les modèles en matière de responsabilité qui étaient apparus sous le Web 2.0 sont aujourd'hui remis en question[11]. L'ingérence croissante dans les contenus soulève de nouvelles interrogations quant à la transparence, la responsabilité et la protection des droits fondamentaux dans le monde numérique. Compte tenu du pouvoir de contrôle exercé par les plateformes, de nouveaux mécanismes d'application de la loi qui visent à supprimer et à empêcher l'accès à des contenus illicites et préjudiciables sont en train d'émerger, ce que d'aucuns ont critiqué, comme le propriétaire de X, Elon Musk, qui a affirmé qu'il s'agissait d'une « censure de la liberté d'expression »[12].

Il convient de préciser que les caractéristiques mêmes qui font des plateformes numériques de puissants outils d'expression - facilité, rapidité, portée et pérennité - les distinguent également des formes traditionnelles de médias. Des risques inédits du fait de leur poids sur le marché, de leur étendue et de l'absence de contrôle éditorial en découlent. Les contenus préjudiciables ou illicites peuvent être « diffusés comme jamais auparavant,

[9] Voir Rowland D., Kohl U. et Charlesworth A., *Information Technology Law*, Routledge Abingdon, 5e éd. 2017, pp. 9 suiv.
[10] Voir *Sanchez c. France [GC]*, *op. cit*, paragraphe 159 ; *Delfi As c. Estonie [GC]*, *op. cit.*, paragraphe 133.
[11] M. D. Cole, C. Etteldorf et C. Ullrich, *Cross-Border Dissemination of Online Content*, *op. cit.*, p. 41 et suiv.
[12] Voir la déclaration d'Elon Musk sur X du 12 juillet 2024. Dans le même esprit, le Gouvernement américain en place envisage des sanctions à l'encontre des responsables de l'UE ou des États membres chargés de la mise en œuvre du DSA, voir H. Pamuk, « *Exclusive: Trump Administration Weighs Sanctions on Officials Implementing EU Tech Law, Sources Say* », Reuters, 26 août 2025. De même, le vice-président américain J.D. Vance a accusé les responsables politiques de l'UE de censurer la liberté d'expression lors de son discours à la Conférence sur la sécurité de Munich, voir N. Bose et D. Chiacu, « *In Munich, Vance Accuses European Politicians of Censoring Free Speech* », Reuters, 14 février 2025.

dans le monde entier, en quelques secondes »[13], et peuvent demeurer accessibles en ligne indéfiniment. Il est donc primordial que les fournisseurs de plateformes, ainsi que tout fournisseur de services intermédiaires, adoptent un comportement responsable et diligent pour que l'environnement en ligne soit sûr, prévisible et digne de confiance, et pour permettre aux utilisateurs d'exercer leurs droits fondamentaux tels que garantis dans les instruments internationaux de protection de ces droits, notamment la liberté d'expression et la liberté d'information, la liberté d'entreprise, le droit à la non-discrimination et la garantie d'un niveau élevé de protection des consommateurs[14]. Les dispositions relatives aux contenus illicites et préjudiciables ne doivent toutefois pas se concentrer uniquement sur les plateformes ; elles doivent également tenir compte du large éventail d'acteurs qui exercent diverses fonctions dans la création, la diffusion et la modération de contenus. Les cadres juridiques et normatifs ont pris un certain retard par rapport au défi relativement complexe que représente la protection des droits fondamentaux et des intérêts de la société dans le cyberespace. Il n'existe, à l'échelle mondiale, que peu de solutions pour lutter efficacement contre les contenus illicites en ligne[15]. Même au sein de l'espace juridique européen qui est relativement cohérent, l'harmonisation de la réglementation des contenus médiatiques reste partielle mais, s'agissant de l'UE, des progrès significatifs ont récemment été réalisés grâce à plusieurs actes juridiques numériques qui abordent directement ou indirectement la question de la diffusion de contenus illicites et préjudiciables.

Le présent rapport se concentre sur l'application des dispositions relatives aux contenus illicites et à la désinformation en ligne. Bien que ces deux catégories de contenus soient particulièrement importantes, notamment pour la résilience de la société et l'intégrité démocratique, elles présentent des différences juridiques et conceptuelles considérables, en particulier pour ce qui est de déterminer les types de discours en ligne qui peuvent légitimement faire l'objet de restrictions. Il est donc indispensable de préciser la terminologie utilisée.

Dans cette publication, le terme « contenu illicite » fait référence à tout matériel qui enfreint les dispositions légales en vigueur, et son caractère illicite est clairement défini par la législation ou la jurisprudence. En conséquence, ce qui est illicite relève principalement de la législation nationale. Cette situation met en exergue l'un des défis que représentent les limites de l'application de la législation en raison de l'absence d'harmonisation des définitions en vigueur dans les législations nationales lorsqu'il s'agit de déterminer ce qui doit être reconnu comme étant illicite ainsi que la manière de résoudre ce problème, y compris à un niveau supranational comme celui de l'Union européenne. Toutefois, du fait de la compréhension commune du terme « illicite », cette notion est privilégiée dans la publication par rapport au terme plus général et moins clairement défini de « contenu illégal ». Certaines lois, en particulier au niveau national, font référence au

[13] *Sanchez c. France [GC]*, *op. cit*, (paragraphe 160, qui renvoie à l'arrêt *Savva Terentyev c. Russie*, requête n° 10692/09 (CEDH, 28 août 2018), paragraphe 79, et la décision rendue dans l'affaire *Savcı Çengel c. Turquie*, requête n° 30697/19 (CEDH, 18 mai 2021), paragraphe 35.

[14] Voir le considérant 3 du DSA.

[15] Pour un bref aperçu, voir J. Ukrow, « Introduction et aperçu » *in* M. Cappello (sous la direction de), *L'application du droit des médias sans frontières*, IRIS *Spécial*, Observatoire européen de l'audiovisuel, Strasbourg, 2018, p. 3 et suiv.

« contenu illégal », comme par exemple la loi allemande *NetzDG*[16], partiellement abrogée). On entend par « contenu illégal » les contenus illicites, mais également les actions ou le matériel qui ne respectent pas les normes administratives, les obligations contractuelles ou les normes réglementaires. Par souci de précision juridique, le terme officiel utilisé dans la législation numérique de l'UE est « contenu illicite »[17].

En revanche, les contenus dits préjudiciables regroupent les contenus qui ne sont pas nécessairement illicites mais qui sont néanmoins jugés préjudiciables pour les individus ou la société - par exemple, la désinformation, les informations sanitaires inexactes ou les contenus qui portent atteinte aux processus démocratiques. Aborder la question de la désinformation dans un contexte juridique, réglementaire ou politique exige de définir ce terme afin de le distinguer des autres types de contenus. La désinformation fait habituellement référence à des informations fausses ou trompeuses qui sont diffusées intentionnellement dans le but d'induire en erreur. Elle se distingue par conséquent de la mésinformation, qui consiste en de fausses informations diffusées sans intention de tromper, ou de l'information malveillante, qui est une information authentique utilisée à mauvais escient ou en dehors de son contexte[18]. Cette catégorie est particulièrement difficile à réglementer, puisqu'elle échappe en grande partie au champ d'application de la législation en vigueur et qu'elle est donc souvent traitée dans le contexte plus vaste des contenus préjudiciables. Par conséquent, le présent rapport aborde les contenus illicites en y incluant la désinformation comme une catégorie distincte, qui n'est pas nécessairement englobée dans la notion de contenu « illicite » et qui présente des défis spécifiques en matière de réglementation.

Face à l'ampleur, à la généralisation et aux répercussions sociétales des contenus illicites et de la désinformation, une série de modèles de réglementation et de gouvernance ont été élaborés pour tenir compte de la diversité des intermédiaires d'internet, qui peuvent intervenir de manière passive ou active et qui assurent toute une série de fonctions et de services. Parmi ces intermédiaires figurent les réseaux sociaux, les blogs, les messageries, les forums de discussion et les bulletins d'information, les plateformes de regroupement et d'évaluation des informations sociales et les plateformes de partage de vidéos, pour n'en citer que quelques-uns. Cette étude se concentre sur les plateformes qui, en leur qualité d'intermédiaires, hébergent et diffusent des contenus.

La première partie de cette publication présente le cadre législatif du Conseil de l'Europe avant de décrire les principaux instruments juridiques de l'Union européenne applicables aux intermédiaires d'internet. On entend généralement par intermédiaire d'internet une entité qui facilite l'utilisation du réseau en proposant des services de communication, d'accès à des contenus ou de transmission et de stockage de données entre les utilisateurs. Les différentes mesures juridiques comportent des définitions distinctes de la notion d'intermédiaire et des services proposés, qui seront précisées le cas échéant. Les

---

[16] *Netzwerkdurchsetzungsgesetz* (loi relative à l'application du droit sur les réseaux sociaux - NetzDG). Cette loi a été partiellement abrogée par le règlement sur les services numériques (DSA).

[17] La définition d'un contenu illicite figure, par exemple, à l'article 3(h), du règlement sur les services numériques (DSA).

[18] Pour une définition de la mésinformation, de l'information malveillante et de la désinformation, voir C. Wardle et H. Derakshan, *Les désordres de l'information - Vers un cadre interdisciplinaire pour la recherche et l'élaboration des politiques*, Rapport de la DGI du Conseil de l'Europe, 2017, p. 20 et suiv.

exemples nationaux qui mettent l'accent sur différents types de contenus illicites ou préjudiciables et sur les réponses apportées par le droit européen et les législations nationales visent à donner une vue d'ensemble des disparités en matière d'application de la réglementation. Le chapitre suivant établira une comparaison entre les différents modèles d'application de la législation. Compte tenu du contexte juridique présenté dans la première partie de cette publication, ainsi que d'une brève description des cadres législatifs nationaux applicables aux plateformes en ligne en général, les exemples nationaux précisent les dispositions spécifiques pour cibler les contenus illicites ou préjudiciables en question et illustrent la mise en œuvre de cette réglementation dans un contexte précis. La dernière partie du document illustrera la manière dont le rapport met en exergue les défis qui restent à relever pour lutter efficacement contre la diffusion en ligne de contenus illicites et préjudiciables.

2. Cadre juridique

2.1. Cadre du Conseil de l'Europe en matière de régulation des contenus et mesures d'exécution

Dr Sandra Schmitz-Berndt, chercheuse associée, Institut du droit européen des médias (EMR)

2.1.1. Mesures d'exécution et cadre relatif aux droits fondamentaux au sein du Conseil de l'Europe

Si « la possibilité pour les individus de s'exprimer sur internet constitue un outil sans précédent d'exercice de la liberté d'expression[19] », la mise en œuvre de règles relatives à certains contenus spécifiques, telles que la restriction de l'accès à certains discours, leur suppression ou leur poursuite en justice, porte en soi atteinte au droit à la liberté d'expression garanti par l'article 10 de la Convention européenne des droits de l'homme[20] (ci-après « la Convention »). Les libertés de communication – liberté d'information, liberté d'expression et liberté de diffusion par les médias de masse – consacrées à l'article 10, paragraphe 1, de la Convention, ainsi que dans les dispositions constitutionnelles comparables, sont indispensables au bon fonctionnement de la démocratie. Considérées comme des moyens de défense contre l'État, elles garantissent l'autodétermination de l'individu par une protection contre toute ingérence de l'État dans les processus de communication. Afin d'établir l'existence d'une telle ingérence, dans l'interprétation moderne du terme, il convient de tenir compte de toute règle ou mesure imposée par l'État qui restreint, entrave ou rend totalement ou partiellement impossible l'exercice d'un comportement protégé par les droits fondamentaux. En ce sens, la mise en exécution de règles concernant la communication peut en soi constituer une ingérence imputable à l'État[21].

---

[19] *Delfi AS c. Estonie* [GC] n° 64569/09 (CEDH, 16 juin 2015), § 110.

[20] Pour une vue d'ensemble, avec synthèses et accès rapide à la jurisprudence, voir Observatoire européen de l'audiovisuel, base de données VERBO, disponible sur <https://verbo.obs.coe.int/> ; précédemment également D. Voorhoof *et al.* et T. McGonagle (éd.), *Freedom of Expression, the Media and Journalists: Case-Law of the European Court of Human Rights* (« Liberté d'expression, médias et journalistes : jurisprudence de la Cour européenne des droits de l'homme »), uniquement en anglais, IRIS *Thèmes,* Observatoire européen de l'audiovisuel, Strasbourg 2024. S'agissant du cadre relatif à l'application de la législation au niveau constitutionnel national, voir J. Ukrow, « Le cadre d'application de la loi à l'encontre des fournisseurs de contenu en ligne et étrangers », *in* M. Cappello (éd.), *L'application du droit des médias sans frontières*, IRIS *Spécial*, Observatoire européen de l'audiovisuel, Strasbourg, 2018.

[21] C. Mensching, « Artikel 10 EMRK », *in* U. Karpenstein et F. C. Mayer (éd.), *Konvention zum Schutz der Menschenrechte und Grundfreiheiten: EMRK,* 3e édition, C. H. Beck, Munich, 2022, point 27 avec d'autres références.

Toutefois, l'importance des droits à la communication va au-delà de la protection des individus contre les ingérences arbitraires des États. La Cour européenne des droits de l'homme a reconnu qu'il pouvait également exister des obligations positives inhérentes à un respect effectif des droits concernés. Par conséquent, selon la Cour, l'exercice réel et efficace de la liberté d'expression ne dépend pas simplement du devoir de l'État de s'abstenir de toute ingérence, mais peut exiger des mesures positives de protection, jusque dans les relations des individus entre eux[22]. Selon les circonstances, des acteurs privés peuvent également être tenus indirectement de respecter ces droits, cette obligation étant très similaire, voire identique, à celle imposée aux États. Ce point prend toute son importance lorsque les infrastructures de base nécessaires aux communications publiques sont fournies par des acteurs privés, ces derniers assumant des rôles qui étaient traditionnellement considérés comme des missions de service public, comme la garantie des services de poste et de télécommunications[23].

L'article 10, paragraphe 2, de la Convention prévoit la possibilité de limiter l'exercice des libertés de communication visées par l'article 10, paragraphe 1, et assortit de conditions les éventuelles restrictions imposées. Il énumère en outre expressément un certain nombre d'objectifs légitimes justifiant une ingérence par les États parties qui ont ratifié la Convention.

La Cour européenne des droits de l'homme a eu l'occasion à maintes reprises de reconnaître que la possibilité pour les individus de s'exprimer sur internet constituait un outil sans précédent de la liberté d'expression[24]. Elle considère que grâce à son accessibilité, ainsi qu'à sa capacité à conserver et à diffuser de grandes quantités de données, internet contribue grandement à améliorer l'accès du public à l'actualité et à faciliter la diffusion de l'information de manière générale, y compris dans le cas de contenus ignorés par les médias traditionnels[25]. Dans le même temps, elle estime que les communications et contenus en ligne risquent, plus que la presse, de porter atteinte à l'exercice et à la jouissance des droits de l'homme et des libertés fondamentales, en particulier du droit au respect de la vie privée[26]. La Cour a reconnu qu'internet, puissant outil de communication unique en son genre, se distinguait de la presse écrite, compte tenu de sa capacité à emmagasiner et à diffuser l'information dans le monde entier ; il doit par conséquent faire l'objet de règles sur mesure, reflétant ses particularités technologiques[27]. En outre, les importants avantages qu'il présente, entre autres pour l'exercice de la liberté d'expression, s'accompagnent d'un certain nombre de risques, notamment le fait que des propos clairement illicites peuvent être diffusés instantanément dans le monde entier et « parfois demeurer en ligne pendant fort longtemps[28] ». Qui plus est, la Cour a reconnu que les communications et contenus en

---

[22] *Özgür Gündem c. Turquie*, n° 23144/93 (CEDH, 16 mars 2000), § 43 en référence à *X et Y c. Pays-Bas*, n° 8978/80 (CEDH, 26 mars 1985), paragraph 23.

[23] Voir BVerfG (Cour constitutionnelle fédérale allemande), jugement du 22 février 2011, 1 BvR 699/06, paragraphe 59.

[24] *Delfi AS c. Estonie* [GC] n° 64569/09, § 110 ; *Cengiz et autres c. Turquie*, n^{os} 48226/10 et 14027/11 (CEDH, 1er décembre 2015), paragraph 52 ; *Ahmet Yildirim c. Turquie*, n° 3111/10 (CEDH, 18 décembre 2012), § 48 ; *Times Newspapers Ltd c. Royaume-Uni (n^{os} 1 et 2)*, n^{os} 3002/03 et 23676/03 (CEDH, 10 mars 2009), § 27.

[25] *Ahmet Yildirim c. Turquie*, n° 3111/10, § 48 ; s'agissant des contenus qui ne sont pas traités par la presse traditionnelle, voir *Cengiz et autres c. Turquie*, n^{os} 48226/10 et 14027/11, § 52.

[26] *Egill Einarsson c. Islande*, n° 24703/15 (CEDH, 7 février 2018), § 46.

[27] *Comité de rédaction de Pravoye Delo et Shtekel c. Ukraine*, n° 33014/05 (CEDH, 5 mai 2011), § 63.

[28] *Delfi AS c. Estonie* [GC] n° 64569/09, § 110.

ligne risquaient, plus que la presse traditionnelle, de porter atteinte à l'exercice et à la jouissance des droits de l'homme et des libertés fondamentales[29].

Dès 2003, le Comité des Ministres du Conseil de l'Europe a adopté une déclaration sur la liberté de la communication sur l'internet[30], dont le principe 6 prévoit une responsabilité limitée des fournisseurs de services pour les contenus diffusés en ligne. En vertu de ce même principe, lorsque les fonctions des fournisseurs de services sont plus larges et qu'ils stockent des contenus émanant d'autres parties, les États membres peuvent les tenir pour coresponsables, dans l'hypothèse où ils ne prennent pas rapidement des mesures pour supprimer ou pour bloquer l'accès aux informations ou aux services dès qu'ils ont connaissance, comme cela est défini par le droit national, de leur caractère illicite ou, en cas de plainte pour préjudice, de faits ou de circonstances révélant la nature illicite de l'activité ou de l'information considérée. Ce faisant, le Conseil de l'Europe a repris le concept de responsabilité applicable en droit national par les États membres de l'Union européenne en vertu de l'article 14 de la directive sur le commerce électronique de l'UE[31].

Le Conseil de l'Europe a par la suite abordé directement ou indirectement, au fil des ans, l'application des règles relatives aux contenus illicites et à la désinformation en ligne dans de nombreux autres documents stratégiques, notamment des recommandations et des déclarations. Contrairement aux conventions du Conseil de l'Europe dont les dispositions s'imposent aux signataires, ces textes normatifs politiques ne sont pas juridiquement contraignants, mais ils servent à étayer l'interprétation des conventions et notamment de celle des droits de l'homme, en appliquant des principes généraux à des scénarios types ou à des contextes spécifiques et en définissant une réponse différenciée et graduelle[32].

Dans le préambule de sa recommandation CM/Rec(2018)2 sur les rôles et les responsabilités des intermédiaires d'internet, instrument d'action reposant sur le principe de l'État de droit, le Comité des Ministres relève en outre qu'« [u]ne grande diversité d'acteurs, communément appelés "intermédiaires d'internet", dont le nombre ne cesse de s'étendre, facilitent les interactions sur l'internet entre les personnes physiques et entre les personnes physiques et morales, en exerçant des fonctions diverses et en proposant des services variés[33] ». « En raison des rôles multiples des intermédiaires, leurs responsabilités et leurs devoirs correspondants ainsi que leur protection en vertu de la loi devraient être définis selon les services spécifiques qu'ils fournissent et les fonctions spécifiques qu'ils exercent[34]. » Tenant compte de l'évolution des rôles variés endossés par les acteurs en ligne, le Conseil de l'Europe a par conséquent cessé d'employer le terme « fournisseurs de services internet », couramment utilisé pour désigner des fournisseurs d'accès, de mise en

[29] *Comité de rédaction de Pravoye Delo et Shtekel c. Ukraine*, nº 33014/05, *op. cit.* § 63.
[30] Conseil de l'Europe, Comité des Ministres, Déclaration sur la liberté de la communication sur l'internet, Decl(28/05/2003).
[31] Union Européenne, Directive 2000/31/CE, du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, JO L 178/1 du 17 juillet 2000.
[32] Cette approche était suggérée dans la recommandation du Conseil de l'Europe sur une nouvelle conception des médias. Voir CM/Rec(2011)7 – Recommandation du Comité des Ministres aux États membres sur une nouvelle conception des médias.
[33] Conseil de l'Europe, Recommandation CM/Rec(2018)2 du Comité des Ministres aux États membres sur les rôles et les responsabilités des intermédiaires d'internet, préambule, paragraphe 4.
[34] *Ibid.*, paragraphe 11.

cache ou d'hébergement, pour privilégier l'appellation, plus large, d'« intermédiaires d'internet ». Abordant les obligations des États et les responsabilités de ces intermédiaires, l'annexe à la recommandation CM/Rec(2018)2 définit des lignes directrices à l'attention des États sur les actions à prendre à l'égard des intermédiaires d'internet. Parmi les obligations incombant aux États en matière de protection et de promotion des droits de l'homme et des libertés fondamentales dans l'environnement numérique, figure notamment la prise en compte des différences notables de taille, de nature, de fonction et de structure organisationnelle des intermédiaires lors de l'élaboration, de l'interprétation et de l'application du cadre législatif[35]. Le Comité des Ministres reconnaît que les fournisseurs de plateformes peuvent jouer des rôles différents dans la production et la diffusion de contenus, ce qui implique une approche graduelle ou différenciée[36]. Cette dernière, conformément à la recommandation CM/Rec(2011)7, veut que chaque acteur dont les services sont considérés comme un média ou une activité intermédiaire ou auxiliaire bénéficie à la fois de la forme (différenciée) et du niveau (graduel) appropriés de protection, et que les responsabilités soient également délimitées[37].

Les États devraient veiller à ce que les dispositions législatives et réglementaires ainsi que les politiques relatives aux intermédiaires d'internet soient effectivement applicables et exécutables, et qu'elles ne restreignent pas indûment le fonctionnement et la circulation des communications transfrontières[38]. L'annexe à la recommandation CM/Rec(2018)2 précise que toute mesure des autorités publiques adressée à des intermédiaires d'internet en vue de restreindre un accès (y compris le blocage ou la suppression de contenus), ou toute autre mesure qui pourrait entraîner une limitation de l'exercice de la liberté d'expression, doit répondre au triple critère prévu par l'article 10 de la Convention. En d'autres termes, toute requête, demande ou autre action des autorités publiques adressée à des intermédiaires d'internet en vue de restreindre un accès (y compris le blocage ou la suppression de contenus) doit être prévue par la loi, poursuivre l'un des buts légitimes énoncés à l'article 10 de la Convention, être nécessaire dans une société démocratique et être proportionnée au but poursuivi[39]. Néanmoins, lors de l'application de telles mesures, les autorités nationales devraient obtenir une ordonnance par une autorité judiciaire ou par une autre instance administrative indépendante dont les décisions font l'objet d'un contrôle juridictionnel, avant d'exiger d'un intermédiaire la restriction de l'accès à des contenus, sauf dans les cas concernant des contenus illégaux quel que soit le contexte, comme les contenus portant sur des abus sexuels d'enfants, ou dans les cas où des mesures expéditives s'imposent, conformément aux conditions prescrites à l'article 10 de la Convention[40].

---

[35] Annexe à la Recommandation CM/Rec(2018)2 du Comité des Ministres aux États membres sur les rôles et les responsabilités des intermédiaires d'internet, paragraphe 1.1.5.
[36] *Ibid.*, paragraphe 1.3.9.
[37] Annexe à la Recommandation CM/Rec(2011)7 du Comité des Ministres aux États membres sur une nouvelle conception des médias, « Critères d'identification des médias et orientations en vue d'une approche graduelle et différenciée », paragraphe 7.
[38] Recommandation CM/Rec(2018)2 du Comité des Ministres aux États membres sur les rôles et les responsabilités des intermédiaires d'internet, paragraphe 1.1.6.
[39] *Ibid.*, paragraphe 1.3.1.
[40] *Ibid.*, paragraphe 1.3.2.

La recommandation CM/Rec(2018)2 conseille en outre aux États de ne pas imposer aux intermédiaires de surveiller les contenus auxquels ils donnent simplement accès, ou qu'ils transmettent ou stockent. Toute demande adressée aux intermédiaires et toute initiative de corégulation doivent par conséquent éviter d'imposer une obligation générale de surveiller[41]. La recommandation aborde également la responsabilité des contenus provenant de tiers, indiquant que les intermédiaires ne devraient pas être considérés responsables pour des contenus auxquels ils donnent simplement accès, qu'ils transmettent ou qu'ils stockent ; en revanche, une coresponsabilité peut être établie dans le cas de contenus qu'ils stockent, s'ils n'agissent pas avec la diligence voulue pour restreindre l'accès à ces contenus ou à ces services dès qu'ils ont connaissance de leur caractère illicite, notamment par le biais de procédures reposant sur la notification[42].

S'agissant des procédures de notification, la recommandation CM/Rec(2018)2 indique que celles-ci ne devraient pas être conçues de telle manière qu'elles incitent les intermédiaires à retirer des contenus licites, en raison par exemple de délais trop courts, et qu'elles devraient en outre contenir suffisamment d'informations pour permettre aux intermédiaires de prendre des mesures appropriées[43]. Compte tenu de l'approche fondée sur les droits de l'homme qui caractérise l'action du Conseil de l'Europe, toute ingérence des intermédiaires dans les échanges libres et ouverts d'informations et d'idées doit être limitée à des buts légitimes spécifiques et respecter les principes de transparence et de responsabilité, tout en assurant l'accès à un recours effectif[44]. Ce point n'empêche cependant pas les États d'imposer aux intermédiaires des obligations visant à réduire les risques en ligne et à lutter contre la diffusion de contenus illicites, par exemple en instaurant des mécanismes de modération des contenus. Les recommandations ultérieures du Conseil de l'Europe concernent ainsi les effets des technologies numériques sur la liberté d'expression[45], les impacts des systèmes algorithmiques sur les droits de l'homme[46] et la lutte contre le discours de haine[47]. Dans une approche transversale, la recommandation CM/Rec(2022)11 sur les principes de gouvernance des médias et de la communication[48] aborde les risques posés par les plateformes diffusant du contenu illicite et préjudiciable, et évoque explicitement, au rang des réponses adaptées, la modération des contenus en fonction des risques et dans le respect des droits de l'homme.

La recommandation CM/Rec(2022)13 sur les effets des technologies numériques sur la liberté d'expression[49] marque un effort supplémentaire pour faire en sorte que les technologies numériques favorisent les droits consacrés par l'article 10 de la Convention,

---

[41] *Ibid*., paragraphe 1.3.5.
[42] *Ibid*., paragraphe 1.3.7.
[43] *Ibid*.
[44] *Ibid*., paragraphes 2.2 et suiv.
[45] Conseil de l'Europe, Recommandation CM/Rec(2022)13 du Comité des Ministres aux États membres sur les effets des technologies numériques sur la liberté d'expression.
[46] Conseil de l'Europe, Recommandation CM/Rec(2020)1 du Comité des Ministres aux États membres sur les impacts des systèmes algorithmiques sur les droits de l'homme.
[47] Conseil de l'Europe, Recommandation CM/Rec(2022)16 du Comité des Ministres aux États membres sur la lutte contre le discours de haine.
[48] Conseil de l'Europe, Recommandation CM/Rec(2022)11 du Comité des Ministres aux États membres sur les principes de gouvernance des médias et de la communication.
[49] Conseil de l'Europe, Recommandation CM/Rec(2022)13 du Comité des Ministres aux États membres sur les effets des technologies numériques sur la liberté d'expression.

plutôt que de les restreindre. En matière d'obligation de rendre des comptes et de recours, elle exige que les États veillent à l'existence de mécanismes de recours effectifs contre les restrictions à la liberté d'expression[50]. Lorsque des intermédiaires d'internet appliquent de telles restrictions, ils devraient fournir aux utilisateurs directement ou indirectement concernés des informations précises sur les règles en vertu desquelles leurs droits ont été limités. Les intermédiaires devraient en outre prévoir des mécanismes de recours rapides et effectifs[51].

Dans la mesure où des propos diffamatoires et d'autres types de discours illicites « peuvent être diffusés comme jamais auparavant dans le monde entier, en quelques secondes, et parfois demeurer en ligne pendant fort longtemps » et où les droits protégés par les articles 10 et 8 de la Convention « méritent un égal respect », « il faut en principe conserver la possibilité pour les personnes lésées par des propos diffamatoires ou par d'autres types de contenu illicite d'engager une action en responsabilité de nature à constituer un recours effectif contre les violations des droits de la personnalité[52] ». Les propos qui ne sont pas compatibles avec les valeurs proclamées et garanties par la Convention ne sont pas protégés par l'article 10 de celle-ci, en vertu de l'article 17 de la Convention qui interdit l'abus de droit. Malgré l'existence d'une abondante jurisprudence concernant la mise en balance des articles 10 et 8 de la Convention, le Conseil de l'Europe a jugé nécessaire d'aborder les spécificités du discours de haine, en particulier dans le contexte en ligne, au sein d'une recommandation distincte consacrée à la lutte contre celui-ci[53]. Cette recommandation CM/Rec(2022)16 donne des orientations aux États pour la mise en œuvre d'un éventail complet et bien calibré de mesures juridiques et non juridiques. Si les principes généraux qui valent pour les publications hors ligne s'appliquent aussi sur internet, la recommandation s'intéresse tout particulièrement à l'environnement numérique, où circulent l'essentiel des discours de haine de nos jours. Les comportements de harcèlement ayant tendance à se perpétuer aussi longtemps que de tels contenus restent en ligne, la recommandation appelle les États membres à se concentrer sur la suppression des discours de haine en ligne, parallèlement aux enquêtes pénales[54].

Puisque les discours de haine en ligne se diffusent au-delà des frontières, la recommandation CM/Rec(2022)16 reconnaît également la nécessité d'une harmonisation, afin de prévenir et combattre efficacement ces discours[55]. Dans la droite ligne de la recommandation CM/Rec(2018)2, cette harmonisation doit porter sur les rôles et les responsabilités de l'ensemble des parties prenantes, y compris des intermédiaires d'internet[56].

La recommandation CM/Rec(2022)16 exige que les procédures, et notamment les conditions de retrait des contenus, ainsi que les responsabilités imposées aux intermédiaires d'internet, soient transparentes, claires et prévisibles, et qu'elles prévoient

[50] *Ibid.*, Annexe, paragraphe 4.1.
[51] *Ibid.*, paragraphe 4.5.
[52] *Delfi AS c. Estonie* [GC] n° 64569/09, § 110.
[53] Conseil de l'Europe, Recommandation CM/Rec(2022)16 du Comité des Ministres aux États membres sur la lutte contre le discours de haine.
[54] *Ibid.*, préambule.
[55] *Ibid.*, paragraphe 16.
[56] *Ibid.*, paragraphe 17.

l'existence de voies de recours[57]. Les auteurs d'infractions étant souvent anonymes, les États doivent mettre en place un système permettant la divulgation, par les fournisseurs de services, de données concernant leurs abonnés[58]. La recommandation aborde également la question de la modération des contenus, laquelle doit être supervisée par des modérateurs humains, dans un contexte d'utilisation d'outils d'intelligence artificielle[59] (IA). Outre la désignation d'un nombre suffisant de modérateurs de contenu, le texte encourage l'adoption de fonctionnements collaboratifs, reposant par exemple sur des signaleurs de confiance et des vérificateurs de faits, ainsi que des coopérations avec les organisations de la société civile qui travaillent sur le discours de haine[60]. Ces recommandations ont été complétées par des notes d'orientation du Conseil de l'Europe, sur la modération de contenu[61] (2021), ainsi que sur la lutte contre la propagation de la mésinformation et de la désinformation en ligne par le biais de la vérification des faits et de la conception de plateformes dans le respect des droits de l'homme[62] (2023).

Dernièrement, la résolution 2590[63] relative à la réglementation de la modération de contenu sur les réseaux sociaux pour sauvegarder la liberté d'expression, adoptée en janvier 2025 par l'Assemblée parlementaire du Conseil de l'Europe (APCE), réaffirme que les fournisseurs de réseaux sociaux sont juridiquement tenus de supprimer tout contenu illicite lorsqu'ils apprennent son existence sur leurs services et indique qu'il « incombe en outre aux réseaux sociaux de lutter contre la diffusion de contenus préjudiciables[64] ». Porteuses de droits fondamentaux, notamment le droit de propriété et la liberté d'entreprise, mais aussi celui d'établir des conditions générales qui ont un caractère contractuel (et sont « à prendre ou à laisser » pour les utilisateurs), les entreprises de réseaux sociaux ont leur mot à dire sur la façon dont les utilisateurs peuvent recourir à leurs services et sur les contenus qu'ils peuvent publier. Elles peuvent en outre mettre en place des politiques de modération de contenus leur permettant d'en déclasser certains, d'en restreindre l'accès ou de les supprimer, ainsi que de suspendre, voire supprimer, certains comptes d'utilisateurs[65]. Compte tenu de leur envergure mondiale et de leur pouvoir contractuel privé, notamment du point de vue de leurs politiques de modération des contenus et des décisions commerciales ou idéologiques qu'ils prennent en la matière, les fournisseurs de réseaux sociaux sont susceptibles d'exercer une influence considérable sur l'opinion publique. Reconnaissant ce rapport de forces inégal et la nécessité de lutter contre la diffusion de contenus préjudiciables, l'APCE souligne la nécessité pour les États de mettre en place, en matière de modération, un cadre réglementaire de nature à corriger ce déséquilibre, qui concilie la modération de contenus avec la protection de la liberté

[57] *Ibid.*, paragraphe 20.
[58] *Ibid.*, paragraphe 24.
[59] *Ibid.*, paragraphe 33.
[60] *Ibid.*, paragraphes 34 et suiv.
[61] Conseil de l'Europe, Comité directeur sur les médias et la société de l'information, Note d'orientation sur la modération de contenu, 2021.
[62] Conseil de l'Europe, Comité directeur sur les médias et la société de l'information, Note d'orientation sur la lutte contre la propagation de la mésinformation et de la désinformation en ligne par le biais de la vérification des faits et de la conception de plateformes dans le respect des droits de l'homme, 2023.
[63] Conseil de l'Europe, Assemblée parlementaire, Réglementer la modération de contenu sur les réseaux sociaux pour sauvegarder la liberté d'expression, Résolution APCE 2590.
[64] *Ibid.*, paragraphe 2.
[65] *Ibid.*, paragraphe 3.

d'expression[66]. La résolution 2590 appelle tant les États membres que les fournisseurs de plateformes de réseaux sociaux à mettre en œuvre des systèmes de modération des contenus garantissant la transparence, l'accès, le contrôle et l'existence de voies de recours, et à faire preuve de retenue, notamment dans le cas de contenus licites ou d'intérêt public[67].

En matière de modération des contenus, mais aussi dans d'autres cas de placement de contenus, les fournisseurs s'appuient de plus en plus sur des systèmes algorithmiques, relevant notamment de l'IA. Le 17 mai 2024, le Conseil de l'Europe a adopté le premier traité juridiquement contraignant à l'échelle internationale pour ses États signataires concernant le recours à l'IA, sous la forme d'une Convention-cadre sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'État de droit[68]. Le texte encourage les États à veiller à ce que leur législation applicable aux systèmes d'IA garantisse la transparence et l'obligation de rendre des comptes, tout en préservant les principes démocratiques et en assurant un contrôle effectif et un réexamen permanent de ces systèmes[69].

Si toutes les recommandations susmentionnées établissent des garanties visant à protéger la liberté d'expression, le cadre du Conseil de l'Europe – axé sur les droits fondamentaux – n'impose aucun mécanisme d'exécution spécifique. Les points qui suivent examinent par conséquent la jurisprudence pertinente de la Cour européenne des droits de l'homme, regroupée en blocs thématiques illustrant le système de réponse graduée.

2.1.2. Mesures d'exécution pour les intermédiaires d'internet et d'autres acteurs en ligne

Comme indiqué plus haut et souligné par la Cour européenne des droits de l'homme, internet joue un rôle important « dans l'exercice du droit à la liberté d'expression en général[70] ». Si les auteurs à l'origine de contenus illicites sont naturellement la cible principale des mesures d'exécution[71], les intermédiaires d'internet, qui relaient les contenus, en ont très tôt fait l'objet eux aussi. En effet, ils sont plus faciles à identifier et disposent par ailleurs des moyens pour restreindre l'accès aux contenus illicites ou pour les supprimer. La jurisprudence évolue à mesure que se diversifient les rôles des intermédiaires, autrefois simples relais ou hébergeurs passifs devenus des éléments actifs de la chaîne de production des contenus et de leur diffusion, qui par exemple gèrent ou

[66] *Ibid.*, paragraphes 4 et suiv.
[67] *Ibid.*, paragraphes 10 et suiv.
[68] Conseil de l'Europe, Convention-cadre du Conseil de l'Europe sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'État de droit (STCE nº 225), 2024. Pour le détail de ses signataires et de son entrée en vigueur, voir ici.
[69] Pour une vue d'ensemble des principes directeurs en matière de régulation de l'IA, voir M. D. Cole, « AI Regulation and Governance on a Global Scale: An Overview of International, Regional and National Instruments », *Journal of AI and Regulation*, 1(1), 2024, p. 126-142 ; concernant la convention-cadre, voir M. Gartner, « Council of Europe: States Adopt First Binding Framework Treaty on AI », *Journal of AI and Regulation*, 1(3), 2024, pp. 342-349.
[70] *Times Newspapers Ltd c. Royaume-Uni (nos 1 et 2)*, nos 3002/03 et 23676/03, § 27.
[71] Concernant la responsabilité des auteurs d'un commentaire, voir *Delfi AS c. Estonie* [GC] nº 64569/09, paragraph 147 et suiv.

sélectionnent les contenus, ou encore assument un rôle éditorial. L'approche graduée dont témoignent les recommandations du Comité des Ministres se retrouve dans la jurisprudence de la CEDH, qui aborde les intermédiaires d'internet en fonction de leurs droits, devoirs et responsabilités.

2.1.2.1. Obligations et responsabilités des intermédiaires d'internet concernant les contenus illégaux provenant de tiers

Le fait d'imposer une responsabilité objective à des portails internet pour des contenus émanant de tiers est jugé incompatible avec l'article 10 de la Convention[72]. Même dans le cas de mesures de droit civil, l'imputation d'une responsabilité concernant des propos émanant de tiers peut avoir des conséquences négatives, par exemple sur l'espace réservé aux commentaires d'un portail en ligne, et produire un effet dissuasif sur la liberté d'expression sur internet[73]. Ceci peut être particulièrement préjudiciable pour les sites web non marchands[74]. Lorsque c'est une responsabilité pénale qui est mise en jeu, sachant que celle-ci doit être adaptée et proportionnée à la gravité des contenus concernés, ce caractère pénal pourrait être perçu comme de nature à accentuer encore les effets des répercussions sur la liberté d'expression[75].

Dans le cas de commentaires illégaux laissés par des tiers, les États peuvent être fondés, pour protéger les droits et intérêts des individus et de la société dans son ensemble, à en imputer la responsabilité à des intermédiaires d'internet sans que cela n'emporte violation de l'article 10 de la Convention, si ceux-ci n'ont pas pris de mesures pour retirer sans délai les contenus clairement illégaux, et ce même en l'absence de notification par la victime alléguée ou par des tiers.

Dans l'affaire emblématique *Delfi AS c. Estonie*, la Cour a examiné pour la première fois la responsabilité civile et le devoir de vigilance incombant à un hébergeur professionnel en matière de propos diffamatoires[76]. Quand bien même le grand portail d'actualité en ligne géré par Delfi AS disposait d'un système de filtrage automatisé et d'une procédure de retrait sur notification, les juridictions estoniennes ont estimé qu'il voyait sa responsabilité engagée en raison de commentaires publiés par des tiers sur le site du portail en réponse à l'un de ses propres articles.

Compte tenu de la nature particulière d'internet, la Cour a estimé que les « devoirs et responsabilités » incombant à un portail d'actualités en ligne aux fins de l'article 10 de la Convention pouvaient, dans une certaine mesure, différer de ceux d'un éditeur

[72] *Magyar Tartalomszolgáltatók Egyesülete et Index.hu Zrt c. Hongrie*, n° 22947/13 (CEDH, 2 février 2016), paragraph 91.
[73] *Sanchez c. France*, n° 45581/15 (CEDH [GC], 15 mai 2023), § 205 en référence à *Magyar Tartalomszolgáltatók Egyesülete et Index.hu Zrt c. Hongrie*, n° 22947/13, § 86.
[74] *Magyar Tartalomszolgáltatók Egyesülete et Index.hu Zrt c. Hongrie*, n° 22947/13, § 86.
[75] *Sanchez c. France*, n° 45581/15, § 206.
[76] Pour un commentaire de cette affaire, voir P. Korpisaari, « From *Delfi* to *Sanchez* – when can an online communication platform be responsible for third-party comments? An analysis of the practice of the ECtHR and some reflections on the Digital Services Act », *Journal of Media Law,* 14(2), 2022, pp. 352-377.

traditionnel vis-à-vis du contenu fourni par des tiers[77]. Si les portails d'actualité en ligne ne jouent pas le rôle d'éditeurs, au sens traditionnel du terme, de contenus fournis par des tiers, ils peuvent en être tenus pour responsables dans certaines circonstances[78]. La différence de traitement des contenus tiers, selon qu'ils sont destinés à des portails d'actualité en ligne ou à des éditeurs traditionnels, est conforme aux instruments internationaux dans ce domaine, lesquels reconnaissent de plus en plus la nécessité d'une distinction entre les principes juridiques régissant les activités des médias traditionnels et ceux gouvernant les portails d'actualité en ligne, sur lesquels les contenus générés par les internautes sont généralement diffusés sans aucun contrôle éditorial au cours du processus de publication[79].

Afin d'établir si un exploitant de portail internet peut être jugé responsable à raison de contenus émanant de tiers, la Cour a identifié quatre critères visant à ménager un juste équilibre entre les intérêts concurrents que sont le droit à la liberté d'expression et le droit à la réputation d'une autre personne ou entité[80].

Ces critères, applicables en matière de responsabilité civile, pénale et administrative, sont 1) le contexte des commentaires ; 2) la responsabilité des auteurs des commentaires ; 3) les mesures appliquées par le requérant et le comportement de la personne lésée ; enfin 4) les conséquences de la procédure interne pour le requérant.

La prise en compte du contexte et du contenu des commentaires contestés est nécessaire, afin de déterminer la licéité globale du contenu déposé par un tiers, c'est-à-dire d'apprécier si les limites autorisées de la liberté d'expression ont été dépassées, tout en tenant compte du contexte immédiat et des spécificités du style de communication sur certains portails internet[81]. Ainsi, l'incidence d'un discours raciste et xénophobe s'accroît et devient plus dommageable dans un contexte électoral, et lorsque le climat politique et social est difficile[82].

Dans l'affaire *Delfi AS c. Estonie*, l'évaluation du contexte s'est étendue à la nature professionnelle et commerciale de la plateforme d'actualité considérée[83]. Le fait de chercher à inciter la publication d'un grand nombre de commentaires relève d'une visée commerciale, de sorte que la Cour a relevé qu'il convenait de distinguer Delfi

> *d'autres types de forums sur internet susceptibles de publier des commentaires provenant d'internautes, par exemple les forums de discussion ou les sites de diffusion électronique, où les internautes peuvent exposer librement leurs idées sur n'importe quel sujet sans que la discussion ne soit canalisée par des interventions du responsable du forum, ou encore les plateformes de médias sociaux où le fournisseur de la plateforme ne produit aucun contenu*

[77] *Delfi AS c. Estonie* [GC] nº 64569/09,§ 113 ; voir également *Orlovskaya Iskra c. Russie*, nº 42911/08 (CEDH, 21 février 2017), paragraph 109.
[78] *Magyar Tartalomszolgáltatók Egyesülete et Index.hu Zrt c. Hongrie*, nº 22947/13, § 62.
[79] Voir *Delfi AS c. Estonie* [GC] nº 64569/09, § 112 et suiv.
[80] *Ibid.*, § 142 et suiv. ; *Magyar Tartalomszolgáltatók Egyesülete et Index.hu Zrt c. Hongrie*, nº 22947/13, § 61.
[81] *Sanchez c. France*, nº 45581/15, § 174 et suiv. ; *Magyar Tartalomszolgáltatók Egyesülete et Index.hu Zrt c. Hongrie*, nº 22947/13, § 77.
[82] *Sanchez c. France*, nº 45581/15, § 176.
[83] *Delfi AS c. Estonie* [GC] nº 64569/09, § 144.

et où le fournisseur de contenu peut être un particulier administrant un site ou un blog dans le cadre de ses loisirs[84].

Si certaines obligations incombent nécessairement aux entités professionnelles qui créent les réseaux sociaux et les mettent à la disposition des autres utilisateurs, le titulaire d'un compte Facebook ne relève de la catégorie des « autres types de forums sur internet susceptibles de publier des commentaires provenant d'internautes » que pour ce qui concerne la fourniture de son « mur » Facebook[85]. Cela ne décharge nullement le titulaire du compte, pas plus que tout autre fournisseur, de ses devoirs et responsabilités vis-à-vis des contenus déposés par des tiers ; en effet, une exclusion de responsabilité risquerait de faciliter voire d'encourager les abus et les dérives, notamment en matière de discours de haine et de désinformation[86].

La mise en jeu de la responsabilité s'agissant de commentaires laissés par des tiers dépend aussi des mesures prises et du comportement de la partie lésée[87]. Les mesures requises peuvent varier en fonction des techniques de modération ou de vérification disponibles et doivent être examinées avec soin, afin d'éviter tout effet dissuasif sur la liberté d'expression[88]. Dans tous les cas, il convient de trouver un équilibre entre les intérêts concurrents[89]. Tenir pour civilement responsable un portail d'information en ligne pour avoir refusé ou omis de supprimer un contenu manifestement illégal, comme dans l'affaire *Delfi AS c. Estonie*, peut se justifier, même en l'absence de notification de la partie lésée ou de tiers[90], ce qui signifie qu'une certaine forme de surveillance serait nécessaire, en particulier autour des contenus propres à susciter des échanges animés[91]. En réalité, la Cour considère qu'il est généralement admis qu'un minimum de contrôle a posteriori ou de filtrage préalable est souhaitable, afin d'identifier au plus vite des propos clairement illégaux et de les supprimer dans un délai raisonnable, et ce même en l'absence de notification d'une partie lésée[92].

2.1.2.2. Obligations et responsabilités des entités non professionnelles vis-à-vis des contenus illicites publiés par des tiers

La responsabilité évoquée ci-dessus peut être imputée à la plateforme d'hébergement, en qualité de fournisseur professionnel, ou aux titulaires de comptes, qui publient leurs

---

[84] *Ibid.*, § 116.
[85] *Sanchez c. France*, nº 45581/15, § 180.
[86] *Ibid.*, § 185.
[87] Pour une vue d'ensemble des attentes applicables aux fournisseurs de plateformes d'hébergement, voir P. Korpisaari, « From *Delfi* to *Sanchez* – when can an online communication platform be responsible for third-party comments? An analysis of the practice of the ECtHR and some reflections on the Digital Services Act », *Journal of Media Law,* 14(2), 2022, pp. 352-377.
[88] Voir *Sanchez c. France*, nº 45581/15, § 182.
[89] *Magyar Tartalomszolgáltatók Egyesülete et Index.hu Zrt c. Hongrie*, nº 22947/13, § 88.
[90] *Ibid.*, § 91 en référence à *Delfi AS c. Estonie* [GC] nº 64569/09, § 157. Voir également T. Enarsson, « Navigating hate speech and content moderation under the DSA: Insights from ECtHR case law », *Information & Communications Technology Law*, 33(3), 2024, p. 384-401, 392 et suivants.
[91] Voir *Magyar Tartalomszolgáltatók Egyesülete et Index.hu Zrt c. Hongrie*, nº 22947/13, § 73.
[92] *Sanchez c. France*, nº 45581/15, § 190.

propres contenus et permettent aux autres de les commenter[93]. Dans l'affaire *Sanchez c. France*, la Cour a eu à déterminer dans quelle mesure le régime de responsabilité des plateformes d'hébergement pouvait être appliqué au titulaire d'une page Facebook, en cas de publication de commentaires illicites sur son mur par des tiers. En l'occurrence, la Cour a reconnu qu'une modération préalable était pratiquement impossible d'un point de vue technique, mais aussi en raison des moyens à mobiliser dans l'hypothèse d'un compte utilisé à des fins non commerciales et connaissant une fréquentation très importante[94].

Une condamnation pénale infligée pour ne pas avoir retiré un contenu tiers conformément au droit national, lorsque le titulaire d'un mur Facebook est réputé assumer le rôle d'un producteur de contenus, ne constitue pas une violation de l'article 10 de la Convention, dès lors que le propriétaire du compte a manqué à certains devoirs et omis de respecter certaines responsabilités qui lui incombaient. Parmi les éléments factuels à prendre en compte, il convient de considérer à quel titre intervient le titulaire du compte ou, plus généralement, l'intermédiaire. Ainsi, une personnalité politique qui utilise son compte sur un réseau social à des fins politiques et qui est rompue à la communication publique doit avoir conscience d'un risque plus grand que des excès et des débordements soient commis en réponse à un billet publié en période électorale, et diffusés auprès d'une plus large audience[95]. L'ajustement des paramètres de confidentialité peut constituer une mesure palliative en vue de restreindre la visibilité d'une publication ou de limiter la possibilité d'y répondre. Lorsqu'il peut être établi que l'intéressé a connaissance des problèmes posés par certains commentaires, il est permis d'attendre de lui un contrôle minimal[96]. C'est tout particulièrement le cas lorsque le compte de réseau social concerné est consulté quotidiennement, que certains utilisateurs se répondent et se complètent en discutant à la suite de la publication initiale et que le contenu de leurs échanges a été signalé comme illégal[97]. Si, dans l'affaire *Sanchez c. France*, la condamnation pénale du titulaire du compte Facebook à raison de commentaires laissés par des tiers ne constitue pas une violation de l'article 10 de la Convention, le seuil permettant d'établir que l'existence des contenus illicites était connue s'avère constituer un sujet hautement controversé, comme en témoignent les opinions concordantes[98] et dissidentes[99] dans l'affaire *Sanchez c. France*[100].

Conformément aux normes du droit international, l'imputation d'une responsabilité peut être évitée si le contenu illicite est supprimé « sans délai » dès que l'intermédiaire a connaissance de son caractère illégal[101].

---

[93] *Ibid.*
[94] *Ibid.*, § 185.
[95] *Ibid.*, § 186 et suiv.
[96] *Ibid.*, § 194.
[97] *Ibid.*, § 199 et suiv.
[98] *Ibid.*, Opinion concordante du juge Küris.
[99] *Ibid.*, Opinion dissidente du juge Ravarani ; Opinion dissidente du juge Bošnjak ; Opinion dissidente commune aux juges Wojtyczek et Zünd.
[100] Voir également M. Husovec *et al.*, « Grand confusion after *Sanchez v. France*: Seven reasons for concern about Strasbourg jurisprudence on intermediaries », *Maastricht Journal of European and Comparative Law*, 31(3), 2024, pp. 385-411.
[101] *Delfi AS c. Estonie* [GC] nº 64569/09, § 153.

2.1.2.3. Obligations et responsabilités des créateurs d'hyperliens

À l'instar de la responsabilité objective des portails internet vis-à-vis des contenus émanant de tiers, l'imputation d'une responsabilité objective pour des hyperliens est incompatible avec l'article 10 de la Convention. Ceux-ci diffèrent en effet des modes de publication traditionnels, car ils se contentent de diriger les utilisateurs vers des contenus disponibles ailleurs sur internet et ne constituent pas un acte de communication distinct[102]. Ils permettent aux utilisateurs de naviguer d'un contenu à l'autre sur un réseau qui se caractérise par la disponibilité d'une immense quantité d'informations[103]. En outre, la personne qui renvoie à une information au moyen d'un hyperlien ne maîtrise pas le contenu auquel le lien donne accès et qui peut être modifié après la création du lien[104].

Compte tenu de ces particularités, l'établissement de la responsabilité du créateur d'un hyperlien doit reposer sur des motifs suffisants et pertinents, et requiert une évaluation approfondie des « obligations et responsabilités » qui lui incombent. Il convient ainsi d'examiner les questions suivantes : le créateur 1) a-t-il souscrit au contenu litigieux ? 2) a-t-il répété le contenu litigieux (sans y souscrire) ? 3) a-t-il simplement placé un hyperlien renvoyant au contenu litigieux (sans y souscrire ni le répéter) ? 4) savait-il ou aurait-il raisonnablement pu savoir que le contenu litigieux était diffamatoire ou illicite pour une autre raison ? 5) a-t-il agi de bonne foi, respecté la déontologie de sa profession et exercé la diligence attendue d'un journaliste responsable[105] ?

On notera dans ce contexte que le fait d'exiger de manière générale que les journalistes se distancient systématiquement et formellement du contenu de toute citation susceptible d'insulter des tiers, de les provoquer ou de porter atteinte à leur honneur n'est pas conciliable avec le rôle de la presse, qui est d'informer sur des faits, des opinions et des idées qui ont cours à un moment donné[106].

Le même raisonnement a par la suite été appliqué au partage en ligne de contenus émanant de tiers sur les plateformes de réseaux sociaux, étant à noter que le fait de relayer certains contenus est un moyen courant de communication et d'interaction sociale, et peut contribuer à l'information des citoyens[107]. Toutefois, lorsque des contenus sont sortis de leur contexte sans autre forme de commentaire et peuvent raisonnablement être perçus comme attisant la discorde ethnique ou la violence, une responsabilité peut être retenue pour avoir rendu accessibles des contenus tiers[108].

---

[102] *Magyar Jeti Zrt c. Hongrie*, nº 11257/16 (CEDH, 4 décembre 2018), § 74. Cette question avait précédemment été examinée par la CJUE en lien avec la notion de « communication au public » au sens de l'article 3, paragraphe 1, de la Directive 2001/29/CE sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information, voir *C-466/12 Nils Svensson e. a. contre Retriever Sverige AB* (CJUE, 13 février 2014), ECLI:EU:C:2014:76, paragraphes 18 et suiv.

[103] *Magyar Jeti Zrt c. Hongrie*, nº 11257/16, § 73.

[104] *Ibid.*, § 75.

[105] *Ibid.*, § 77.

[106] *Ibid.*, § 80 en référence à *Thoma c. Luxembourg*, nº 38432/97 (CEDH, 29 mars 2001), § 64. Une question similaire est en instance devant la CJUE, dans le cadre d'une demande de décision préjudicielle émanant du tribunal régional de Budapest (*C-843/24 24.hu*).

[107] *Kilin c. Russie*, nº 10271/12 (CEDH, 11 mai 2021), § 79.

[108] *Ibid.*, § 87 et suiv.

2.1.3. Portée des mesures d'application

Si les règles de modération de contenu figurant dans les conditions générales des plateformes de réseaux sociaux peuvent également prévoir la suspension ou la suppression du compte d'un utilisateur[109], la Cour a défini des limites s'agissant des mesures d'exécution imposées par les États, à l'occasion de plusieurs arrêts. Bien que la suppression ou le blocage de l'accès à un contenu illicite particulier puisse respecter le triple critère établi par l'article 10 de la Convention, toute mesure qui ne se contenterait pas de cibler le contenu illicite proprement dit et toucherait des contenus légaux serait peu susceptible de satisfaire à l'exigence de prévisibilité et risquerait de ne pas remplir non plus la condition de proportionnalité.

2.1.3.1. Blocage de l'accès aux sites web

La Cour a eu à se prononcer à plusieurs reprises sur les mesures prises par des autorités nationales pour bloquer l'accès à certains sites internet. Un blocage de l'accès à l'intégralité de YouTube a entraîné une ingérence dans l'exercice des droits des utilisateurs – qui n'étaient pas directement visés par la mesure – à recevoir et à communiquer des informations et des idées ; en conséquence, ces utilisateurs étaient fondés à faire valoir ce droit devant la Cour[110]. Dans le cas d'espèce, la mise en œuvre des décisions des juridictions nationales concernant certains contenus spécifiques entraînait le blocage de tout accès à l'ensemble du site web[111]. La Cour a estimé que la particularité de la plateforme concernée et les répercussions potentielles du blocage de l'accès à de grandes quantités d'informations restreignaient considérablement les droits des internautes et avaient un effet collatéral important[112].

En revanche, la Cour a estimé que le simple fait d'avoir été indirectement touchés par une mesure de blocage visant deux sites web de partage de musique ne suffisait pas pour que les utilisateurs de ce service puissent se prévaloir de la « qualité de victime » au sens de l'article 34 de la Convention et ne leur donnait donc pas la capacité juridique de saisir la Cour[113]. Le blocage de l'accès à un site internet peut également entraîner celui d'un autre site web possédant la même adresse IP et a peu de chance de satisfaire à l'exigence de prévisibilité prévue par la Convention, tout en restreignant considérablement les droits des internautes[114].

En cas d'imposition de restrictions préalables, un cadre juridique est nécessaire, afin de garantir à la fois un contrôle strict de la portée des interdictions et un examen judiciaire

---

[109] Conseil de l'Europe, Assemblée parlementaire, Réglementer la modération de contenu sur les réseaux sociaux pour sauvegarder la liberté d'expression (Résolution 2590 de l'ACPE, § 3), 2025.

[110] *Cengiz et autres c. Turquie*, nos 48226/10 et 14027/11, §§ 52 et suiv., ainsi que *Ahmet Yildirim c. Turquie*, no 3111/10, § 49 et suiv.

[111] *Ahmet Yildirim c. Turquie*, no 3111/10, § 66.

[112] *Ibid.* ; *Cengiz et autres c. Turquie*, nos 48226/10 et 14027/11, § 64.

[113] *Akdeniz et autres c. Turquie*, nos 41139/15 et 41146/15 (CEDH, 4 mai 2021), § 24.

[114] *Vladimir Kharitonov c. Russie*, no 10795/14 (CEDH, 23 juin 2020), § 45 et suiv. S'agissant du blocage des adresses IP, le principal problème réside dans le fait que de nombreuses adresses sont partagées entre plusieurs fournisseurs de contenu (hébergement web mutualisé). Dès lors qu'une adresse IP donnée se retrouve bloquée, tout le contenu web qui lui est associé devient inaccessible.

efficace de la mesure, visant à prévenir tout abus de pouvoir[115]. L'examen judiciaire d'une mesure de blocage, fondé sur une mise en balance des intérêts concurrents en jeu et visant à trouver un juste équilibre entre eux, est inconcevable sans un cadre établissant des règles précises et spécifiques concernant l'application des restrictions préventives à la liberté d'expression[116]. Dans les affaires concernant l'imposition de restrictions préalables à la publication d'appels à participer à un événement public, la Cour a estimé qu'il devait être possible d'obtenir un examen judiciaire de la mesure de blocage avant la date de l'événement public en question, sans quoi cet examen devenait sans objet[117].

Une décision de blocage total visant un site web est considérée comme une mesure extrême, que la Cour a comparée à l'interdiction d'un journal ou d'un diffuseur[118]. En conséquence, le blocage complet et injustifié de médias, qui ignore la distinction entre contenu licite et illicite, a été jugé arbitraire et manifestement déraisonnable[119]. Il en va de même si le blocage est maintenu après suppression du contenu jugé illégal[120].

Il est nécessaire en outre de veiller à ce que tout blocage soit proportionné à l'objectif poursuivi. Comme évoqué plus haut, la réglementation relative aux contenus illégaux et les mesures d'application correspondantes doivent être adaptées au plus juste. Toute mesure de blocage doit viser strictement le contenu illicite et éviter les effets arbitraires ou excessifs. Il est permis d'en conclure que l'imposition de décisions ordonnant un blocage intégral est peu susceptible d'être conforme à l'article 10 de la Convention ; les autorités doivent examiner si des solutions moins intrusives, telles que la suppression de publications spécifiques, peuvent atteindre le même objectif sans limiter de manière disproportionnée l'accès à l'expression licite. Doivent notamment être pris en compte les répercussions sur les tiers et l'effet dissuasif sur la liberté d'expression en ligne.

2.1.3.2. Blocage de comptes de réseaux sociaux

La question du blocage des comptes de réseaux sociaux a été abordée dans l'affaire *Kablis c. Russie* qui concernait notamment un compte sur un réseau social, qui avait été bloqué pour éviter des infractions à la législation dans le domaine de la diffusion d'information et pour préserver l'ordre public. Tout d'abord, la Cour a estimé que la possibilité pour la personne concernée de créer simplement un nouveau compte sur le réseau social n'était pas pertinente pour déterminer si l'ingérence était justifiée[121]. Dans une société démocratique, toute ingérence dans la liberté d'expression doit être nécessaire, c'est-à-dire qu'elle doit répondre à un besoin social impérieux et que les autorités doivent fournir des motifs pertinents et suffisants pour justifier la restriction imposée. La raison invoquée pourrait être, par exemple, que le compte de réseau social présente un risque pour la

[115] *Kablis c. Russie*, nos 48310/16 et 59663/17 (CEDH, 30 avril 2019), § 92.
[116] *Ahmet Yildirim c. Turquie*, no 3111/10, § 64.
[117] *Kablis c. Russie*, nos 48310/16 et 59663/17, § 85 et suiv.
[118] *OOO Flavus et autres c. Russie*, nos 12468/15, 23489/15 et 19074/16 (CEDH, 23 juin 2020), paragraph 37 ; *Bulgakov c. Russie*, no 20159/15 (CEDH, 23 juin 2020), § 34 et références supplémentaires.
[119] *OOO Flavus et autres c. Russie*, nos 12468/15, 23489/15 et 19074/16, § 34 ; *Bulgakov c. Russie*, no 20159/15, paragraph 34.
[120] *Bulgakov c. Russie*, no 20159/15, § 34 et suiv.
[121] *Kablis c. Russie*, nos 48310/16 et 59663/17, § 84.

sécurité publique ou est susceptible de porter atteinte à l'ordre public ou la commission d'infractions pénales[122]. Comme dans le cas du blocage d'un site ou d'une page web dans son intégralité, l'article 10 de la Convention exige que les autorités tiennent compte, entre autres aspects, du fait que le blocage d'un compte sur un réseau social dans son intégralité rend inaccessibles de grandes quantités d'informations. Une telle mesure restreint considérablement les droits des internautes et a un effet collatéral important sur les contenus qui n'ont pas été jugés illégaux[123]. Un examen minutieux est donc essentiel pour veiller à ce que toute restriction de ce type soit proportionnée à l'objectif légitime poursuivi.

2.2. Cadre de l'Union européenne en matière de régulation des contenus et mesures d'exécution

Dr Mark D. Cole, Director for Academic Affairs, Institute of European Media Law (EMR) and Professor in Media and Telecommunication Law, University of Luxembourg Institut du droit européen des médias (EMR)

2.2.1. Mesures d'exécution au regard du droit primaire de l'UE

Après avoir abordé les limites imposées par l'article 10 de la Convention européenne des droits de l'homme aux mesures d'exécution adoptées par les États parties à celle-ci, il est nécessaire de se pencher sur les difficultés particulières liées à l'application des textes dans le cadre du droit primaire de l'Union européenne[124]. Si les droits fondamentaux posent des limites essentielles à l'action des États, la mise en œuvre effective de la régulation des contenus, en particulier au sein de l'environnement numérique, doit elle aussi être évaluée à l'aune des principes constitutionnels de l'Union, tels que la répartition des compétences[125], les libertés du marché intérieur, les valeurs communes et le principe de coopération loyale au sens de l'article 4, paragraphe 3, du Traité sur l'Union européenne[126] (TUE). Ces dimensions soulèvent des interrogations complexes concernant les modalités de la coordination des mesures d'application entre les différents États membres.

En substance, deux aspects essentiels entrent en jeu dès lors que l'on considère le marché intérieur et les relations entre les États membres de l'UE, ainsi que celles avec les institutions à l'échelle de l'Union. Tout d'abord, le cadre juridique de l'Union prévoit des dispositions spécifiques pour le règlement des différends. Ensuite, les interactions entre

---

[122] *Ibid.*, § 88.

[123] *Ibid.*, § 94 en référence à *Ahmet Yildirim c. Turquie*, n° 3111/10, § 66, et à *Cengiz et autres c. Turquie*, n°s 48226/10 et 14027/11, § 64.

[124] À cet égard, voir également J. Ukrow, « Le cadre d'application de la loi à l'encontre des fournisseurs de contenu en ligne et étrangers », *in* M. Capello (éd.), *L'application du droit des médias sans frontières*, IRIS *Spécial,* Observatoire européen de l'audiovisuel, Strasbourg, 2018.

[125] Voir M. D. Cole, J. Ukrow et C. Etteldorf, *On the Allocation of Competences between the European Union and its Member States in the Media Sector*, Nomos, Baden-Baden, 2021.

[126] Traité sur l'Union européenne dans sa version consolidée, 15 mars 2025.

États membres sont définies par des principes tels que celui du « pays d'origine[127] », qui occupe une place importante dans le droit de l'UE et constitue l'une des pierres angulaires du marché interne, notamment à travers la jurisprudence de la Cour de justice de l'Union européenne[128] (CJUE). En vertu de ce principe, un opérateur économique établi dans un État membre est tenu de respecter les règles de droit de son pays d'origine, mais n'est soumis à aucune obligation juridique supplémentaire dans le ou les États membres dans lesquels ses biens ou ses services sont proposés ou peuvent être consommés ; autrement dit, aucune exigence supplémentaire ne peut lui être imposée en sus de celles qui sont en vigueur dans son lieu d'établissement. Cette conception réduit les coûts, les formalités administratives et les charges de personnel, tout en évitant des doublons en matière de contrôles ou d'exigences qui, autrement, entraveraient l'activité économique transfrontalière.

C'est par conséquent à l'État membre d'origine qu'il incombe au premier chef d'apprécier la légalité d'un service. La possibilité de choisir son pays d'origine est enracinée dans la liberté d'établissement, qui permet aux entreprises et aux travailleurs indépendants de sélectionner librement leur lieu d'établissement au sein de l'Union. Cependant, la restriction de la capacité des États membres à prendre des mesures à l'encontre des prestataires de services étrangers ne s'applique dans le cadre de la libre circulation des services que lorsque le prestataire est établi dans un autre État membre ou dans un État tiers partie à l'accord sur l'Espace économique européen (EEE). Les prestataires qui ne sont pas établis dans un État membre de l'UE ou de l'EEE sont, eux, soumis aux règles générales du droit international public. De surcroît, le droit dérivé peut prévoir d'autres possibilités de dérogation spécifiques au principe du pays d'origine. Les États membres destinataires, ou ceux dans lesquels le service assuré par un prestataire établi dans un autre État membre est réellement consommé, peuvent intervenir à titre exceptionnel, notamment lorsqu'une restriction justifiée et proportionnée à la libre circulation des services est nécessaire. Cette intervention peut reposer sur des motifs explicites ou implicites reconnus par le droit de l'Union, tels que l'ordre public[129], la sécurité publique ou la protection des consommateurs. Tout motif de cet ordre est interprété de manière stricte par la CJUE[130].

Lorsque la législation dérivée définit concrètement la portée des libertés fondamentales, ces règles d'harmonisation doivent prévaloir dans l'appréciation juridique. Dans le contexte de la présente publication, les principaux textes à considérer sont

---

[127] Pour une analyse générale du principe du pays d'origine, voir par exemple M. D. Cole, « The Country of Origin Principle – From State Sovereignty under Public International Law to Inclusion in the Audiovisual Media Services Directive of the European Union », *in* W. Meng, G. Ress et T. Stein (éd.), *Europäische Integration und Globalisierung – Festschrift zum 60-jährigen Bestehen des Europa-Instituts*, Nomos, Baden-Baden, 2011, pp. 113-130 ; M. D. Cole, C. Etteldorf et C. Ullrich, *Updating the Rules for Online Content Dissemination*, *Schriftenreihe Medienforschung der LfM NRW*, volume 83, Nomos, Baden-Baden, 2021, p. 143 et suiv. ; D. Rowland, U. Kohl et A. Charlesworth, *Information Technology Law*, Routledge, Abingdon, 5e édition, 2017, p. 268 et suiv. ; K. Schilling, *Binnenmarktkollisionsrecht*, De Gruyter, Berlin, 2006, p. 74 et suiv. ; M.-D. Garabiol-Furet, « Plaidoyer pour le principe du pays d'origine », *Revue du Marché commun et de l'Union Européenne*, 2006, pp. 82-87.

[128] C-376/22 *Google Ireland c. KommAustria* [2023] ECLI:EU:C:2023:835 ; C-665/22 *Amazon Services Europe c. AGCOM* [2024] ECLI:EU:C:2024:435 ; affaires jointes C-664/22 et C-666/22 *Google Ireland e. a. contre AGCOM* [2024] ECLI:EU:C:2024:434 ; C-663/22 *Expedia Inc. c. AGCOM* [2024] ECLI:EU:C:2024:433 ; affaires jointes C-662/22 et C-667/22 *AirBnB e. a. contre AGCOM* [2024] ECLI:EU:C:2024:432.

[129] Voir C-376/22 *Google Ireland c. KommAustria*.

[130] Comme le souligne l'avocat général Szpunar dans ses Conclusions dans l'affaire *C-376/22 Google Ireland c. KommAustria* [2023] ECLI:EU:C:2023:467, paragraphe 64.

notamment la directive Services de médias audiovisuels[131] (SMA) et la directive sur le commerce électronique[132], qui établissent des règles sectorielles régissant la prestation transfrontière de services dans le marché intérieur.

2.2.2. Droit dérivé de l'Union européenne relatif à la régulation des contenus et aux mesures d'application

2.2.2.1. Régulation des médias et des VSP : la directive SMA et l'EMFA

La directive SMA définit le cadre juridique dans lequel les États membres peuvent prendre des mesures à l'encontre des fournisseurs transfrontières de services de télévision linéaire, de services vidéo à la demande et de plateformes de partage de vidéos (VSP) dans le domainecoordonné par ses dispositions, notamment en matière de communications commerciales audiovisuelles, de protection des mineurs et de lutte contre l'incitation à la haine. Dans la mesure où il s'agit d'une directive, les États membres sont tenus de transposer ses dispositions dans leur droit national, ce qui signifie, par exemple, qu'ils doivent veiller, par des mesures appropriées, à ce que les services de médias audiovisuels assurés par les fournisseurs de services relevant de leur compétence ne diffusent aucune incitation à la violence ou à la haine[133], ni aucune incitation publique à commettre une infraction terroriste[134].

Ce cadre comporte une obligation pour tous les fournisseurs de restreindre l'accès aux contenus considérés comme préjudiciables aux mineurs, c'est-à-dire susceptibles de nuire à leur développement physique, mental ou moral, sans nécessairement être illégaux. Parmi les mesures proposées en ce sens par l'article 6 *bis* de la directive SMA figurent le choix de l'heure de l'émission, l'utilisation d'outils permettant de vérifier l'âge ou d'autres mesures techniques, proportionnées au préjudice que pourrait causer le programme.

---

[131] Directive 2010/13/UE du Parlement européen et du Conseil du 10 mars 2010 visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels (directive Services de médias audiovisuels), JO L 95/1 du 15 avril 2010, modifiée en dernier lieu par la Directive (UE) 2018/1808 du Parlement européen et du Conseil du 14 novembre 2018 modifiant la directive 2010/13/UE visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels (directive « Services de médias audiovisuels »), compte tenu de l'évolution des réalités du marché, JO L 303 du 28 novembre 2018, ainsi que par le Règlement (UE) 2024/1083 du Parlement européen et du Conseil du 11 avril 2024 établissant un cadre commun pour les services de médias dans le marché intérieur et modifiant la directive 2010/13/UE (règlement européen sur la liberté des médias), JO L 2024/1083 du 17 avril 2024.

[132] Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, JO L 178 du 17 juillet 2000.

[133] S'agissant du champ d'application, voir l'article 6, paragraphe 1, point a), de la directive SMA.

[134] Conformément à l'article 5 de la Directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil, JO L 88/6 du 31 mars 2017, auquel fait référence la directive SMA dans ses dispositions.

Dans la mesure où une part significative des contenus proposés sur les plateformes de partage de vidéos ne relèvent pas de la responsabilité éditoriale du fournisseur de VSP, l'article 28 *ter* de la directive SMA prévoit l'obligation, pour les États membres, de veiller à ce que les fournisseurs de ces plateformes relevant de leur compétence préservent les utilisateurs de contenus préjudiciables et prennent les mesures appropriées pour protéger le grand public des programmes, vidéos créées par des utilisateurs et communications commerciales comportant des contenus préjudiciables[135]. Ces mesures doivent être nécessaires, efficaces et proportionnées, tout en conciliant la nécessité de protéger les utilisateurs et les droits fondamentaux des fournisseurs et utilisateurs des plateformes, notamment le droit à la liberté d'expression. Les dispositions prises peuvent revêtir la forme de mécanismes de notification et de signalement des contenus, de systèmes de vérification de l'âge, d'outils de contrôle parental, ainsi que de procédures transparentes de modération des contenus[136].

Si les autorités ou organismes de régulation nationaux doivent disposer des pouvoirs d'exécution nécessaires pour garantir le respect de la législation nationale, les États membres doivent également encourager le recours à la corégulation et promouvoir l'autorégulation au moyen de codes de conduite adoptés à l'échelon national, lesquels doivent notamment permettre une mise en œuvre effective au moyen, entre autres, de sanctions efficaces et proportionnées[137].

En complément de la directive SMA, le règlement européen sur la liberté des médias[138] (EMFA) instaure une nouvelle série de règles visant à protéger le pluralisme et l'indépendance des médias dans l'Union. Il comporte de surcroît des dispositions concernant les procédures de coopération entre les autorités ou organismes de régulation nationaux. Avec ce texte, les pratiques antérieures de coopération entre ces autorités et organismes, qui avaient lieu sous l'égide du Groupe des régulateurs européens pour les services de médias audiovisuels[139] (ERGA) et n'étaient pas juridiquement contraignantes, ont été officialisées et ainsi incorporées à la directive SMA. Cette dernière s'était initialement contentée de mettre en place un organe de coopération sans en fixer les modalités de

---

[135] Voir le considérant 47 de la Directive (UE) 2018/1808 du Parlement européen et du Conseil du 14 novembre 2018 modifiant la directive 2010/13/UE visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels (directive « Services de médias audiovisuels »), compte tenu de l'évolution des réalités du marché, JO L 303 du 28 novembre 2018.

[136] Article 28 *ter*, paragraphe 3, de la directive SMA.

[137] Article 4 *bis*, paragraphe 1, de la directive SMA. Les États membres et la Commission européenne peuvent en outre promouvoir l'autorégulation au moyen de codes de conduite de l'Union, voir l'article 4 *bis*, paragraphe 2, de la directive SMA.

[138] Règlement (UE) 2024/1083 du Parlement européen et du Conseil du 11 avril 2024 établissant un cadre commun pour les services de médias dans le marché intérieur et modifiant la directive 2010/13/UE (règlement européen sur la liberté des médias), JO L 2024/1083 du 17 avril 2024.

[139] Groupe des régulateurs européens pour les services de médias audiovisuels : voir le « Memorandum of Understanding between the National Regulatory Authority Members of the European Regulators Group for Audiovisual Media Services (ERGA) » (protocole d'accord entre les membres des autorités de régulation nationale du groupe des régulateurs européens pour les services de médias audiovisuels) du 3 décembre 2020, et M. D. Cole et C. Etteldorf, « Future Regulation of Cross-Border Audiovisual Content Dissemination », *Schriftenreihe Medienforschung der LfM NRW*, volume 84, Nomos, Baden-Baden, 2023, p. 149 et suiv., ainsi que p. 176 et suiv. Le Groupe des régulateurs européens pour les services de médias audiovisuels est remplacé par le Comité européen pour les services de médias, instauré par l'article 8 de l'EMFA.

fonctionnement détaillées, alors même que la nécessité d'une coopération étroite, en particulier pour régler les dossiers transfrontières, se faisait de plus en plus sentir depuis l'élargissement du champ d'application de la directive aux plateformes de partage de vidéos[140]. L'article 14 du règlement européen sur la liberté des médias instaure ainsi un cadre de coopération structuré, aux fins de l'application cohérente et efficace du règlement, et de la mise en œuvre de la directive SMA, garantissant un dialogue et une obligation de justification des actions de la part de l'autorité compétente[141]. En outre, une disposition spécifique porte sur les demandes de coopération concernant les obligations des fournisseurs de plateformes de partage de vidéos (article 15 de l'EMFA) et reflète la nature paneuropéenne de ceux-ci : bien que les prestataires proposent couramment leurs services dans les différents pays de l'Union, ils relèvent « seulement » de la compétence de leur État membre d'origine, tant en vertu de la directive sur le commerce électronique que de la directive SMA[142].

Le Comité européen pour les services de médias, qui se substitue et succède au Groupe des régulateurs, a notamment pour mission de veiller à la coordination des mesures d'application dans l'ensemble des États membres[143]. L'article 17 de l'EMFA prévoit en outre une règle de coordination au sein du comité en ce qui concerne les mesures visant les « fournisseurs de services de médias malhonnêtes » établis en dehors de l'Union, qui présentent un risque sérieux et grave pour la sécurité publique[144]. Ce point constitue une réaction directe aux difficultés constatées lorsqu'il s'est agi d'apporter à une réponse commune face aux risques engendrés par la diffusion de chaînes de télévision russes dans l'Union, après que la Fédération de Russie a déclenché une guerre contre l'Ukraine. Le Comité européen pour les services de médias peut coordonner des mesures de régulation adoptées à l'échelon national concernant les services de médias qui ciblent des publics dans l'Union, lorsque ces services portent atteinte ou présentent un risque sérieux et grave d'atteinte à la sécurité publique ou à la défense, par exemple parce qu'ils pourraient potentiellement être contrôlés par des gouvernements ou entités de pays tiers. Le comité peut alors formuler un avis afin de favoriser une réponse plus unifiée et efficace.

2.2.2.2. Régulation des plateformes en ligne : le DSA et le DMA

Le système de régulation développé dans le cadre de la directive sur le commerce électronique opérait une distinction entre intermédiaires actifs et passifs : la responsabilité était imputée selon que l'intermédiaire restait neutre (passif) ou que son implication allait au-delà de l'hébergement passif et qu'il interagissait avec le contenu hébergé, par exemple

[140] Considérant 43 de l'EMFA.
[141] Voir M. D. Cole et C. Etteldorf, *Research for CULT Committee – European Media Freedom Act - Background Analysis*, Parlement européen, Département thématique des politiques structurelles et de cohésion, Bruxelles, 2023, p. 50.
[142] Pour une synthèse des rapports entre la directive SMA et la directive sur le commerce électronique, voir J. Oster et E. Wagner, « § 38 Kommunikations- und Medienrecht », *in* M. Ludwigs (éd.), *Handbuch des EU-Wirtschaftsrechts,* 63e édition mise à jour, C. H. Beck, Munich, 2025, note marginale 83.
[143] Article 13 de l'EMFA.
[144] Article 13, paragraphe 1, point l) et article 17 de l'EMFA.

en le modérant, en le sélectionnant ou en l'optimisant[145]. Les exemptions de responsabilité reposant sur cette distinction, qui figuraient auparavant dans la directive sur le commerce électronique, sont désormais intégrées dans le règlement sur les services numériques[146] (DSA), dans une volonté de continuer à tenir compte des rôles variés qu'endossent les intermédiaires vis-à-vis des contenus émanant de tiers, bien que ces rôles aient considérablement évolué entre la directive sur le commerce électronique et le DSA[147].

Le DSA se fixe pour objectif de mettre en place « un environnement en ligne sûr, prévisible et fiable qui facilite l'innovation et dans lequel les droits fondamentaux consacrés par la Charte[148], y compris le principe de protection des consommateurs, sont efficacement protégés[149] ». Entre autres dispositions, le règlement harmonise pleinement les règles applicables aux services intermédiaires dans le marché intérieur et lutte contre la diffusion de contenus illicites en ligne[150]. La notion de « contenu illicite » doit être entendue comme correspondant de manière générale aux règles en vigueur dans l'environnement hors ligne[151]. Par conséquent, le DSA en adopte une définition large, désignant « toute information qui, en soi ou par rapport à une activité, y compris la vente de produits ou la fourniture de services, n'est pas conforme au droit de l'Union ou au droit d'un État membre qui est conforme au droit de l'Union, quel que soit l'objet précis ou la nature précise de ce droit[152] ». Cette définition devrait recouvrir des contenus qui, en vertu du droit applicable, sont soit eux-mêmes illicites, comme les discours haineux illégaux ou les contenus à caractère terroriste et les contenus discriminatoires illégaux, soit rendus illicites par les règles en vigueur, du fait qu'ils se rapportent à des activités illégales[153].

Le considérant 12 du DSA illustre la notion de contenu illicite par des exemples tels que le partage d'images représentant des abus sexuels commis sur des enfants, le partage illégal d'images privées sans consentement, le harcèlement en ligne, la vente de produits non conformes ou contrefaits, la vente de produits ou la fourniture de services en violation du droit en matière de protection des consommateurs, l'utilisation non autorisée de matériel protégé par le droit d'auteur, l'offre illégale de services de logement ou encore la vente illégale d'animaux vivants. À cet effet, le DSA établit notamment, par le biais de règles harmonisées relatives à la fourniture de services intermédiaires, un cadre pour l'exemption conditionnelle de responsabilité des fournisseurs de services intermédiaires

---

145 Voir M. D. Cole, C. Etteldorf et C. Ullrich, *Cross-Border Dissemination of Online Content*, *Schriftenreihe Medienforschung der LfM NRW*, volume 81, Nomos, Baden-Baden, 2020, p. 176 et suiv. ; D. Rowland, U. Kohl et A. Charlesworth, *Information Technology Law*, Routledge, Abingdon, 5e édition, 2017, p. 104 et suiv. ; S. Schmitz, *The Struggle in Online Copyright Enforcement*, Nomos, Baden-Baden 2015, p. 574 et suiv.

146 Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques), JO L 277/1, 27 octobre 2022.

147 M. D. Cole, C. Etteldorf et C. Ullrich, *Cross-Border Dissemination of Online Content*, *Schriftenreihe Medienforschung der LfM NRW*, volume 81, Nomos, Baden-Baden, 2021, p. 222 et suiv. ; M. C. Buiten, « The Digital Services Act – From Intermediary Liability to Platform Regulation », *JIPITEC*, 12, 2021, pp. 361-380 ; Madiega T., *Réforme du régime européen de responsabilité des intermédiaires en ligne – Contexte de la future législation relative aux services numériques*, Service de recherche du Parlement européen, PE 649.404, Bruxelles, mai 2020.

148 Charte des droits fondamentaux de l'Union européenne, 2012/C 326/02, JO C 326/391 du 26 octobre 2012.

149 Article 1, paragraphe 1, du DSA.

150 Considérant 9 du DSA.

151 Considérant 12 du DSA.

152 Article 3, point h), du DSA.

153 Considérant 12 du DSA.

(article 1er, paragraphe 2, point a), du DSA) et, indépendamment des questions de responsabilité, des obligations de diligence spécifiques adaptées à certaines catégories de fournisseurs de services intermédiaires (article 1er, paragraphe 2, point b), du DSA).

Le chapitre II du DSA définit les règles en matière de responsabilité des fournisseurs de services intermédiaires : simple transport (article 4), mise en cache (article 5) et hébergement[154] (article 6). Les services de simple transport et de mise en cache n'entraînent pas de responsabilité pour le fournisseur, à condition que celui-ci n'exerce aucune ingérence. Les fournisseurs d'hébergement sont exemptés de responsabilité vis-à-vis des contenus stockés pour le compte de leurs utilisateurs, sauf s'ils ont effectivement connaissance d'un contenu ou d'une activité illicite et omettent d'agir promptement pour retirer le contenu ou empêcher l'accès à celui-ci[155]. Le fournisseur peut avoir effectivement connaissance ou prendre conscience du caractère illicite du contenu par différents moyens, notamment en effectuant des enquêtes de sa propre initiative ou grâce à des notifications soumises par des tiers, dans la mesure où celles-ci sont assez précises et suffisamment étayées pour permettre à un opérateur économique diligent d'identifier et d'évaluer raisonnablement le contenu présumé illicite et, le cas échéant, d'agir à son encontre[156]. Les fournisseurs d'hébergement, quelle que soit leur taille, doivent mettre en place des mécanismes de notification et d'action aisément accessibles et simples à utiliser, pour faciliter ces notifications. S'agissant de la suppression du contenu, le DSA ne fixe pas de délai, se contentant d'exiger à son article 6, paragraphe 1, point b), que le fournisseur « agisse promptement ». Afin d'accélérer les mesures prises à l'encontre des contenus illicites, il dispose que les notifications soumises par les « signaleurs de confiance[157] » agissant dans le cadre réglementaire du DSA doivent être traitées en priorité par les intermédiaires[158]. Le statut de signaleur de confiance est attribué par le coordinateur pour les services numériques de l'État membre dans lequel l'entité présentant la demande est établie ; il n'est accordé qu'à un nombre limité d'entités ayant fait la preuve de leur expertise et de leurs compétences particulières aux fins d'identifier les contenus illicites[159]. Cette expertise peut également être limitée à un domaine spécifique, appelé « domaine d'expertise désigné[160] », comme c'est le cas de HateAid gGmbH en Allemagne, sur les questions de cyberviolence et de discours illicite. Au chapitre de la transparence, les signaleurs de confiance sont tenus de publier des rapports compréhensibles et détaillés sur les notifications soumises, ainsi que, notamment, sur l'action entreprise par le fournisseur concerné en réponse[161]. La Commission européenne prépare actuellement des lignes

[154] Pour un aperçu des régimes de responsabilité prévus par le DSA, voir M. Capello (éd.), *Décrypter la législation sur les services numériques (DSA)*, IRIS *Spécial*, Observatoire européen de l'audiovisuel, Strasbourg, 2021, p. 13 et suiv.
[155] Article 6 du DSA.
[156] Voir considérant 22 et article 6 du DSA. S'agissant de l'exigence d'avoir « effectivement connaissance » du contenu, voir T. Radtke, « Article 6 DSA », *in* H. Gersdorf et B. Paal (éd.), *BeckOK Informations- und Medienrecht*, 48e édition, C. H. Beck, Munich, 2025, paragraphes 27 et suiv.
[157] Au sujet des signaleurs de confiance, voir J. van de Kerkhof, « Article 22 Digital Services Act: Building Trust with Trusted Flaggers », *Internet Policy Review*, 14(1), 2025. Pour une vue d'ensemble, voir également https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa.
[158] Article 22, paragraphe 1, du DSA.
[159] Article 22, paragraphe 2, du DSA. Au 25 août 2025, 38 signaleurs de confiance ont été désignés.
[160] Article 22, paragraphe 1, du DSA.
[161] Article 22, paragraphe 3, du DSA.

directrices visant à aider les coordinateurs pour les services numériques en rationalisant le processus de désignation des signaleurs de confiance et en fournissant des orientations sur les circonstances pouvant conduire à la révocation de leur statut[162].

Bien que l'ensemble des intermédiaires soient concernés par les obligations de retrait des contenus illicites sur notification s'ils veulent éviter d'engager leur responsabilité, les très grandes plateformes en ligne (TGP) ainsi que les très grands moteurs de recherche (TGMR) qui, en raison de leur portée significative, ont un impact sur la société qui emporte des risques, sont soumis à des obligations de diligence supplémentaires. Le seuil opérationnel est fixé à 45 millions d'utilisateurs mensuels, soit l'équivalent de 10 % de la population de l'Union[163]. L'obligation de procéder à des évaluations des risques et de concevoir des mesures d'atténuation de ceux-ci concerne aussi la diffusion de contenus illicites et ses effets négatifs, réels ou prévisibles, pour l'exercice des droits de l'homme. Les risques liés à la diffusion en ligne de contenus illicites, ainsi que de certains contenus préjudiciables, doivent être repérés, analysés et traités de manière diligente[164]. Les mesures adoptées doivent être raisonnables et efficaces, tout en restant proportionnées à la capacité économique du fournisseur[165]. Ce dernier peut ainsi notamment adopter des dispositions spécifiques dans ses conditions générales, adapter son système de modération des contenus et ses processus décisionnels en interne[166]. Cela ne comporte pas d'obligation générale de surveillance, l'article 8 du DSA stipulant qu'il n'y a aucune obligation générale de surveillance ou de recherche active des faits. Le DSA évoque bien plus la modération des contenus comme un facteur susceptible d'avoir une incidence sur le degré de risque de diffusion des contenus illicites[167].

Au sens de l'article 3, point t), du DSA, on entend par « modération des contenus » les activités, qu'elles soient automatisées ou non, entreprises par des fournisseurs de services intermédiaires qui sont destinées à détecter et à identifier les contenus illicites ou les informations incompatibles avec leurs conditions générales, qui ont été partagés par les destinataires du service, et à lutter contre ces contenus ou ces informations. Les mesures prises à ce titre peuvent avoir une incidence sur la disponibilité, la visibilité et l'accessibilité des contenus illicites, et passer par leur rétrogradation, leur démonétisation, le fait de rendre l'accès à ceux-ci impossible ou leur retrait. Il est également possible de peser sur la capacité des destinataires du service à fournir des informations, par exemple en supprimant ou en suspendant leur compte. Dans le détail, la conception des processus et systèmes de modération (notamment le recours à des décisions individuelles et à une modération à grande échelle) est laissée à la discrétion de l'entreprise qui les met en œuvre. Dans le même temps, cependant, le DSA fixe sans ambiguïté une obligation de supprimer promptement certains types de contenus.

Le respect et l'application de codes de conduite au sens de l'article 45 du DSA peuvent être considérés comme une mesure recevable d'atténuation des risques. Dans le cas de catégories bien précises de contenus illicites en particulier, il convient d'explorer

[162] L'adoption de ces lignes directrices est prévue d'ici la fin de l'année 2025.
[163] Article 33 du DSA. Au 25 août 2025, 33 TGP et deux TGMR ont été désignés.
[164] Considérants 53 et 55 du DSA.
[165] Voir le considérant 86 du DSA.
[166] Considérant 87 du DSA.
[167] Article 34, paragraphe 2, point b), et article 35, paragraphe 1, point c), du DSA.

des mesures passant par l'autorégulation et la corégulation, y compris au moyen de codes de conduite[168]. Certains codes existants relatifs aux risques systémiques importants, qui prennent la forme de « codes de bonnes pratiques », ont été utilisés antérieurement au DSA en guise de mesures d'autorégulation. Ils pourraient servir de base et devenir des « codes de conduite » au sens du DSA. L'article 45 du DSA énumère un certain nombre de critères pour ce faire : les codes doivent notamment établir des objectifs spécifiques, contenir des indicateurs clés de performance et tenir dûment compte des besoins et des intérêts de toutes les parties intéressées. La Commission européenne et le Comité européen des services numériques[169] nouvellement créé sont chargés d'apprécier si les codes de conduite contribuent effectivement à la bonne application du DSA[170].

S'il impose des obligations aux services intermédiaires, le DSA met également en place un cadre complet visant à garantir leur respect. Cette dimension passe par une série de mesures d'enquête et d'exécution mises à la disposition des autorités nationales et de la Commission européenne par le règlement en fonction de l'attribution des compétences de surveillance, qui varient selon le type de fournisseurs.

À cette fin, les États membres sont tenus de désigner une ou plusieurs autorités compétentes indépendantes, chargées de la surveillance des fournisseurs et de l'exécution du DSA. Toutefois, ce dernier n'impose pas aux États membres de confier aux autorités compétentes la mission de se prononcer sur la licéité d'éléments de contenus spécifiques. Les réponses apportées en matière civile, pénale et administrative, y compris par exemple les demandes de suppression de contenus illicites, sont régies par la législation nationale des États membres[171]. Ces derniers sont tenus de déterminer un régime de sanctions effectives, proportionnées et dissuasives, applicables aux infractions au DSA qui relèvent de leur compétence[172]. Compte tenu du caractère transfrontière des services concernés et de la portée horizontale des obligations, chaque État membre doit en outre désigner un coordinateur pour les services numériques, qui joue le rôle de point de contact unique pour toutes les questions liées à la surveillance et à l'exécution au niveau de l'Union[173]. Le Comité européen des services numériques fait office de groupe consultatif indépendant, afin de garantir une application uniforme du DSA et de permettre une coopération efficace entre la Commission européenne et les coordinateurs pour les services numériques[174].

S'agissant du respect des obligations par les fournisseurs de TGP et TGMR, le DSA confère la compétence à la Commission européenne, qui devient de ce fait une autorité de régulation. Les articles 65 et suivants du DSA disposent que la Commission peut exercer des pouvoirs d'enquête de sa propre initiative et engager des procédures contre cette catégorie de fournisseurs. En complément, elle peut adopter une décision constatant un manquement et infliger au fournisseur des amendes ou des astreintes[175]. Toute infraction au DSA est passible d'une amende jusqu'à concurrence de 6 % du chiffre d'affaires mondial

[168] Voir le considérant 104 du DSA.
[169] Voir l'article 61 du DSA.
[170] Article 45, paragraphe 4, du DSA.
[171] Voir par exemple P. Zurth, « Private Rechtsdurchsetzung im Digital Services Act », *Gewerblicher Rechtsschutz und Urheberrecht*, 125(19), 2023, pp. 1329-1408 et notamment p. 1331.
[172] Article 52 du DSA.
[173] Article 49, paragraphe 2, et considérant 110 du DSA.
[174] Article 61 du DSA.
[175] Articles 73, 74, 76 et 79 du DSA.

annuel réalisé par le fournisseur de TGP/TGMR concerné, et peut en outre déclencher une période de surveillance renforcée, permettant de s'assurer du bon respect du règlement[176]. En cas d'urgence, des mesures provisoires peuvent être imposées. En présence d'une infraction persistante entraînant un préjudice grave pour les utilisateurs et constituant une infraction pénale qui implique une menace pour la vie ou la sécurité des personnes, la suspension temporaire du service peut même être demandée[177].

Les pouvoirs d'enquête et d'exécution de la Commission européenne sont complétés par des mécanismes visant à garantir un niveau adéquat de transparence et de responsabilisation. Tous les services intermédiaires sont ainsi tenus de publier un rapport annuel de transparence sur la modération des contenus qu'ils ont assurée au cours de la période concernée[178]. Celui-ci doit notamment comprendre des informations concernant le nombre d'injonctions reçues des autorités des États membres, les pratiques de modération des contenus, le nombre d'éléments retirés et le nombre de notifications soumises par des signaleurs de confiance, ainsi que les autres demandes de suppression. Compte tenu des risques systémiques qu'ils présentent, les fournisseurs de TGP/TGMR sont soumis à des obligations renforcées de rendre des comptes, qui portent également sur leur personnel et ses qualifications, et qui prévoient la publication de rapports tous les six mois[179]. La Commission européenne a en outre mis en place une base de données sur la transparence conformément à l'article 24, paragraphe 5, du DSA, laquelle centralise et met à disposition du grand public les exposés des motifs[180] que les fournisseurs de TGP/TGMR sont tenus de fournir lorsqu'ils rendent impossible ou restreignent l'accès à des contenus.

Si la Commission européenne n'a encore infligé aucune amende au titre du DSA – bien que plusieurs procédures soient en cours, notamment concernant les obligations en matière de protection des mineurs[181] –, elle a d'ores et déjà pris des mesures d'exécution[182] au titre du règlement sur les marchés numériques[183] (DMA). Ce dernier vise à mettre en place un « marché contestable et équitable[184] » dans le secteur numérique et s'intéresse principalement aux questions de concurrence en lien avec les « services de plateforme

[176] Articles 74 et 75 du DSA.
[177] Article 82 et article 51, paragraphe 3, du DSA.
[178] Article 15 du DSA. Voir également C. Etteldorf, « Une avancée majeure au niveau de l'UE : la législation sur les services numériques », *in* M. Capello (éd.), *Transparence et responsabilité en matière d'algorithmes des services numériques*, IRIS *Spécial*, Observatoire européen de l'audiovisuel, Strasbourg, 2023, p. 31 et 39.
[179] Article 42 du DSA.
[180] Article 17 du DSA.
[181] Voir par exemple la décision de la Commission européenne d'ouvrir une procédure en vertu de l'article 66, paragraphe 1, du règlement (UE) 2022/2065 du 18 décembre 2023 contre Twitter International Unlimited. Pour un aperçu des principales actions visant à assurer l'application des dispositions, voir le site dédié de la Commission, disponible sur https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses.
[182] Le 23 avril 2025, la Commission a infligé à Apple et à Meta des amendes de 500 millions d'euros et de 200 millions d'euros respectivement. Voir Commission européenne, « La Commission estime qu'Apple et Meta enfreignent le règlement sur les marchés numériques », communiqué de presse, 23 avril 2025.
[183] Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques), JO L 265/1, 12 octobre 2022.
[184] Sur ce dernier point, voir M. D. Cole, « La proposition de législation sur les marchés numériques (DMA) : à propos des contrôleurs d'accès, de l'équité et de la transparence dans l'environnement en ligne » *in* Capello M. (éd.), *Décrypter la législation sur les services numériques (DSA)*, IRIS *Spécial*, Observatoire européen de l'audiovisuel, Strasbourg, 2022.

essentiels » proposés par ceux qu'il appelle « contrôleurs d'accès ». L'article 2, paragraphe 2, du DMA énumère les services considérés comme des services de plateforme essentiels, notamment les moteurs de recherche en ligne, les services de réseaux sociaux, les services de plateformes de partage de vidéos et les services de publicité en ligne, tandis que son chapitre II entre dans le détail des fournisseurs désignés comme contrôleurs d'accès. Comme pour les fournisseurs de TGP/TGMR dans le cadre du DSA, les contrôleurs d'accès sont des entités qui ont un poids important sur le marché intérieur et fournissent un service de plateforme essentiel (ou plusieurs) qui constitue un point d'accès majeur permettant aux entreprises, qui y ont recours, d'atteindre leurs utilisateurs finaux. Les contrôleurs d'accès sont des acteurs qui bénéficient actuellement d'une « position solide et durable » ou jouiront, selon toute probabilité, d'une telle position dans un avenir proche[185]. Il s'agit par conséquent d'entreprises présentant une importance systémique. L'article 3, paragraphe 2, du DMA fixe des seuils quantitatifs très élevés, mais 23 services de plateforme essentiels, assurés par sept fournisseurs différents, ont d'ores et déjà été identifiés comme étant des contrôleurs d'accès[186]. Le DMA définit, pour le secteur en ligne, les types de comportements qui doivent être considérés comme abusifs s'ils sont le fait de contrôleurs d'accès et instaure un certain nombre d'obligations et d'interdictions qui leur sont spécifiques. Il s'agit par exemple de règles concernant les informations relatives à la publicité, notamment l'accès aux informations sur le fonctionnement de la chaîne de valeur de la publicité en ligne (article 5, paragraphes 9 et 10, et article 6, paragraphe 8, du DMA), ainsi que le classement des contenus (article 6, paragraphe 5, du DMA).

En matière d'application, le DMA s'éloigne de l'approche multiacteurs du DSA et centralise le contrôle de la mise en œuvre au niveau de la Commission européenne. Cette dernière a le pouvoir d'ouvrir des enquêtes de marché[187] et d'engager des procédures susceptibles d'aboutir à l'adoption de décisions visant à faire respecter les obligations des contrôleurs d'accès et à leur infliger des amendes, jusqu'à concurrence de 20 % de leur chiffre d'affaires annuel mondial en cas d'infractions répétées[188].

2.2.2.3. Régulation de la publicité à caractère politique : le règlement TTPA

Compte tenu de sa capacité à toucher un large public, il n'est guère étonnant qu'internet soit abondamment utilisé par les partis et responsables politiques pour diffuser leurs opinions ou « faire passer [...] un message politique[189] ». Dans ce contexte, en particulier, le microciblage fondé sur le profilage faisant appel à l'apprentissage automatique et à l'IA représente une menace significative, non seulement pour l'autonomie des personnes, mais aussi pour la démocratie elle-même. Dans ce dernier cas, c'est ce qu'a notamment révélé le scandale Cambridge Analytica[190]. Le règlement relatif à la transparence et au ciblage de la

[185] Article 3 du DMA.
[186] Un site de la Commission répertorie les contrôleurs d'accès ainsi désignés, voir https://digital-markets-act.ec.europa.eu/gatekeepers_en.
[187] Articles 16 à 19 du DMA.
[188] Articles 20, 29 et 30 du DMA.
[189] Voir *Magyar Kétfarkú Kutya Párt c. Hongrie*, nº 201/17 (CEDH, 20 janvier 2020), § 88-89.
[190] Voir M.-E. Dowling, « Cyber Information Operations: Cambridge Analytica's Challenge to Democratic Legitimacy », *Journal of Cyber Policy*, 7(2), 2022, pp. 230-248.

publicité à caractère politique[191] (règlement TTPA) d'avril 2024, qui constitue une réponse réglementaire à cette situation, aborde les préoccupations liées à la manipulation de l'information et aux ingérences étrangères dans les élections, en harmonisant les règles relatives à la transparence et aux obligations de diligence raisonnable connexes, applicables à la fourniture de services de publicité à caractère politique. Le règlement TTPA vient notamment compléter le DSA, le DMA, ainsi que le règlement général sur la protection des données (RGPD), dans la perspective de préserver l'intégrité des processus électoraux, tout en tenant compte des difficultés qui se posent à l'ère du numérique en matière de régulation et d'exécution.

La définition donnée par le règlement TTPA de la publicité à caractère politique est large, le terme désignant un message a) par, pour ou pour le compte d'un « acteur politique », sauf s'il s'agit d'un message à caractère purement privé ou commercial ; ou b) susceptible d'influencer le résultat d'une élection ou d'un référendum, un processus législatif ou réglementaire, ou encore un comportement de vote. La notion d'acteur politique est elle aussi définie à l'article 2 et recouvre un large éventail d'acteurs, notamment les partis politiques, les candidats et les organisations chargées de campagnes politiques. Le chapitre II du règlement TTPA définit des règles en matière de transparence pour la publicité à caractère politique ; il prévoit notamment la présence d'avis de transparence et d'informations relatives aux parraineurs, ce qui signifie entre autres que toute publicité à caractère politique doit être signalée comme telle et doit fournir des informations concernant son parraineur ainsi que toute entité contrôlant ce dernier, le cas échéant[192]. Le règlement TTPA interdit par conséquent certains types de contenus diffusés en ligne, à savoir ceux qui constituent des publicités à caractère politique non déclarées comme telles. Il proscrit de surcroît toute publicité à caractère politique émanant de parraineurs de pays extérieurs à l'Union dans les trois derniers mois précédant une élection ou un référendum[193]. Conformément aux obligations en matière de transparence fixées par l'article 12 du règlement TTPA, lorsqu'une publicité à caractère politique fait appel à des techniques de ciblage ou d'amplification reposant sur les données à caractère personnel, les responsables du traitement des données sont tenus d'assortir le message publicitaire d'informations supplémentaires, permettant à l'individu de saisir la logique sous-jacente à la technique employée, de comprendre les principaux paramètres régissant son utilisation et de savoir si des données tierces ou d'autres méthodes d'analyse ont été mises à contribution. Dans l'optique d'une plus grande transparence encore, l'article 13 du règlement TTPA impose à la Commission européenne de mettre en place un répertoire européen des annonces publicitaires à caractère politique en ligne, à l'instar du registre des publicités que doivent tenir certains intermédiaires dans le cadre du DSA.

La supervision et l'exécution font appel à différents acteurs, notamment aux autorités chargées de la protection des données, et imposent aux États membres de désigner une ou plusieurs autorités compétentes pour l'application, la supervision et

[191] Règlement (UE) 2024/900 du Parlement européen et du Conseil du 13 mars 2024 relatif à la transparence et au ciblage de la publicité à caractère politique, JO L 2024/900 du 20 mars 2024.
[192] Article 11, paragraphe 1, du règlement TTPA.
[193] Article 5, paragraphe 2, du règlement TTPA. Les termes « élection » ou « référendum » désignent tout type de processus électoral organisé à l'échelon de l'Union ou au niveau national, régional ou local dans un État membre.

l'exécution effectives du règlement TTPA[194]. Ces autorités disposent de divers moyens d'enquête et d'exécution, comportant notamment des demandes d'accès aux données ainsi que la compétence pour émettre des avertissements ou infliger des amendes[195]. Compte tenu de la nature transfrontière de certaines publicités en ligne à caractère politique, le règlement TTPA fixe également des règles en matière de compétence : dès lors qu'un prestataire de services de publicité à caractère politique propose ses services dans plus d'un État membre, il est généralement réputé relever de l'autorité ou des autorités compétentes de l'État membre dans lequel il est principalement établi.

Dans l'exercice de leurs pouvoirs de surveillance et d'exécution, les autorités compétentes de tous les États membres doivent toutefois coopérer et s'entraider en tant que de besoin, et utiliser pour ce faire les structures existantes, notamment les réseaux de coopération nationaux, le réseau européen de coopération électorale[196], le Comité européen des services numériques (EBDS) et le Comité européen pour les services de médias[197] (anciennement ERGA). À cet égard, l'article 23 du règlement TTPA encadre la coopération entre États membres et prévoit notamment une procédure de notification transfrontière. Les sanctions comprennent des amendes jusqu'à concurrence de 6 % du revenu ou du budget annuel du parraineur ou du prestataire de services de publicité à caractère politique, le montant le plus élevé étant retenu, ou de 6 % de son chiffre d'affaires annuel mondial au cours de l'exercice précédent. Les États membres peuvent adopter d'autres mesures et notamment imposer des astreintes[198].

2.2.2.4. Régulation du contenu relatif aux données à caractère personnel : le RGPD

Devenu le principal cadre juridique régissant le traitement des données à caractère personnel, le RGPD[199] énonce des règles et des principes relatifs à la protection des personnes physiques à l'égard dudit traitement, compte tenu de l'évolution rapide des technologies et de la mondialisation[200]. Son article 3 étend son champ d'application territorial pour y inclure notamment les activités des responsables du traitement et des sous-traitants de l'Union, que le traitement ait lieu ou non dans l'Union, ainsi que les responsables du traitement et les sous-traitants établis hors de l'Union, lorsqu'ils proposent des biens ou des services à des personnes concernées sur le territoire de l'Union. Pour ces responsables du traitement et sous-traitants, le RGPD fixe des obligations allant du principe de minimisation des données à des obligations de notification en cas de violation des données. Les personnes concernées se voient reconnaître de nombreux droits en lien avec

[194] Article 22, paragraphes 1 à 4, du règlement TTPA, qui prévoit que les autorités compétentes peuvent être différentes en fonction des différentes tâches de surveillance et d'exécution.
[195] Article 22, paragraphe 5, du règlement TTPA.
[196] Voir Commission européenne, « Terms of Reference, European Cooperation Network on Elections » définissant le cadre de référence du réseau.
[197] Article 22, paragraphe 8, du règlement TTPA.
[198] Article 25 et considérant 104 du règlement TTPA.
[199] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE [2016], JO L 119/1 du 4 mai 2016.
[200] Voir considérants 1 et suiv. du RGPD.

le traitement de leurs données à caractère personnel, tels que le droit de savoir si des données à caractère personnel les concernant font ou non l'objet d'un traitement (article 15), le droit de faire rectifier des données inexactes ou incomplètes (article 16), le droit à l'effacement (article 17), ou encore le droit de s'opposer au traitement de données à caractère personnel (article 21).

Le régime d'application du RGPD associe des mécanismes d'exécution nationaux, une coopération transfrontalière et des règles de coordination. Dans le cadre de son régime d'exécution administrative, chaque État membre doit mettre en place des autorités nationales de contrôle indépendantes[201], qui sont tenues de se plier aux mécanismes de coopération prévus par le RGPD[202].

Ces autorités sont investies d'importants pouvoirs d'enquête et d'exécution[203]. Chaque autorité de protection des données est compétente pour enquêter sur les réclamations introduites en vertu du RGPD sur le territoire de son État membre et, dans l'optique d'une application cohérente du règlement, pour coopérer avec les autres autorités de protection des données, au titre du mécanisme dit « de contrôle de la cohérence », qui fait appel au Comité européen de la protection des données[204] (CEPD). Dans le cadre du dispositif de guichet unique du RGPD, une autorité de contrôle chef de file, qui est l'autorité de protection des données dont relève l'établissement principal du responsable du traitement dans l'Union, a compétence lorsque l'affaire présente un caractère transfrontalier, mais les autres autorités de contrôle concernées doivent être informées et peuvent s'opposer à une décision proposée par l'autorité chef de file[205]. Les problèmes et les défis rencontrés dans le cadre de ce régime d'exécution, qui fait appel à différents acteurs, sont abordés dans un nouveau règlement procédural visant à harmoniser les conditions de recevabilité et les procédures dans les actions transfrontières[206]. L'article 83 du RGPD permet aux autorités de contrôle d'infliger des amendes administratives significatives, jusqu'à concurrence de 20 millions d'euros ou de 4 % du chiffre d'affaires annuel mondial des intéressés, le montant le plus élevé étant retenu. Les États membres doivent en outre déterminer d'autres sanctions applicables en cas de non-respect du règlement[207].

---

[201] Articles 51 et suiv. du RGPD.

[202] Pour une analyse de la façon dont le régime du RGPD s'efforce de répondre aux défis posés par la directive sur la protection des données à caractère personnel, voir A. Giurgiu et T. A. Larsen, « Roles and Powers of National Data Protection Authorities: Moving from Directive 95/46/EC to the GDPR: Stronger and More 'European' DPAs as Guardians of Consistency? », *European Data Protection Law Review*, 2(3), 2016, pp. 342–352.

[203] Article 58 du RGPD.

[204] Article 55 du RGPD.

[205] Pour un aperçu des mécanismes de coopération au titre de l'article 60 du RGPD, voir H. Hijmans, « The DPAs and their Cooperation: How Far Are We in Making Enforcement of Data Protection Law more European? », *European Data Protection Law Review*, 2(3), 2016, pp. 362–372.

[206] Le Conseil de l'UE et le Parlement européen sont parvenus le 16 juin 2025 à un accord politique sur un règlement établissant de nouvelles règles de procédure en matière d'application du RGPD. Voir Conseil de l'UE, « Protection des données : accord du Conseil et du Parlement européen pour que l'application transfrontière du RGPD fonctionne mieux pour les citoyens », communiqué de presse, 16 juin 2025. Pour un aperçu et une évaluation de la proposition de la Commission, voir L. Mustert, « The Commission Proposal for a New GDPR Procedural Regulation: Effective and Protected Enforcement Ensured? », *European Data Protection Law Review*, 9(4), 2023, pp. 454–464.

[207] Article 84 du RGPD.

Bien que le RGPD n'ait pas été conçu pour cibler spécifiquement les contenus illicites ou la désinformation, il joue indirectement un rôle important dans la lutte contre ceux-ci, en réglementant l'utilisation des données à caractère personnel dans le cadre de la modération, du profilage et du ciblage des contenus. En imposant par exemple des restrictions sur l'utilisation des données à caractère personnel pour le microciblage, le RGPD s'attaque à un puissant vecteur de propagation de la désinformation. Les principes de minimisation des données et de limitation des finalités constituent des contraintes supplémentaires pour les systèmes de ciblage. De plus, l'article 17 du RGPD, qui aborde le « droit à l'oubli », exige des autorités de protection des données qu'elles veillent, à la demande de la personne concernée, à ce que les intermédiaires suppriment les contenus dont la conservation enfreint le RGPD, le droit de l'Union ou le droit des États membres auquel est soumis le responsable du traitement. Une personne concernée a notamment le droit de faire effacer ses données à caractère personnel lorsque celles-ci ne sont plus nécessaires ou pertinentes[208].

2.2.2.5. Régulation des technologies de communication : le règlement sur l'IA

Le règlement sur l'IA[209] relève de la réglementation sur la sécurité des produits et institue à ce titre des dispositions relatives à la sécurité des technologies visées. Cependant, contrairement à la législation antérieure en la matière, il protège également les droits fondamentaux, encadre les utilisations de l'IA et intègre des principes éthiques. Par conséquent, s'il ne concerne pas directement l'application de règles relatives aux contenus, comme c'est le cas du RGPD, il peut néanmoins venir en appui à la lutte contre les risques que représentent la désinformation et les contenus illicites, en particulier dans le cas de contenus générés par des systèmes d'IA ou auxquels ces derniers donnent de l'écho. Ceci tient notamment au fait que le règlement sur l'IA s'attaque expressément au phénomène des « hypertrucages » (*deep fakes*), à savoir des images ou contenus audio ou vidéo générés ou manipulés par l'IA, présentant une ressemblance avec des personnes, des objets, des lieux, des entités ou des événements existants et pouvant être perçus à tort par une personne comme authentiques ou véridiques[210]. Le règlement vient en conséquence compléter d'autres textes législatifs sur le numérique, en ajoutant un niveau supplémentaire d'obligations pour l'utilisation des systèmes d'IA.

À l'instar du DSA, le règlement sur l'IA, axé sur les risques, instaure des obligations en matière de transparence, de responsabilité et d'atténuation des risques. Il prévoit des obligations différentes en fonction du degré de risque présenté par le système d'IA considéré. Son article 5 interdit les pratiques en matière d'IA présentant un risque inacceptable ; sont notamment visés les systèmes d'IA qui ont recours à des techniques

[208] C-131/12 *Google Spain SL, Google Inc. contre AEPD* [2014] ECLI:EU:C:2014:317 ; voir également S. Pouillaude, « Harmonising the Enforcement of the Right to Be Forgotten: Navigating New Speech Regulation Challenges in the EU », *European Data Protection Law Review*, 10(2), 2024, pp. 162–177.

[209] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle) [2024], JO L 2024/1689 du 12 juillet 2024.

[210] Article 3, paragraphe 60, du règlement sur l'IA.

délibérément manipulatrices ou trompeuses, susceptibles d'amener une personne à prendre une décision qu'elle n'aurait pas prise autrement. L'article 6 définit quant à lui les systèmes d'IA à haut risque comme des systèmes d'IA présentant un risque important pour la santé, la sécurité ou les droits fondamentaux des personnes physiques, et les soumet à des obligations juridiques et à une surveillance stricte. Il s'agit notamment d'exigences en matière de gestion des risques, de documentation technique et de tenue de registres, de transparence et de surveillance humaine[211]. Le règlement sur l'IA impose des règles spécifiques aux systèmes d'IA à usage général qui présentent des risques systémiques, tels que des effets négatifs réels ou raisonnablement prévisibles sur les processus démocratiques et la diffusion de contenus illicites, faux ou discriminatoires[212]. Il impose de surcroît des obligations de transparence aux fournisseurs et aux déployeurs de systèmes d'IA présentant des risques limités, par exemple les systèmes destinés à interagir avec des personnes physiques (comme les « dialogueurs » ou agents conversationnels), ou à générer des contenus audio, images, vidéos ou textes manipulés[213]. Ainsi, les systèmes d'IA utilisés pour générer ou manipuler des images ou des contenus audio ou vidéo qui ressemblent sensiblement à des personnes, des objets, des lieux, des entités ou des événements existants et pouvant être perçus à tort par une personne comme authentiques ou véridiques (hypertrucages) doivent indiquer que les sorties d'IA ont été créées ou manipulées artificiellement et mentionner leur origine artificielle[214]. Cette mesure permet aux utilisateurs de prendre conscience d'être en présence de contenus synthétiques. Les contenus qui ne sont pas étiquetés conformément à l'article 50 du règlement sur l'IA sont illicites.

L'exécution et la supervision du règlement sur l'IA suivent le nouveau cadre législatif de l'UE pour la législation applicable aux produits[215], qui a créé une boîte à outils de mesures à utiliser dans ce type de textes. Les États membres doivent établir ou désigner au moins une autorité notifiante et une autorité de surveillance du marché, qui exercent leurs pouvoirs en toute indépendance et impartialité[216]. Les autorités de surveillance du marché supervisent et contrôlent le respect des règles applicables aux systèmes d'IA, y compris les interdictions et les dispositions concernant les IA à haut risque, tandis que les autorités notifiantes désignent et chapeautent les organismes notifiés, qui sont des instances indépendantes qui procèdent à l'évaluation de la conformité des systèmes avant leur mise sur le marché. Il convient de relever dans ce contexte que, dans le cas des systèmes d'IA à haut risque, le contrôle du respect du règlement est intégré dans un système d'évaluation de conformité ex ante. Le nouveau Bureau de l'IA[217], créé à l'échelon de l'Union, permet de garantir une application et un contrôle harmonisés, notamment lorsqu'il s'agit de modèles d'IA à usage général[218]. Ce bureau est ainsi investi de pouvoirs d'enquête et d'exécution[219]. L'article 65 du règlement crée en outre un Comité européen de l'intelligence

[211] Articles 8 et suiv. du règlement sur l'IA.
[212] Voir l'article 55 et le considérant 110 du règlement sur l'IA.
[213] Article 50 du règlement sur l'IA.
[214] Article 50, paragraphe 4, du règlement sur l'IA.
[215] Voir le site web dédié de la Commission européenne.
[216] Article 70 du règlement sur l'IA.
[217] Article 64 du règlement sur l'IA.
[218] Voir l'article 88 du règlement sur l'IA.
[219] Voir les articles 88 et suiv. du règlement sur l'IA.

artificielle, chargé entre autres de faciliter la coordination entre les autorités nationales compétentes et de contribuer à l'harmonisation des pratiques administratives dans les États membres[220]. Le règlement sur l'IA prévoit un régime d'amendes administratives graduelles, jusqu'à concurrence de 35 millions d'EUR ou de 7 % du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu, en cas de non-respect de l'interdiction des pratiques en matière d'IA visées à l'article 5, et jusqu'à concurrence de 7,5 millions d'EUR ou 1 % du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu, pour la fourniture d'informations inexactes, incomplètes ou trompeuses aux organismes notifiés ou aux autorités nationales compétentes en réponse à une demande d'informations[221].

2.2.2.6. Autres approches visant à réglementer les contenus jugés illégaux

Outre la législation dérivée de l'Union présentée jusqu'ici, des instruments sectoriels régulent également les contenus en ligne jugés illégaux, et des dispositions de plus en plus harmonisées voient le jour en matière de droit pénal.

En ce qui concerne les contenus liés au terrorisme, le règlement sur les contenus à caractère terroriste[222] (dit TERREG ou règlement TCO) prévoit des mécanismes d'application et oblige les plateformes à prendre des mesures sélectives contre les contenus interdits. Il impose aux fournisseurs de services d'hébergement opérant dans l'Union de supprimer les contenus à caractère terroriste dans l'heure qui suit la réception d'une injonction de retrait[223]. En conséquence, le TERREG met en place un modèle de réponse rapide dans lequel l'exécution des obligations est directement assurée par les autorités nationales compétentes en vertu du règlement ; celles-ci sont chargées d'émettre les injonctions de retrait et d'imposer des sanctions. Les États membres déterminent le régime des sanctions administratives applicables aux violations du TERREG et veillent à ce que le non-respect systématique ou persistant des obligations soit passible de sanctions financières pouvant atteindre jusqu'à 4 % du chiffre d'affaires mondial du fournisseur de services[224]. Le règlement prévoit également une coopération entre les autorités nationales compétentes, les fournisseurs de services d'hébergement et Europol[225]. L'application du règlement est supervisée par la Commission européenne, à laquelle les États membres remettent chaque année un rapport sur les mesures prises conformément au TERREG, comportant notamment le nombre d'injonctions de retrait émises.

D'autres instruments législatifs de l'Union visent à harmoniser le statut d'illicéité de certains comportements en ligne ; c'est le cas de la directive sur la lutte contre la violence à l'égard des femmes et la violence domestique[226], qui fait de l'incitation à la violence ou à la haine fondée sur le sexe sur internet et du partage non consenti d'images intimes des

[220] Article 66 du règlement sur l'IA.
[221] Article 99 du règlement sur l'IA.
[222] Règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne, JO L 172/79 du 17 mai 2021.
[223] Article 3 du TERREG.
[224] Article 18 du TERREG.
[225] Article 14 du TERREG.
[226] Directive (UE) 2024/1385 du Parlement européen et du Conseil du 14 mai 2024 sur la lutte contre la violence à l'égard des femmes et la violence domestique, JO L 2024/1385 du 24 mai 2024.

infractions pénales, mais ne prévoit aucun mécanisme d'application spécifique autre que l'encouragement à la coopération en matière d'autorégulation entre les intermédiaires concernés, par exemple au moyen de codes de conduite. La criminalisation des discours de haine est également abordée dans la décision-cadre 2008/913/JAI[227] du Conseil, laquelle fournit une base de référence pour la qualification pénale des discours et crimes de haine dans l'ensemble des États membres, lorsqu'il s'agit de contenus racistes et xénophobes. Bien qu'il s'agisse d'un instrument de coopération intergouvernementale qui n'est pas applicable directement, la décision-cadre exige que les États membres transposent ses dispositions dans leur droit national, à des fins de rapprochement des législations. Par ailleurs, la proposition de règlement établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants[228] vise à instaurer des obligations en matière d'évaluation et d'atténuation des risques, de détection, de signalement et de retrait des contenus pédopornographiques, pouvant aller jusqu'à des mesures de filtrage proactif par les plateformes en ligne, un point qui fait l'objet de débats et de controverses[229]. Cette proposition vise à pallier les faiblesses d'une directive antérieure[230], qui exigeait le retrait et le blocage de ces contenus, sans pour autant réglementer dans le détail la procédure à suivre. Un mécanisme prévu par cette directive fournissait par ailleurs un cadre permettant aux États membres de prendre des mesures pour bloquer les sites web étrangers partageant du matériel pédopornographique. Sa mise en œuvre était toutefois facultative, de sorte que seule la moitié des États membres avait adopté une législation nationale spécifique.

2.2.3. Mesures ciblant les contenus illicites et préjudiciables dans le cadre de la PESC

Dans le cadre de la Politique étrangère et de sécurité commune (PESC), l'Union a adopté des mesures ciblées visant à lutter contre la diffusion de contenus illicites et préjudiciables par des acteurs étrangers, en particulier dans un contexte de campagnes de désinformation et de cybermenaces. Ces mesures sont généralement mises en œuvre par le biais de décisions et de règlements du Conseil, imposant des mesures restrictives à l'encontre des personnes ou entités responsables de réaliser ou de soutenir des activités de manipulation de l'information et d'ingérence menées depuis l'étranger (FIMI), qui menacent la sécurité, la démocratie ou l'ordre public de l'Union ou de ses États membres. En réaction à la guerre initiée par la Russie contre l'Ukraine, l'Union a pris des mesures qui ont conduit à la suspension des activités de diffusion et des licences de plusieurs médias contrôlés par l'État

[227] Décision-cadre 2008/913/JAI du Conseil du 28 novembre 2008 sur la lutte contre certaines formes et manifestations de racisme et de xénophobie au moyen du droit pénal, JO L 328/55 du 6 décembre 2008.
[228] Commission européenne, Proposition de règlement du Parlement européen et du Conseil établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants, COM(2022) 209 final, 2022.
[229] M. R. Leiser et A. D. Murray, « Rethinking Safety-by-Design and Techno-Solutionism for the Regulation of Child Sexual Abuse Material », *Technology and Regulation*, 2025, pp. 131–171.
[230] Directive 2011/93/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil, JO L 335/1 du 17 décembre 2011.

russe[231]. La révocation des licences n'ayant, dans les faits, pas empêché la diffusion de contenus dans l'Union, le Conseil de l'UE a adopté des sanctions qui prennent la forme d'une décision et d'un règlement interdisant aux opérateurs de diffuser ou de contribuer d'une autre manière à la diffusion, au sein de l'Union, de contenus provenant de certains médias contrôlés par l'État (en l'occurrence RT et Sputnik) et invoquant leur rôle dans la propagation de faits déformés et de la désinformation[232]. Ces mesures ont par la suite été étendues à plusieurs autres médias russes[233] et le Tribunal de l'Union européenne a confirmé qu'elles étaient compatibles avec les droits fondamentaux. Une requête déposée auprès de la CJUE par une coalition néerlandaise de fournisseurs d'accès à internet et d'organismes de presse, visant à obtenir l'annulation des ordonnances relatives à l'interdiction de diffuser ou de soutenir la diffusion des contenus émanant des entités sanctionnées, a été rejetée[234]. D'autres mesures restrictives ont suivi à l'encontre d'entités russes, visant cette fois également des personnes physiques, pour avoir mené des campagnes de désinformation[235].

Ces mesures, fondées sur la compétence de l'Union en matière d'action extérieure, témoignent de l'évolution du rôle de la PESC dans la lutte contre les menaces étrangères

---

[231] Pour un aperçu, voir F. J. Cabrera Blázquez, « Commission européenne : interdiction des médias russes Russia Today et Sputnik au sein de l'Union européenne », IRIS 2022-3:1/6, Observatoire européen de l'audiovisuel, Strasbourg, 2022, et « The Implemenation of EU Sanctions against RT and Sputnik », uniquement en anglais, Observatoire européen de l'audiovisuel, Strasbourg, 2022 ; M. D. Cole et C. Etteldorf, « Future Regulation of Cross-Border Audiovisual Content Dissemination », *Schriftenreihe Medienforschung der LfM NRW*, volume 84, Nomos, Baden-Baden, 2023, pp. 217 et suivantes.

[232] Règlement (UE) 2022/350 du Conseil du 1er mars 2022 modifiant le règlement (UE) no 833/2014 concernant des mesures restrictives eu égard aux actions de la Russie déstabilisant la situation en Ukraine, JO L 65/1 du 2 mars 2022 ; et Décision (PESC) 2022/351 du Conseil du 1er mars 2022 modifiant la décision 2014/512/PESC concernant des mesures restrictives eu égard aux actions de la Russie déstabilisant la situation en Ukraine, JO L 65/1 du 2 mars 2022.

[233] Par exemple : Règlement (UE) 2022/879 du Conseil du 3 juin 2022 modifiant le règlement (UE) nº 833/2014 concernant des mesures restrictives eu égard aux actions de la Russie déstabilisant la situation en Ukraine, JO L 153/53 du 3 juin 2022 et Règlement d'exécution (UE) 2022/994 du Conseil du 24 juin 2022 mettant en œuvre le règlement (UE) 2022/879 modifiant le règlement (UE) no 833/2014 concernant des mesures restrictives eu égard aux actions de la Russie déstabilisant la situation en Ukraine, JO LI 167/1 du 24 juin 2022 ; Règlement (UE) 2022/2474 du Conseil du 16 décembre 2022 modifiant le règlement (UE) no 833/2014 concernant des mesures restrictives eu égard aux actions de la Russie déstabilisant la situation en Ukraine, JO L 322/1 du 16 décembre 2022 et Règlement d'exécution (UE) 2023/180 du Conseil du 27 janvier 2023 mettant en œuvre le règlement (UE) 2022/2474 modifiant le règlement (UE) no 833/2014 concernant des mesures restrictives eu égard aux actions de la Russie déstabilisant la situation en Ukraine, JO L 26/1 du 30 janvier 2023 ; Règlement (UE) 2023/427 du Conseil du 25 février 2023 modifiant le règlement (UE) nº 833/2014 concernant des mesures restrictives eu égard aux actions de la Russie déstabilisant la situation en Ukraine, JO L 59/6 du 25 février 2023 et Règlement d'exécution (UE) 2023/722 du Conseil du 31 mars 2023 mettant en œuvre le règlement (UE) 2023/427 modifiant le règlement (UE) nº 833/2014 concernant des mesures restrictives eu égard aux actions de la Russie déstabilisant la situation en Ukraine, JO L 94/19 du 3 avril 2023.

[234] T-307/22 *A2B Connect e. a. contre Conseil* (Tribunal, 26 mars 2025) ECLI:EU:T:2025:331. WE WILL CHECK AT THE END BEFORE PRINT WHETHER THERE WAS AN APPEAL. Voir également, précédemment, T-125/22 *RT France c. Conseil* (Tribunal, 27 juillet 2022) ECLI:EU:T:2022:483.

[235] Décision (PESC) 2023/1566 du Conseil du 28 juillet 2023 modifiant la décision 2014/145/PESC concernant des mesures restrictives eu égard aux actions compromettant ou menaçant l'intégrité territoriale, la souveraineté et l'indépendance de l'Ukraine, JO L 190/21 du 28 juillet 2023 ; Règlement d'exécution (UE) 2023/1563 du Conseil du 28 juillet 2023 mettant en œuvre le règlement (UE) no 269/2014 concernant des mesures restrictives eu égard aux actions compromettant ou menaçant l'intégrité territoriale, la souveraineté et l'indépendance de l'Ukraine, JO L 190/1 du 28 juillet 2023.

en matière d'information et viennent compléter les efforts de réglementation internes déployés dans le cadre d'instruments tels que le DSA. Elles permettent en outre de mieux comprendre l'évolution du cadre réglementaire, par exemple des règles relatives aux services de médias malhonnêtes et de la coopération accélérée dans le cadre du règlement européen sur la liberté des médias[236].

Dans le cadre de ce qui était alors le deuxième pilier de l'Union en matière de politique étrangère et de sécurité commune, le Service européen pour l'action extérieure (SEAE) s'est également montré particulièrement actif dans la lutte contre la désinformation. Depuis 2015, le SEAE rend compte régulièrement des questions de désinformation, y compris des tentatives d'ingérence électorale et des activités de manipulation de l'information et d'ingérence menées depuis l'étranger (FIMI), sur son site web de sensibilisation EUvsDisinfo[237], ainsi que sur les réseaux sociaux. Il s'est d'abord appuyé, pour ce faire, sur les conclusions du Conseil européen en matière de relations extérieures du 19 mars 2015[238], avant d'inscrire son action dans le cadre du plan d'action contre la désinformation de la Haute représentante de l'Union pour les affaires étrangères et la politique de sécurité du 5 décembre 2018[239].

En 2022, le SEAE a adopté une « boussole stratégique » en matière de sécurité et de défense, prévoyant la mise en place d'une boîte à outils relative aux activités de manipulation de l'information et d'ingérence menées depuis l'étranger ; elle vise à renforcer la capacité de l'Union à détecter et à analyser la menace, mais aussi à y répondre, et à continuer d'améliorer ses capacités de communication stratégique et de lutte contre la désinformation[240]. Cette boîte à outils couvre différents domaines et présente des mesures à court, moyen et long terme pour lutter contre ce type d'activités. Ces mesures vont des contre-mesures en amont des incidents (telles que les programmes d'éducation aux médias) à des contre-mesures consécutives aux incidents (notamment le partage d'informations et le recours à des réponses juridiques et à des sanctions), en passant par des contre-mesures de minimisation[241] (telles que la suppression de contenus en ligne en fonction des réglementations ou des mécanismes existants). Comme dans le domaine de la cybersécurité, l'accent est mis sur le partage d'informations, afin d'améliorer le degré de préparation. En conséquence, un centre de partage et d'analyse de l'information consacré aux activités de manipulation de l'information et d'ingérence menées depuis l'étranger

[236] À cet égard, voir S. Eskens, « The Role of Regulation on the Transparency and Targeting of Political Advertising and European Media Freedom Act in the EU's Anti-Disinformation Strategy », *Computer Law & Security Review*, 58, 2025, 106185.
[237] Voir https://euvsdisinfo.eu/.
[238] Conseil européen, Réunion du Conseil européen (19 et 20 mars 2015) – Conclusions, (2015) EUCO 11/15.
[239] Commission européenne, Haute représentante de l'Union pour les affaires étrangères et la politique de sécurité, Communication conjointe au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions - Plan d'action contre la désinformation, JOIN(2018) 36 final.
[240] SEAE, « Une boussole stratégique en matière de sécurité et de défense », 2022, p. 46.
[241] SEAE, « 2nd EEAS Report on Foreign Information Manipulation and Interference Threats » (Deuxième rapport du SEAE sur les menaces de manipulation de l'information et d'ingérence étrangères), uniquement en anglais, janvier 2024, p. 17 et suiv.

(FIMI-ISAC) a vu le jour en 2023 ; il prend la forme d'un réseau décentralisé faisant appel à la société civile et à d'autres parties prenantes[242].

[242] SEAE, « EEAS Stratcom's Responses to Foreign Information Manipulation and Interference (FIMI) in 2023 », communiqué de presse, 28 juin 2024.

3. Lutte contre la désinformation

3.1. Mesures d'exécution à l'échelon de l'UE

Dr *Mark D. Cole, Directeur des affaires académiques à l'Institut européen des médias (EMR) et professeur en droit des médias et des télécommunications à l'université du Luxembourg*

La désinformation peut revêtir de nombreuses formes qui sont pour beaucoup jugées problématiques. Le terme recouvre ainsi la désinformation politique[243], la désinformation en matière de santé[244], les théories du complot[245], les *deep fakes* ou hypertrucages[246] et les médias manipulés[247], ainsi que les opérations d'influence étrangère. Par ailleurs, certaines escroqueries, par exemple les faux placements, ainsi que certaines manipulations sociales et culturelles, telles que les rumeurs destinées à attiser les tensions raciales, religieuses ou ethniques, peuvent relever elles aussi de ce terme générique, dès lors que des contenus erronés ou trompeurs sont utilisés pour induire en erreur les internautes et profiter d'eux financièrement ou pour causer un préjudice public.

La section qui suit se concentre sur la désinformation orchestrée par les États, afin d'illustrer combien les campagnes de désinformation dans l'Union ont changé d'envergure et de qualité. Parallèlement, on observe un renforcement des mesures et de leur application au moyen de solutions juridiques contraignantes.

À l'échelon de l'Union, plusieurs initiatives contre la désinformation ont vu le jour depuis 2015, année où le Conseil européen soulignait « la nécessité de contrer les campagnes de désinformation menées par la Russie[248] », dans le sillage de l'annexion illégale de la Crimée par celle-ci en 2014. Si les premières mesures stratégiques étaient axées sur les menaces dites « hybrides[249] » (c'est-à-dire les activités menées par des acteurs

[243] Voir Commission européenne, « Digital Services Act – Application of the Risk Management Framework to Russian Disinformation Campaigns », Office des publications de l'Union européenne, Luxembourg, 2023.
[244] Commission européenne et haut représentant de l'Union pour les affaires étrangères et la politique de sécurité, Communication conjointe au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions – Lutter contre la désinformation concernant la COVID-19 – Démêler le vrai du faux, 2020.
[245] Voir le site dédié de la Commission européenne, « Identifying Conspiracy Theories » (« Identifier les théories du complot »).
[246] Europol, « Facing Reality? Law Enforcement and the Challenges of Deepfakes », Office des publications de l'Union européenne, Luxembourg, 2022, p. 10 et suiv.
[247] A. Marwick et R. Lewis, *Media Manipulation and Disinformation Online*, Data & Society Research Institute, 2017 ; C. Wardle et H. Derakhshan, « Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making », rapport du Conseil de l'Europe DGI(2017)09, p. 20 et suiv. Voir également le site dédié de la Commission européenne, « Communication stratégique et lutte contre les activités de manipulation de l'information et d'ingérence menées depuis l'étranger ».
[248] Conseil européen, Réunion du Conseil européen (19 et 20 mars 2015) – Conclusions, 2015.
[249] Avec, par exemple, le lancement de la *task force* East Stratcom en 2015 et la communication conjointe sur la lutte contre les menaces hybrides (Commission européenne et haute représentante de l'Union pour les affaires étrangères et la politique de sécurité, Communication conjointe au Parlement européen et au Conseil – Cadre commun en matière de lutte contre les menaces hybrides – Une réponse de l'Union européenne, 2016). Voir

étatiques ou non, faisant appel à un mélange de méthodes militaires et non militaires sans déclaration de guerre officielle), les suivantes ont visé à élargir le périmètre de ces initiatives à la « désinformation », entendue comme désignant des « informations dont on peut vérifier qu'elles sont fausses ou trompeuses, qui sont créées, présentées et diffusées dans un but lucratif ou dans l'intention délibérée de tromper le public et qui sont susceptibles de causer un préjudice public[250] ». Cette définition a été intégrée en 2018 dans une communication de la Commission sur la lutte contre la désinformation en ligne[251], par laquelle la Commission européenne appuyait la mise en place d'un code de bonnes pratiques contre la désinformation, destiné aux plateformes en ligne et aux annonceurs. Le texte annonçait l'adoption d'éventuelles mesures d'ordre réglementaire, si ce code « devai[t] ne pas être satisfaisan[t][252] ». Le *Code of Practice on Disinformation* (Code de bonnes pratiques contre la désinformation) de l'Union européenne a fini par être publié et signé en octobre 2018[253]. Pour la première fois, les acteurs du secteur se sont volontairement accordés sur des normes d'autorégulation destinées à lutter contre la désinformation, marquant ainsi le passage de simples actions politiques à des mesures juridiques. Invoquant la communication de la Commission et répondant à l'appel du Conseil européen en faveur de mesures visant à « protéger les systèmes démocratiques de l'Union et lutter contre la désinformation, y compris dans le contexte des élections européennes à venir[254] », la Commission européenne et la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité ont ensuite publié une communication conjointe relative à un plan d'action contre la désinformation[255]. Ce dernier prévoit notamment la création d'un Observatoire européen des médias numériques (EDMO) indépendant[256], pensé comme une plateforme fédérant une communauté transfrontière et pluridisciplinaire de vérificateurs de faits indépendants, de chercheurs universitaires et d'autres parties prenantes, tous amenés à collaborer. Les activités de l'EDMO consistent notamment à cartographier les organisations de vérification des faits et à soutenir les pouvoirs publics dans le suivi des politiques mises en place par les plateformes en ligne en vue de limiter la propagation et l'impact de la désinformation.

Si le plan d'action contre la désinformation portait sur le phénomène au sens large, la Covid-19 a incité la Commission européenne et le haut représentant de l'Union pour les affaires étrangères et la politique de sécurité à se concentrer sur des initiatives plus ciblées,

également Parlement européen, Résolution du Parlement européen du 23 novembre 2016 sur la communication stratégique de l'Union visant à contrer la propagande dirigée contre elle par des tiers, 2016.

[250] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions – Lutter contre la désinformation en ligne : une approche européenne, COM(2018) 236 final, 26 April 2018.

[251] *Ibid.*

[252] *Ibid.*, section 3.1.1.

[253] Commission européenne, *Code of Practice on Disinformation*, 2018.

[254] Conseil européen, Conclusions du Conseil européen, communiqué de presse, 18 octobre 2018.

[255] Commission européenne et haute représentante de l'Union pour les affaires étrangères et la politique de sécurité, Communication conjointe au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions – Plan d'action contre la désinformation, 2018.

[256] L'EDMO est géré par un consortium dirigé par le European University Institute de Florence, en Italie, et est entièrement indépendant des autorités publiques, y compris de la Commission européenne. Pour de plus amples informations, voir https://digital-strategy.ec.europa.eu/en/policies/european-digital-media-observatory.

dans le contexte de la désinformation liée à la pandémie[257]. Afin de compléter les mesures axées sur la lutte contre la désinformation, la Commission européenne s'est emparée du sujet sous forme d'autres instruments stratégiques spécialisés, tels que le plan d'action pour la démocratie européenne[258], qui vise à renforcer la démocratie par la promotion d'élections libres et équitables, le soutien aux médias libres et indépendants, et la lutte contre la désinformation.

Une première évaluation de la mise en œuvre du code de bonnes pratiques contre la désinformation en septembre 2020 a permis de recenser plusieurs manquements[259] et a conduit à la publication d'un code de bonnes pratiques renforcé le 16 juin 2022[260]. Le 13 février 2025, la Commission européenne et le Comité européen des services numériques[261] (EBDS) ont approuvé l'intégration de ce nouveau code de 2022 dans le cadre juridique du règlement sur les services numériques[262] ; il est devenu à cette occasion le « *Code of Conduct on Disinformation* » (Code de conduite sur la désinformation)[263]».

C'est par conséquent ce texte qui sert d'étalon de mesure pertinent pour évaluer le respect du DSA en matière de risques de désinformation par les fournisseurs de très grandes plateformes en ligne (TGP) et de très grands moteurs de recherche en ligne[264] (TGMR) qui suivent et défendent ses engagements[265]. Ces derniers sont regroupés par domaines : placements de publicité, publicité à caractère politique, intégrité des utilisateurs, responsabilisation des utilisateurs, responsabilisation de la communauté de la recherche, responsabilisation de la communauté des vérificateurs de faits, création et maintien d'un centre pour la transparence, création d'une *task force* permanente, et suivi de l'application du code. S'agissant par exemple des placements de publicité, les signataires s'engagent notamment à démonétiser la désinformation (entre autres en s'abstenant, pour les fournisseurs de technologie publicitaire, de placer des publicités sur des sites web connus pour diffuser régulièrement de la désinformation) et à prévenir l'utilisation abusive des systèmes publicitaires pour diffuser de la désinformation sous forme de messages publicitaires[266]. Pour ce qui est de la responsabilisation de la communauté des vérificateurs

[257] Commission européenne et haut représentant de l'Union pour les affaires étrangères et la politique de sécurité, Communication conjointe au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions – Lutter contre la désinformation concernant la COVID-19 – Démêler le vrai du faux, 2020.

[258] Commission européenne, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions relative au plan d'action pour la démocratie européenne, 2020. Ce plan d'action est également annoncé par le règlement sur les services numériques (DSA) et le règlement relatif à la transparence et au ciblage de la publicité à caractère politique (règlement TTPA), dont il est question dans les pages qui suivent.

[259] Commission européenne, document de travail des services de la Commission, *Assessment of the Code of Practice on Disinformation – Achievements and Areas for further Improvement*, SWD(2020) 180 final.

[260] Commission européenne, *Strengthened Code of Practice on Disinformation* (Code de bonnes pratiques renforcé contre la désinformation »), 2022.

[261] Voir chapitre 2.2.2.2.

[262] Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques – DSA), JO L 277 du 27 octobre 2022.

[263] Commission européenne, *Code of Conduct on Disinformation*, 2025.

[264] Pour les notions de TGP et de TGMR, voir le chapitre 2.2.2.2.

[265] L'intégration du code de conduite sur la désinformation dans le cadre du DSA a pris effet au 1er juillet 2025.

[266] Commission européenne, Code of Conduct on Disinformation, 2025, p. 10 et suiv.

de faits, leur activité joue un rôle important pour la lutte contre les risques liés à la désinformation et aux contenus illégaux dans le cadre du DSA[267]. Si ce dernier n'impose pas directement la vérification des faits, le code de conduite reconnaît cette pratique comme une mesure d'atténuation essentielle dans le cadre plus large de la gestion des risques systémiques. Il demande donc à ses signataires de s'engager à coopérer avec les vérificateurs de faits, y compris pour ce qui est des ressources et du soutien mis à la disposition de ces derniers[268].

L'incorporation du code de bonnes pratiques contre la désinformation dans le cadre du DSA peut être considérée comme une réponse plus ferme, comparée aux engagements limités pris antérieurement et à l'efficacité restreinte des initiatives et actions précédemment menées par les TGP et les TGMR[269].

Le code de conduite proprement dit ne précise pas les modalités de la vérification des faits. Afin de promouvoir et d'améliorer la qualité de ces opérations, les organismes spécialisés dans ce domaine ont mis en place le Réseau européen des normes de vérification des faits[270] (European Fact-Checking Standards Network – EFCSN). Il s'agit d'une association dont les membres s'engagent à respecter certaines normes de qualité énoncées dans un code européen de normes organismes indépendants de vérification des faits[271]. Ce code constitue un outil d'autorégulation pour les vérificateurs de faits et fournit notamment une méthodologie permettant de vérifier l'exactitude des affirmations formulées dans l'espace public, ainsi que des normes éthiques.

Il convient de distinguer ces acteurs des « signaleurs de confiance », soumis directement au DSA. Ceux-ci sont désignés par les organismes de régulation nationaux (les coordinateurs pour les services numériques) et doivent répondre à des critères stricts en matière d'expertise, d'indépendance, de transparence et d'exactitude. Ils se concentrent sur le respect de la loi, et pas seulement sur la précision ou la véracité. C'est la raison pour laquelle ils se voient attribuer un statut prioritaire dans le dispositif de notifications et d'actions évoqué plus haut. Les vérificateurs de faits, quant à eux, aident les plateformes à étiqueter, contextualiser ou déclasser les contenus faux ou mensongers, plutôt que de demander leur suppression. Comme évoqué plus haut, les organismes de vérification des faits ne constituent pas une catégorie d'acteurs officiellement définie dans le DSA ; ils jouent toutefois un rôle important en matière d'atténuation des risques.

L'intégration de la vérification des faits peut entrer en tension avec le modèle économique des plateformes et la dynamique des utilisateurs. Les fournisseurs de réseaux sociaux explorent par conséquent d'autres solutions, à l'instar des « notes de la communauté[272] » déployées par X, qui visent à lutter contre la désinformation grâce à une vérification des faits collaborative. Le dispositif permet aux utilisateurs inscrits d'apporter du contexte ou des corrections à des publications potentiellement mensongères, en les

[267] *Ibid.*, p. 37 et suiv.
[268] *Ibid.*
[269] Voir EDMO, *Implementing the EU Code of Practice on Disinformation – An Evaluation of VLOPSE Compliance and Effectiveness (January-June 2024)*, EDMO, Florence, juin 2025.
[270] Voir https://efcsn.com/.
[271] Le code européen de normes à l'intention des organismes indépendants de vérification des faits est publié sur le site de l'EFCSN.
[272] Voir https://help.x.com/fr/using-x/community-notes.

affichant sous forme de notes sous le message d'origine. Ce mécanisme fait l'objet d'une procédure formelle ouverte par la Commission européenne à l'encontre de X depuis le 18 décembre 2023, qui porte notamment sur le respect des obligations relatives à la lutte contre la diffusion de contenus illicites dans l'Union et l'efficacité des mesures prises pour combattre la manipulation de l'information sur la plateforme[273]. Si les conclusions préliminaires de l'enquête ont mis en évidence des violations des obligations prévues par le DSA, l'enquête sur la modération des contenus, entre autres, était toujours en cours en août 2025. En janvier 2025, la Commission européenne a adressé plusieurs demandes d'informations à X, notamment des demandes d'accès aux interfaces de programmation d'applications (API), afin de procéder à l'évaluation – complexe – des risques systémiques et de leur atténuation[274].

Les rapports de transparence que sont tenus d'établir tous les fournisseurs de services intermédiaires permettent de mieux cerner les pratiques en matière de modération des contenus ; ils révèlent également le nombre de demandes de suppression, leur origine et leur traitement (voir également ci-dessus). En outre, la base de données relative à la transparence établie en vertu du DSA fournit des données empiriques sur les exposés des motifs soumis par les fournisseurs à la Commission. Toutefois, au-delà d'une synthèse du nombre total d'exposés des motifs communiqués, ces données ne donnent qu'un aperçu limité du type d'infractions, la catégorie la plus fréquemment rapportée étant « autre violation des conditions générales du fournisseur[275] ».

À l'échelon de l'Union, il existe également des mesures ciblées contre la désinformation dans des contextes spécifiques ; ainsi, lors des élections de 2024 au Parlement européen, une coopération sans précédent a été mise en place, afin de coordonner les réponses à la manipulation et à l'ingérence étrangères en matière d'information (FIMI) et à la désinformation[276]. Elle s'est notamment inscrite dans le cadre de structures spécifiques, telles que le réseau européen de coopération électorale[277], et a pris la forme de plusieurs mesures clés adoptées en réponse aux atteintes à l'intégrité du processus électoral, qui ont nécessité la collaboration et la coopération des institutions de l'Union, des États membres et de diverses entités, notamment les médias, les vérificateurs de faits et les organisations de la société civile[278]. En avril 2024, l'activation du dispositif

[273] Commission européenne, « La Commission ouvre une procédure formelle à l'encontre de X au titre du règlement sur les services numériques », communiqué de presse, 18 décembre 2023.
[274] Commission européenne, « La Commission adresse des mesures d'enquête supplémentaires à X dans le cadre des procédures en cours au titre de la législation sur les services numériques », communiqué de presse, 17 janvier 2025.
[275] Des recherches ont montré qu'il s'agissait dans plus de 99,8 % des cas d'infractions aux conditions générales. Voir R. Kaushal *et al.*, « *Automated Transparency: A Legal and Empirical Analysis of the Digital Services Act Transparency Database* », *FAccT '24: Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency, June 3-6, 2024, Rio de Janeiro, Brazil*, ACM, New York, 2024, pp. 1121-1132.
[276] Voir Commission européenne, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions – Rapport sur les élections au Parlement européen de 2024, Com(2025) 287 final, 2025.
[277] Voir Commission européenne, Terms of Reference, European Cooperation Network on Elections.
[278] Voir *ibid.*, p. 13 et suiv.

intégré pour une réaction au niveau politique dans les situations de crise[279] (IPCR) par la présidence belge du Conseil a permis une prise de décision politique rapide et coordonnée à l'échelon de l'Union, notamment en facilitant la circulation de l'information entre les États membres et les institutions européennes en matière de désinformation[280]. Des mesures de suivi et des actions adoptées dans le cadre du réseau contre la désinformation de la Commission européenne sont venues compléter cette initiative ; ce réseau, mis en place au titre du plan d'action contre la désinformation, constitue un autre mécanisme interne de la Commission pour combattre la désinformation[281]. L'EDMO a quant à lui fourni des informations actualisées sur les discours de désinformation diffusés dans l'Union[282], tandis que des renseignements complémentaires ont pu être extraits des rapports remis par les fournisseurs de plateformes en ligne sur les mesures prises par leurs soins pour protéger l'intégrité des processus électoraux, conformément à leurs engagements au titre du code de bonnes pratiques contre la désinformation et à leurs obligations de notification au titre du DSA. L'article 34, paragraphe 1, point c), du DSA, en particulier, exige des fournisseurs de TGP et de TGMR qu'ils évaluent et atténuent les risques systémiques pesant sur les processus électoraux et le discours civique, y compris les risques de désinformation. Les lignes directrices à l'intention des fournisseurs de TGP et de TGMR concernant l'atténuation des risques systémiques pour les processus électoraux[283] comportaient également des conseils quant aux mesures d'atténuation des risques à mettre en place, spécifiquement lors des élections. Les coordinateurs pour les services numériques désignés dans le cadre du DSA ont également mis en place des mesures, principalement sous la forme d'une coordination et d'une mobilisation des parties prenantes dans leur contexte national, en complément des efforts de la Commission européenne[284]. En ce qui concerne le code de bonnes pratiques contre la désinformation, ses signataires ont mis sur pied un système de réaction rapide qui permet aux participants, autres que des plateformes, de communiquer rapidement les informations qu'ils jugent potentiellement préjudiciables à l'intégrité des

[279] EU, Décision d'exécution (UE) 2018/1993, du Conseil du 11 décembre 2018 concernant le dispositif intégré de l'Union européenne pour une réaction au niveau politique dans les situations de crise, JO L 320/28 du 17 décembre 2022. Ce dispositif prévoit un mécanisme de gestion de crise en appui à la présidence du Conseil de l'UE pour faire face aux catastrophes naturelles ou aux catastrophes d'origine humaine transsectorielles de grande ampleur.

[280] Conseil de l'UE, « Ingérence étrangère : la présidence renforce l'échange d'informations dans la perspective des élections européennes de juin 2024 », communiqué de presse, 24 avril 2024.

[281] Commission européenne, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions – Rapport sur les élections au Parlement européen de 2024, Com(2025) 287 final, 2025, p. 15.

[282] Voir le bulletin sur la désinformation dans le cadre des élections européennes de l'EDMO, EU Elections Disinfo Bulletin.

[283] Commission européenne, Communication de la Commission – Lignes directrices de la Commission à l'intention des fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne sur l'atténuation des risques systémiques pour les processus électoraux, présentées en vertu de l'article 35, paragraphe 3, du règlement (UE) 2022/2065, [2024] JO C 2024/3014 du 26 avril 2024. Concernant ces lignes directrices, voir également le rapport du Comité européen des services numériques sur les élections européennes, *Report on the European Elections, Digital Services Act and Code of Practice on Disinformation*, Office des publications de l'Union européenne, Luxembourg, 2024, p. 11.

[284] Comité européen des services numériques, *Report on the European Elections, Digital Services Act and Code of Practice on Disinformation*, p. 13 et suiv.

processus électoraux, contribuant ainsi à dresser un tableau complet des campagnes de désinformation[285].

En résumé, du point de vue des institutions de l'Union, les engagements en matière d'autorégulation et les obligations incombant aux fournisseurs de TGP et de TGMR, la coopération menée dans le cadre de structures spécifiques, la facilitation des échanges d'informations et le renforcement de leur collecte, complétés par plusieurs exercices de simulation, ont permis d'améliorer le degré de préparation de l'Union et de faciliter la détection des risques[286]. Désormais, ces mesures sont de plus en plus souvent complétées par une législation contraignante visant à combattre spécifiquement la désinformation. Citons notamment le nouveau règlement relatif à la transparence et au ciblage de la publicité à caractère politique[287] (règlement TTPA), qui instaure des règles communes à l'UE pour lutter contre certaines pratiques problématiques dans la diffusion de la publicité à caractère politique dans l'Union, y compris les financements extérieurs. En outre, la coopération réglementaire accélérée dans le cadre du règlement européen sur la liberté des médias (EMFA) vise à faciliter l'adoption d'une réaction rapide face à la désinformation étrangère venant de « services de médias malhonnêtes » qui mettent en danger la sécurité publique d'un État membre[288]. Il reste à voir dans quelle mesure les États membres opteront pour la solution prévue par le règlement européen sur la liberté des médias, consistant à bloquer les services de médias non européens au sein de l'Union par le biais de mesures nationales prises par les autorités chargées des médias sous la coordination du Comité européen des services de médias (EBMS) nouvellement créé, ou pour des sanctions imposées par le Conseil de l'UE.

[285] Les acteurs concernés ont détecté et dénoncé diverses tentatives visant à induire en erreur les électeurs par la désinformation, par exemple en diffusant des informations erronées concernant les modalités de vote ou les politiques européennes. Voir Commission européenne, « European Elections: EU Institutions Prepared to Counter Disinformation », communiqué de presse, 5 juin 2024.

[286] Commission européenne, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions – Rapport sur les élections au Parlement européen de 2024, Com(2025) 287 final, 2025, 6 juin 2025, p. 18 ; Comité européen des services numériques, *Report on the European Elections, Digital Services Act and Code of Practice on Disinformation*, 2024, p. 18 et suiv.

[287] Règlement (UE) 2024/900 du Parlement européen et du Conseil du 13 mars 2024 relatif à la transparence et au ciblage de la publicité à caractère politique, JO L 2024/900 du 20 mars 2024.

[288] Article 13, paragraphe 1, point l), et article 17 du règlement européen sur la liberté des médias. Pour un aperçu de la façon dont l'EMFA et le règlement TTPA complètent la stratégie de l'Union en matière de désinformation, voir S. Eskens, « The Role of Regulation on the Transparency and Targeting of Political Advertising and European Media Freedom Act in the EU's Anti-Disinformation Strategy », *Computer Law & Security Review*, 58 - 106185, 2025.

3.2. L'exemple de la Roumanie

Dr Roxana Radu, professeure associée en technologies numériques et politiques publiques, Blavatnik School of Government, Université d'Oxford

3.2.1. Cadre juridique national relatif aux plateformes

Les plateformes en ligne exercent une influence significative sur le quotidien des citoyens roumains. Ces derniers sont fortement dépendants de Facebook, WhatsApp, YouTube et TikTok qui constituent leurs principales sources d'information[289] (y compris pour l'actualité). Dans un pays où le taux d'alphabétisation numérique est l'un des plus faible en Europe[290], la propagation de fausses informations et de désinformation a atteint un premier pic pendant la pandémie de Covid-19[291] avant de continuer à façonner l'opinion publique jusqu'à aboutir à l'annulation de l'élection présidentielle de 2024.

L'approche de la Roumanie à l'égard des plateformes en ligne consiste à harmoniser sa législation nationale avec les textes juridiques de l'Union européenne, dans l'optique d'un marché unique numérique cohérent. Les plateformes en ligne sont tenues de respecter la législation nationale, par exemple la *Lege nr. 365/2002 privind comerțul electronic* (loi relative au commerce électronique) qui pose des règles fondamentales concernant les transactions en ligne, ainsi que la réglementation européenne, et notamment le RGPD[292] et le DSA, qui visent à protéger les droits fondamentaux des utilisateurs en imposant aux plateformes des obligations en matière de transparence, de responsabilité et de respect des règles.

Ainsi que le détaille le chapitre 2 de la présente publication, le DSA instaure des obligations pour les intermédiaires. Pour les TGP et les TGMR, c'est la Commission européenne qui joue le rôle d'autorité compétente, en étroite collaboration avec les coordinateurs pour les services numériques désignés au niveau national. En Roumanie, ce rôle revient à l'Autorité nationale de gestion et de régulation des communications (ANCOM).

L'autre autorité pertinente est le Conseil national de l'audiovisuel (CNA), qui, selon l'évaluation réalisée en 2025 par la Commission européenne, continue de « manquer de personnel et de ressources technologiques suffisants pour remplir son mandat, en particulier dans le contexte de la mise en œuvre du règlement sur les services numériques[293] ». Le mandat du CNA a été élargi à l'occasion de la transposition en droit

[289] Institut Reuters pour l'étude du journalisme, *Digital News Report 2025 – Romania*, 2025.
[290] Projet TRIO, *Romania National Report Summary*, mars 2023 ; Issue Monitoring, *Romania's Digital Environment: Navigating the Path to a Tech-Driven Future*, 23 août 2024.
[291] EU DisinfoLab, *Disinformation Landscape in Romania*, Septembre 2023.
[292] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JO L 119 du 4 mai 2016.
[293] Commission européenne – Resource Centre on Media Freedom, 2025 Rule of Law Report – Country Chapter: Romania, juillet 2025.

national de la directive européenne sur les services de médias audiovisuels[294] (directive SMA), et des modifications ont été apportées en conséquence à la *Legea audiovizualului nr. 504/2002* (loi nº 504/2022 relative à l'audiovisuel) ainsi qu'à l'*Ordonata Guvernului nr. 39/2005 privind cinematografia* (Ordonnance gouvernementale nº 39/2005 relative à la cinématographie). Depuis ces changements, les plateformes de streaming (fournisseurs de vidéo à la demande) sont tenues de reverser une partie des recettes qu'elles génèrent localement, soit sous forme de prélèvements, soit en investissant dans l'industrie cinématographique nationale, selon des conditions bien définies[295].

Mis à part l'alignement de sa réglementation sur celle de l'Union, la Roumanie a adopté très peu d'initiatives axées sur la sensibilisation du grand public et les contenus en ligne de qualité. Elle n'a érigé en priorités ni les programmes d'éducation numérique, ni la vérification indépendante des faits, ni le financement de la recherche publique ou du journalisme local ; la résistance de la société civile à la désinformation reste ainsi insuffisante et l'offre tout comme la demande en la matière ne sont pas à l'ordre du jour[296].

3.2.2. Règles spécifiques en matière de désinformation

La montée en puissance de la désinformation en ligne s'est manifestée avec une acuité particulière pendant la pandémie de Covid-19, au cours de laquelle un décret présidentiel déclarant l'état d'urgence a autorisé le gouvernement à adopter toutes les mesures jugées nécessaires pour freiner la propagation de fausses informations, lui conférant notamment le pouvoir de fermer les sources de « *fake news* » (intox), par l'intermédiaire de l'ANCOM[297]. La vulnérabilité des citoyens à l'« infodémie[298] » liée à la Covid en Roumanie a compté parmi les plus élevées en Europe ; en témoignent la croyance répandue dans les théories du complot et les faibles taux de vaccination[299]. C'est dans ce contexte que le Sénat de la Roumanie a adopté la décision nº 24 relative à la communication de la Commission « Lutter

[294] Directive (UE) 2018/1808 du Parlement européen et du Conseil du 14 novembre 2018 modifiant la directive 2010/13/UE visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels (directive « Services de médias audiovisuels »), compte tenu de l'évolution des réalités du marché, JO L 303 du 28 novembre 2018.

[295] D. **Cristian**, « Romania Imposes Financial Contributions on Streaming Platforms to Support National Film Fund », *Business Review*, 17 octobre 2022.

[296] M. Cercelescu, *Dezinformarea în epoca post-adevăr. Avem, în România, legislație sau alte măsuri pentru combaterea dezinformării?*, JURIDICE.ro, 1er mars 2019 ; D. Munteanu, *Barometrul rezilienței societale la dezinformare*, Centrul Euro-Atlantic pentru Reziliență (E-ARC), Bucarest, 2022.

[297] *Decree on the Establishment of the State of Emergency in the Territory of Romania* (Décret relatif à l'instauration de l'état d'urgence sur le territoire roumain), Journal officiel de Roumanie, 1re partie, nº 212/16, mars 2020.

[298] R. Radu, « Fighting the 'Infodemic': Legal Responses to Covid-19 Disinformation », *Social Media + Society*, 6(3), 2020.

[299] A. Mosila, « The Challenge of Populism and Disinformation on the Pandemic Response in Romania », *EuropeNow Journal*, 20 novembre 2023 ; C. Cucu, « Disinformation Landscape in Romania », EU DisinfoLab, septembre 2023.

contre la désinformation concernant la Covid-19 – Démêler le vrai du faux »[300/301]. Ses recommandations n'ont toutefois pas conduit à l'adoption de mesures concrètes en vue d'armer la société face à la désinformation. Un rapport publié en 2022 par le Centre euroatlantique pour la résilience a souligné que les outils juridiques et institutionnels de la Roumanie n'étaient « pas correctement calibrés pour la phase actuelle du développement technologique [...]. Les dispositions juridiques et les institutions compétentes ne couvrent pas l'ensemble des menaces et ne permettent pas de riposter rapidement et efficacement[302]. »

Dans le contexte national roumain, la lutte contre la désinformation revêt les formes suivantes : 1) mise en place de garde-fous juridiques plus larges, de portée générale ; 2) déploiement d'efforts stratégiques plus ciblés pour relever les nouveaux défis ; et 3) mise en œuvre d'initiatives européennes plus ambitieuses. Fondamentalement, les dispositions existantes du code pénal et les garanties constitutionnelles offrent déjà un vaste éventail de protections contre la diffusion d'informations fausses ou mensongères. L'article 404 du code pénal (mis à jour) érige en infraction criminelle punissable d'un à cinq ans d'emprisonnement la diffusion délibérée de fausses informations portant atteinte à la sécurité nationale[303]. Dans les faits, il s'avère toutefois difficile d'appliquer cette disposition aux formes très élaborées que prend la désinformation. En premier lieu, cette dernière ne se présente pas toujours sous l'aspect de contenus inventés de toutes pièces ; elle peut procéder de contenus authentiques qui ont été manipulés ou sortis de leur contexte, de contenus frauduleux ou de liens fallacieux[304]. En second lieu, les citoyens eux-mêmes sont souvent vulnérables à ce type de contenus et peuvent les relayer sans se rendre compte de leurs conséquences potentielles pour la sécurité nationale[305]. Environ un quart des utilisateurs roumains de plateformes en ligne déclarent par ailleurs partager des actualités via les réseaux sociaux, les messageries instantanées ou par courriel[306].

La Constitution roumaine comporte des dispositions relatives à la liberté d'expression et au droit à l'information, qui rendent responsables les éditeurs, producteurs, auteurs ou diffuseurs des contenus publiés et imposent aux médias de masse de garantir l'exactitude des informations communiquées au public. Cependant, les formes contemporaines de désinformation mettent à mal ce cadre : le préjudice est souvent diffus,

---

[300] Commission européenne et haut représentant de l'Union pour les affaires étrangères et la politique de sécurité, Communication conjointe au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions Lutter contre la désinformation concernant la Covid-19 – Démêler le vrai du faux, 2020.

[301] Sénat roumain, *Hotărâre nr. 24 din 8 martie 2021 referitoare la Comunicarea Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor – Combaterea dezinformării în legătură cu COVID-19 – Asigurarea unei informări corecte – JOIN(2020) 8 final* (Décision no 24 du 8 mars 2021, relative à la Communication de la Commission au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions – Lutter contre la désinformation concernant la Covid-19 – Démêler le vrai du faux), 25 mars 2021.

[302] D. Munteanu, *Barometrul rezilienței societale la dezinformare*, Centrul Euro-Atlantic pentru Reziliență (E-ARC), Bucarest, 2022.

[303] *Codul Penal din 17 Iulie 2009* (Code pénal, loi nº 286/2009), mis à jour au 5 février 2017.

[304] Haut-Commissariat des Nations unies aux droits de l'homme (HCDH), Report on Disinformation, A/HRC/47/25, 2021.

[305] D. Munteanu, *Barometrul rezilienței societale la dezinformare*, Centrul Euro-Atlantic pentru Reziliență (E-ARC), Bucarest, 2022.

[306] Institut Reuters pour l'étude du journalisme, *Digital News Report 2025 – Romania*, 2025.

touchant le public en général plutôt que des individus identifiables, par l'intermédiaire de réseaux obscurs qui changent constamment de forme. Consciente de l'ampleur du problème, la Roumanie a inclus un plan de lutte contre la désinformation dans sa stratégie de défense nationale pour 2020-2024, mais son calendrier de mise en œuvre (depuis 2021) reste un document classé confidentiel[307]. Parmi les efforts ciblés en cours de déploiement, le ministère de la Défense a annoncé publiquement son intention de lutter contre la désinformation grâce à la plateforme InfoRadar, qui assure un suivi des fausses informations et des campagnes de désinformation sur les sujets intéressant l'armée, et offre aux citoyens la possibilité de signaler les contenus correspondants par un formulaire de contact. Le ministère de la Numérisation a quant à lui mis en place un point de contact permettant le signalement des *deep fakes* liés aux élections, tandis que le projet de loi exigeant que les contenus de ce type s'accompagnent d'avertissements lors de leur diffusion est toujours en attente d'approbation définitive[308].

La Roumanie inscrit également son action dans le cadre plus large de l'Union destiné à lutter contre la désinformation et à promouvoir les processus démocratiques. En vertu de l'*Ordonanţă de Urgenţă nr. 6/2019* (ordonnance d'urgence n° 6/2019), l'Autorité électorale permanente (AEP) a été désignée point de contact unique s'agissant des incidents de cybersécurité et des campagnes de désinformation dans le contexte des élections au Parlement européen. En 2024, l'AEP a publié un guide visant à prévenir et à combattre la désinformation au sein de l'électorat. Détaillant les mécanismes de la désinformation, ce document propose des outils pour identifier et analyser les contenus mensongers, ainsi que des recommandations à l'intention des journalistes, des créateurs de contenu et des candidats aux élections[309]. Malgré ces efforts, l'application de la réglementation est restée limitée jusqu'à ce que le CNA et l'ANCOM alertent officiellement la Commission européenne quant aux irrégularités significatives constatées dans le traitement des contenus politiques par TikTok pendant les élections présidentielles de novembre 2024[310], ce qui a conduit à l'ouverture d'une enquête officielle par la Commission européenne au titre du DSA le 17 décembre 2024[311].

---

[307] I. Stanoiu, « *Serviciile de informații, Administrația Prezidențială și guvernul au scris și țin la secret planul național anti-dezinformare, care a eșuat* », *Context.ro*, 5 février 2025.

[308] *Legislative Proposal L295/2023, Propunere legislativă privind interzicerea utilizării malițioase a tehnologiei și limitarea fenomenului Deepfake* (Proposition de loi visant à interdire l'usage malveillant de la technologie et à limiter le phénomène des *deep fakes*).

[309] Autorité électorale permanente (AEP), *Ghid de prevenire și combatere a acțiunilor de dezinformare a alegătorilor*, mars 2024.

[310] **Digital Policy Alert**, « Romania: Announced NAC and ANCOM Referral to the European Commission for an Investigation into TikTok for Alleged Failure to Address Disinformation and Electoral Manipulation Amplification under DSA », *Digital Policy Alert*, 26 novembre 2024.

[311] Commission européenne, « La Commission ouvre une procédure formelle à l'encontre de TikTok au titre du règlement sur les services numériques en ce qui concerne les risques liés à l'intégrité des élections », communiqué de presse, 17 décembre 2024.

3.2.3. L'annulation de l'élection présidentielle roumaine de 2024

L'intégrité électorale était déjà l'enjeu d'affrontements dans le cyberespace bien avant que les électeurs ne se rendent aux urnes le 24 novembre 2024 pour choisir leur président. La désinformation a largement contribué à compromettre le processus électoral, s'appuyant sur des vulnérabilités structurelles profondes, notamment l'instabilité politique, l'incertitude économique et la polarisation de la société. Les discours en ligne ont mis cruellement en lumière certaines fractures socio-économiques et politiques présentes de longue date[312]. Călin Georgescu, un candidat défendant un programme pro-russe, a contre toute attente pris la tête du premier tour dans la course à la présidence, alors qu'il ne recueillait que 6 % des voix selon les sondages d'intentions de vote. Cette remontée a été favorisée par un financement de campagne opaque[313], le recours à des influenceurs en ligne, ainsi que le système de recommandation de Tik Tok[314], qui compte 9 millions d'utilisateurs roumains. Faisant suite à des informations crédibles signalant des ingérences étrangères et des irrégularités électorales[315], la Cour constitutionnelle a estimé que l'ensemble du processus électoral avait été compromis dans son intégrité, puis a annulé les résultats et ordonné la tenue d'un nouveau scrutin[316]. Călin Georgescu s'est quant à lui vu interdire de se présenter de nouveau[317].

L'annulation du scrutin a montré que toutes les mesures nationales destinées à protéger les processus électoraux s'étaient dans les faits avérées insuffisantes. À l'échelon européen, les normes posées par les lignes directrices de la Commission de 2024 en matière d'atténuation des risques systémiques pour les processus électoraux[318] n'ont pas été respectées. Les grandes plateformes n'ont pas pris les mesures nécessaires pour faire face aux menaces en temps réel, ce qui soulève des questions quant à leur responsabilité. En Roumanie, TikTok n'a pas fait respecter sa propre interdiction de la publicité à caractère politique[319], ce qui a permis la promotion agressive de comptes et de contenus liés aux élections. Malgré les notifications répétées par des autorités nationales signalant des irrégularités électorales[320], la plateforme n'est pas intervenue.

L'exemple du scrutin roumain annulé illustre par ailleurs le caractère évolutif de la désinformation, qui a facilement circulé entre influenceurs, outils de monétisation et

---

312 R. Radu, « TikTok, Telegram, and Trust: Urgent Lessons from Romania's Election », *TechPolicy Press*, 25 juin 2025.
313 Administration de la présidence roumaine, Document CSAT SRI I, 4 décembre 2024.
314 EDMO, « Analysis of the 2024 Romanian Presidential Elections: The Role of Social Media and Emerging Political Trends », 26 novembre 2024.
315 Administration de la présidence roumaine, Document CSAT SRI I, 4 décembre 2024.
316 Cour constitutionnelle de Roumanie, communiqué de presse, 6 décembre 2024.
317 S. Rainsford et L. Gozzi, « Final ruling bars far-right Georgescu from Romanian vote », *BBC News*, 11 mars 2025.
318 Communication de la Commission – Lignes directrices de la Commission à l'intention des fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne sur l'atténuation des risques systémiques pour les processus électoraux, présentées en vertu de l'article 35, paragraphe 3, du règlement (UE) 2022/2065, C/2024/3014, 26 avril 2024.
319 TikTok, TikTok Ads Policy – Politics, Government, and Elections, page mise à jour en juillet 2025.
320 DIGI24, « ANCOM: TikTok nu a acţionat la solicitarea AEP ce semnala diverse nereguli legate de conţinutul ilegal distribuit », *Digi24*, 26 novembre 2024.

promotion des contenus électoraux par les algorithmes[321]. Marqué par un faible niveau de culture numérique, une instabilité politique et économique, ainsi qu'un mécontentement généralisé des électeurs, le pays n'était pas préparé pour lutter à grande échelle contre la désinformation. Le problème a encore été aggravé par une inertie législative et une capacité institutionnelle limitée, qui ont créé des conditions propices à la propagation incontrôlée d'informations trompeuses. L'enquête ouverte par la Commission européenne en décembre 2024 sur les politiques de TikTok en matière de publicités à caractère politique et de contenus politiques payants, ainsi que sur le rôle de ses systèmes de recommandation dans l'amplification de ces contenus, est toujours en cours[322]. Le recueil des éléments de preuve s'avère lent, entre autres, parce que le DSA ne fixe pas de délais maximums à la clôture des procédures formelles. Seule la Commission européenne est à même d'évaluer le bon respect de la réglementation par les fournisseurs de TGP, épaulée en l'espèce par la *Coimisiún na Meán* irlandaise, le siège européen de TikTok se trouvant en Irlande.

À l'échelon national, deux initiatives législatives ont vu le jour en guise de réponse. Le 16 janvier 2025, le gouvernement roumain a publié l'ordonnance d'urgence n° 1/2025[323] modifiant les règles relatives à la publicité à caractère politique, sans consulter les parties intéressées[324]. Le texte exigeait un étiquetage adapté de tous les contenus électoraux, y compris ceux qui émanaient de simples citoyens. Un projet de loi visant à lutter contre la désinformation et les contenus préjudiciables en ligne a également été présenté en mars 2025, puis adopté par le Sénat roumain en juin 2025[325]. Il instaure à l'égard des TGP des règles plus strictes que celles prévues par le DSA. Dans sa forme actuelle, le texte, qui doit être examiné par la Chambre des députés dans les mois à venir, impose aux plateformes de limiter la diffusion de contenus potentiellement préjudiciables à un maximum de 150 utilisateurs, d'interdire leur promotion et de supprimer les contenus illégaux dans les 15 minutes suivant leur publication lorsqu'ils sont classés comme tels par des systèmes automatisés. Il interdit également la promotion rémunérée de contenus incitant à la haine, à la violence ou à la désinformation sur des sujets d'intérêt national. Tout manquement à l'obligation d'agir efficacement, mesuré par un seuil de 30 % de signalements d'utilisateurs confirmés, entraînerait une amende à concurrence de 1 % du chiffre d'affaires, appliquée par l'ANCOM. Si cette législation vise à renforcer la protection du grand public, sa définition large des contenus préjudiciables, son recours massif à l'intelligence artificielle (IA) et les délais accélérés qu'elle fixe suscitent des inquiétudes quant à sa viabilité pratique et aux risques qu'elle pose pour la liberté d'expression, comme en témoignent les mises en garde

[321] R. Ings, « The TikTokers accused of triggering an election scandal », *BBC News*, 30 avril 2025.
[322] Commission européenne, « La Commission ouvre une procédure formelle à l'encontre de TikTok au titre du règlement sur les services numériques en ce qui concerne les risques liés à l'intégrité des élections », communiqué de presse, 17 décembre 2024.
[323] Gouvernement de la Roumanie, *Emergency Ordinance No. 1/2025 on certain measures for the organisation and conduct of the 2025 elections for the President of Romania and the 2025 local by-elections* (Ordonnance d'urgence n° 1/2025 relative à certaines mesures pour l'organisation et le déroulement des élections présidentielles roumaines de 2025 et des élections locales partielles de 2025), 17 janvier 2025.
[324] Funky Citizens, « *Romania's Elections Overview – 22 April 2025* », *EDMO*, 22 avril 2025.
[325] R. Mocanu, « *A fost adoptată de Senat legea împotriva manipulării online, propusă de USR* », *MediaFax*, 16 juin 2025.

de certains experts[326]. Elle va nettement au-delà des obligations imposées par le DSA et pourrait créer un précédent, si elle est approuvée.

3.3. L'exemple de la France

Dr *William Gilles, maître de conférences, Université Paris 1 Panthéon-Sorbonne, et Irène Bouhadana, maître de conférences, Université Paris 1 Panthéon-Sorbonne*

3.3.1. Cadre juridique national concernant les plateformes

Le droit français applicable aux plateformes est encadré au premier chef par la jurisprudence constitutionnelle, qui précise les procédures permettant au législateur d'adopter des mesures concernant ces mêmes plateformes. Ainsi, dans sa décision relative à la loi favorisant la diffusion et la protection de la création sur internet[327] (dite « loi Hadopi 1 »), le Conseil constitutionnel a estimé que la liberté d'expression et de communication instituée par l'article 11 de la Déclaration des droits de l'homme et du citoyen du 26 août 1789[328] « impliqu[ait] la liberté d'accéder » aux « services de communication au public en ligne », et par conséquent à internet[329].

Dans une décision de 2020 portant sur la loi visant à lutter contre les contenus haineux sur internet[330] (dite « loi Avia »), le Conseil constitutionnel a réitéré sa jurisprudence, précisant que la liberté d'expression et de communication supposait aussi celle de s'exprimer[331]. Il estime, par conséquent :

> *En l'état actuel des moyens de communication et 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 et l'expression des idées et des opinions, ce droit implique la liberté d'accéder à ces services et de s'y exprimer.*

Il ajoute que le législateur français a la possibilité d'adopter un cadre juridique destiné à faire cesser les abus de l'exercice de la liberté d'expression et de communication qui portent atteinte à l'ordre public et aux droits de tiers, en classant parmi ces abus, pour la première fois, la diffusion d'images pornographiques représentant des mineurs et la provocation à des actes de terrorisme ou l'apologie de tels actes.

---

326 CMS LawNow, « *Romania proposes stricter rules against harmful content on social media* », *CMS LawNow*, 10 mars 2025.
327 Loi nº 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet, Journal officiel de la République française (JORF) nº 0135 du 13 juin 2009 (loi Hadopi).
328 Déclaration des droits de l'homme et du citoyen.
329 Conseil constitutionnel, Décision nº 2009-580 DC du 10 juin 2009.
330 Loi n° 2020-766 visant à lutter contre les contenus haineux sur internet, JORF nº 0156 du 25 juin 2020 (loi Avia).
331 Conseil constitutionnel, Décision nº 2020-801 DC du 18 juin 2020.

Cependant, la décision rendue en 2020 par le Conseil constitutionnel a dans le même temps retoqué plusieurs dispositions de la loi Avia, au motif que les atteintes portées par le texte à la liberté d'expression et de communication n'étaient ni adaptées, ni nécessaires, ni proportionnées au but poursuivi. Les dispositions invalidées auraient permis à l'autorité administrative compétente de demander aux hébergeurs ou aux éditeurs d'un service de communication en ligne de retirer les contenus à caractère pédopornographique ou ceux constituant une provocation à des actes de terrorisme ou une apologie de ceux-ci ; faute de retrait dans un délai de 24 heures, elles lui auraient également permis d'ordonner aux fournisseurs d'accès à internet d'empêcher sans délai l'accès à ces contenus. Le Conseil constitutionnel a considéré, en premier lieu, que la détermination du caractère illicite des contenus en cause ne reposait pas sur leur caractère manifeste, mais était soumise à la seule appréciation de l'administration. En outre, l'engagement d'un recours contre la demande de retrait n'aurait pas été suspensif : ne disposant que d'une heure pour bloquer l'accès au contenu visé, l'éditeur ou l'hébergeur n'aurait pas pu obtenir une décision de justice avant d'être contraint de le retirer ; il se serait de surcroît exposé à 250 000 euros d'amende et à une peine d'emprisonnement d'un an s'il n'avait pas retiré le contenu dans ce délai. De la même façon, le Conseil constitutionnel a censuré les dispositions de la loi qui imposaient aux opérateurs de plateformes en ligne, sous peine de sanction pénale, de retirer ou de rendre inaccessibles dans un délai de 24 heures des « contenus manifestement illicites en raison de leur caractère haineux ou sexuel ».

Les autres dispositions du texte – devenu « loi Avia » après son examen par le Conseil constitutionnel, ainsi qu'on l'a signalé plus haut – visaient à lutter contre les contenus haineux sur internet. La loi est venue modifier le Code de l'éducation[332], afin de renforcer la formation des élèves et étudiants, ainsi que de leurs enseignants, à l'utilisation des outils et ressources numériques, en vue d'empêcher la diffusion de contenus haineux et de promouvoir la citoyenneté numérique. La loi Avia a également créé l'Observatoire de la haine en ligne[333], rattaché à l'Autorité de régulation de la communication audiovisuelle et numérique[334] (ARCOM), l'autorité publique indépendante française chargée de garantir la liberté de communication. En service depuis 2020, cet observatoire a pour mission de suivre et d'analyser les contenus haineux en ligne. Il se compose de quatre collèges : les administrations, les chercheurs, les associations et les opérateurs, ce dernier regroupant Dailymotion, Facebook, Google, LinkedIn, Microsoft, Qwant, Snapchat, TikTok, Twitch, X (anciennement Twitter), Wikimédia France et Yubo. Enfin, la loi Avia a également modifié la loi pour la confiance dans l'économie numérique[335] (loi LCEN), qui constitue la législation française de référence définissant le cadre juridique applicable aux acteurs en ligne. Ce texte a en outre été modifié par la loi visant à sécuriser et à réguler l'espace numérique[336] (loi SREN), en vue d'adapter le droit français à celui de l'Union européenne à la suite de l'adoption des règlements DMA et DSA. Il a plus récemment été modifié par la loi visant à

[332] Code de l'éducation.
[333] Voir ARCOM, « Observateur de la haine en ligne : analyser pour mieux lutter ».
[334] PLEASE DELETE
[335] Loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, JORF nº 0143 du 22 juin 2004.
[336] Loi nº 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, JORF nº 0117 du 22 mai 2024.

sortir la France du piège du narcotrafic[337] en vue d'intégrer ces questions. Dans le même temps, il a été précisé que la régulation des plateformes n'était pas l'objet premier de cette législation.

Enfin, concernant la régulation des plateformes, le décret nº 2020-1102 du 31 août 2020[338] crée, au sein de la direction générale des entreprises et sous l'autorité des ministres chargés de l'économie, de la culture et du numérique, un service à compétence nationale appelé « Pôle d'expertise de la régulation numérique » (PEReN). Celui-ci a pour mission de fournir une expertise et une assistance technique aux agences gouvernementales et aux autorités indépendantes chargées de la régulation des plateformes numériques. Le décret nº 2022-603 du 21 avril 2022[339], modifié par le décret nº 2025-385 du 28 avril 2025[340], précise la liste des autorités administratives et publiques indépendantes pouvant recourir aux services du PEReN, à savoir : l'Autorité de la concurrence (ADLC), l'Autorité des marchés financiers (AMF), l'Autorité nationale des jeux (ANJ), l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP), l'Autorité de régulation de la communication audiovisuelle et numérique (ARCOM), l'Autorité de régulation des transports (ART), la Commission de régulation de l'énergie (CRE), la Commission nationale de l'informatique et des libertés (CNIL), ainsi que le Défenseur des droits (DDD).

3.3.2. Dispositions spécifiques concernant la désinformation

L'avènement de la société des données et l'essor des plateformes ont mis en évidence les risques que posent les nouvelles technologies du point de vue de la dissémination de *fake news*, et la France n'est pas épargnée par ce nouvel état de fait. Elle en a pris conscience avec une acuité particulière pendant l'élection présidentielle de 2017, avec l'émergence d'une ingérence étrangère mettant en péril le bon déroulement du scrutin. Ce contexte a incité le législateur français à adopter sa première législation relative aux fausses informations, destinée spécifiquement à combattre la diffusion de celles-ci pendant les élections : la loi nº 2018-1202 relative à la lutte contre la manipulation de l'information[341]. Ce cadre juridique a par la suite été modifié, notamment par la loi SREN qui met en œuvre en droit français le DSA, d'application directe, et désigne l'ARCOM comme coordinateur

[337] Loi n° 2025-532 du 13 juin 2025 visant à sortir la France du piège du narcotrafic, JORF nº 0137 du 14 juin 2025.
[338] Décret nº 2020-1102 du 31 août 2020 portant création d'un service à compétence dénommé « Pôle d'expertise de la régulation numérique » (PEReN), JORF nº 0214 du 2 septembre 2020.
[339] Décret nº 2022-603 du 21 avril 2022 fixant la liste des autorités administratives et publiques indépendantes pouvant recourir à l'appui du pôle d'expertise de la régulation numérique et relatif aux méthodes de collecte de données mises en œuvre par ce service dans le cadre de ses activités d'expérimentation, JORF nº 0095 du 23 avril 2022.
[340] Décret nº 2025-385 du 28 avril 2025 complétant le décret n° 2022-603 du 21 avril 2022 fixant la liste des autorités administratives et publiques indépendantes pouvant recourir à l'appui du pôle d'expertise de la régulation numérique et relatif aux méthodes de collecte de données mises en œuvre par ce service dans le cadre de ses activités d'expérimentation, JORF nº 0102 du 30 avril 2025.
[341] Loi nº 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information, JORF nº 0297 du 23 décembre 2018.

pour les services numériques. Le cadre juridique visant à limiter la diffusion de fausses informations est présenté ci-après tel qu'en vigueur à l'heure actuelle.

Le Code électoral[342] français a tout d'abord été modifié, afin de renforcer l'intégrité des élections et de limiter le risque d'ingérence étrangère en la matière. Dans sa dernière version en date, l'article L163-1 du Code électoral impose une obligation de transparence aux très grandes plateformes en ligne et aux très grands moteurs de recherche, au sens du DSA, lors de la diffusion d'informations se rattachant à un débat d'intérêt général. Ainsi, pendant les trois mois précédant le premier jour du mois des élections et jusqu'à la date à laquelle elles sont remportées, ces acteurs sont tenus de mettre à disposition, au sein du registre prévu à l'article 39 du DSA, une information loyale, claire et transparente concernant l'identité des personnes qui financent la promotion de contenus d'information se rattachant à un débat d'intérêt général, mais aussi sur l'utilisation des données à caractère personnel dans ce contexte. Ils doivent également faire figurer dans ce registre, le cas échéant, le montant des rémunérations perçues lorsque celui-ci est supérieur à 100 EUR (hors taxes) par contenu d'information diffusé à l'occasion de ce débat d'intérêt général. Ces dispositions comptent parmi celles qui imposent aux plateformes en ligne une obligation de coopération en matière de diffusion de fausses informations. Elles viennent s'ajouter aux dispositions du DSA concernant les obligations générales des plateformes, y compris en dehors des périodes électorales, telles que celles qui portent sur la transparence de leurs systèmes de recommandation.

L'article L163-2 du Code électoral, quant à lui, instaure la possibilité pour un candidat, le ministère public, un parti ou toute personne ayant intérêt à agir, de saisir le juge des référés pendant cette même période électorale, dès lors que des allégations ou imputations inexactes ou trompeuses de faits de nature à altérer la sincérité du scrutin sont diffusées de manière délibérée, artificielle ou automatisée et massive. Le magistrat doit alors se prononcer dans un délai de 48 heures, tandis qu'en cas d'appel, le juge est soumis au même délai. L'objectif est d'apporter une réponse prompte à la diffusion de fausses informations susceptibles d'influer sur le résultat des élections.

Plus généralement, le législateur a cherché à intégrer une dimension éducative dans la lutte contre la désinformation. C'est dans cet esprit qu'il a modifié le Code de l'éducation[343], afin qu'une formation à l'analyse critique de l'information disponible dans les médias soit dispensée aux élèves d'école primaire (article L312-5) et du collège (article L332-5), tout comme aux enseignants chargés d'assurer cette éducation (article L721-2). Les médias radiophoniques et audiovisuels, ainsi que les fournisseurs de plateformes de partage de vidéos, sont tenus de contribuer à cet objectif éducatif en adoptant des mesures à cet effet[344] (articles 28, 43-11 et 60 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication, dite « loi Léotard »).

La loi Léotard octroie en outre à l'ARCOM des compétences pour lutter contre la diffusion de fausses informations. Son article 17-2 réaffirme son rôle dans ce domaine, lorsque la diffusion de ces informations est susceptible de troubler l'ordre public ou de porter atteinte à la sincérité d'un scrutin.

---

[342] Code électoral.
[343] Code de l'éducation.
[344] Loi nº 86-1067 du 30 septembre 1986 relative à la liberté de communication, JORF du 1er octobre 1986.

La loi Léotard permet également à l'ARCOM de prendre des mesures contre les services de communication audiovisuelle ayant conclu une convention avec elle, dès lors qu'ils sont contrôlés par un État étranger ou placés sous l'influence de celui-ci et diffusent de façon délibérée de fausses informations. Si des informations de nature à altérer la sincérité du scrutin sont diffusées pendant les trois mois précédant une élection, et jusqu'à la date à laquelle celle-ci est organisée (article 33-1-1), l'ARCOM peut faire suspendre ou cesser la diffusion de ce service, afin de prévenir ou de faire cesser le trouble qui en résulte. Si ces fausses informations sont susceptibles de porter atteinte aux intérêts fondamentaux de la nation, par exemple au fonctionnement régulier de ses institutions, l'ARCOM peut, après mise en demeure, résilier unilatéralement la convention de diffusion (article 42-6). S'il constate un manquement aux obligations prévues par la loi Léotard, lesquelles comprennent notamment les exemples mentionnés plus haut, le président de l'ARCOM peut saisir le Conseil d'État en référé en vue d'obtenir une décision immédiatement exécutoire. Cette dernière est destinée à faire appliquer des mesures visant à garantir le respect de la loi, à mettre fin à l'irrégularité ou à en supprimer les effets (article 42-10). Plus généralement, l'ARCOM peut saisir le procureur de la République de toute infraction aux dispositions de la loi Léotard.

Conformément à l'article 58 de la loi Léotard, il incombe de plus à l'ARCOM de veiller à ce que les opérateurs de plateformes en ligne respectent les obligations prévues par la loi LCEN. Afin de lutter contre les manipulations de l'information susceptibles de troubler l'ordre public ou d'altérer la sincérité des scrutins, l'ARCOM émet des recommandations sur ce thème aux fournisseurs de très grandes plateformes en ligne, de très grands moteurs de recherche et de plateformes de partage de vidéos, et publie périodiquement un bilan des mesures adoptées. C'est à elle enfin qu'il revient de s'assurer que les plateformes en ligne respectent les dispositions applicables en matière de lutte contre les contenus haineux (article 62).

En dehors de ce contexte, le législateur français n'a adopté aucune disposition juridique spécifique concernant d'autres cas qui relèveraient de la diffusion de fausses informations. S'agissant de la diffusion d'informations en ligne, soulignons qu'il a affirmé le principe de la liberté de communication électronique au public, toute restriction relevant du champ d'application des exceptions prévues par la loi Léotard. Parmi les limites mentionnées, il est néanmoins possible de former un recours contre celle de la désinformation en invoquant différents scénarios prévus à l'article 1 de la loi Léotard, et plus particulièrement la nécessité de sauvegarder la dignité humaine, la liberté, le pluralisme de la pensée et de l'opinion ou l'ordre public, voire la nécessité de protéger les enfants et les adolescents lorsqu'ils sont visés.

En complément, plusieurs dispositions de la loi du 29 juillet 1881 sur la liberté de la presse[345], bien qu'elles ne visent pas expressément les fausses informations, peuvent être appliquées pour sanctionner leurs effets. En matière pénale, la désinformation relève de différents crimes et délits définis par cette loi. Trois cas de figure sont particulièrement éloquents à ce titre.

D'une part, les fausses informations sont susceptibles de conduire à une provocation à commettre des crimes et délits passibles d'une peine pouvant aller jusqu'à cinq ans

[345] Loi du 29 juillet 1881 sur la liberté de la presse.

d'emprisonnement et 45 000 EUR d'amende, conformément aux articles 24 et 24 bis de la loi sur la liberté de la presse. Ces dispositions visent des situations dans lesquelles une fausse information a directement conduit à la commission du crime ou du délit. À titre d'exemple, dans une décision rendue le 15 octobre 2019[346], la Cour de cassation a eu à se prononcer sur des messages stigmatisants concernant l'origine ou la religion supposées de personnes et assimilant l'appartenance religieuse à une maladie. Ces fausses informations, diffusées sur Twitter et Facebook, avaient été qualifiées d'injures raciales et d'exhortation à la discrimination, à la haine ou à la violence, justifiant la condamnation de leur auteur au titre des articles 24 et 27 de la loi sur la liberté de la presse, dans la mesure où ces « propos exhortaient le public, explicitement ou implicitement, à la discrimination envers des groupes de personnes visées en raison de leur appartenance raciale ou religieuse ».

D'autre part, les fausses informations peuvent également être punies en qualité de délit contre les personnes au sens de l'article 29 de la loi sur la liberté de la presse, lorsqu'elles prennent la forme d'injures, ou, en d'autres termes, d'expressions outrageantes, de termes de mépris ou d'invectives (avec des sanctions allant de 12 000 à 75 000 euros), ou encore de diffamation. Dans ce dernier cas, est visée la désinformation consistant à alléguer ou à imputer un fait portant atteinte à l'honneur ou à la réputation d'une personne ou du corps auquel elle appartient. Le contrevenant pourrait alors encourir une amende allant de 12 000 à 45 000 EUR selon les circonstances, les peines les plus sévères s'appliquant notamment à la diffamation envers les tribunaux, les administrations publiques, les fonctionnaires, les citoyens chargés d'un service ou d'un mandat public et le Président de la République, ou encore à la diffamation commise à raison de l'origine, de l'appartenance ou de la non-appartenance à une ethnie, une nation, une race ou une religion déterminée. En France, un récent exemple a concerné la diffusion en ligne de fausses informations devenues virales, qui affirmaient que Brigitte Macron, l'épouse du Président de la République, était une femme transgenre ayant subi plusieurs interventions chirurgicales à cette fin. Initialement condamnés pour diffamation le 12 septembre 2024 par le tribunal correctionnel de Paris, les auteurs de ces fausses informations ont ensuite été acquittés par la cour d'appel de Paris le 10 juillet 2025, au bénéfice de la « bonne foi ». La procédure est en cours, l'intéressée s'étant pourvue en cassation[347].

Enfin, l'article 27 de la loi sur la liberté de la presse prévoit une amende de 45 000 EUR à l'encontre de toute personne qui publie, diffuse ou reproduit des nouvelles mensongèrement attribuées à un tiers, cette amende étant portée à 135 000 EUR si cet acte vise à ébranler la discipline ou le moral des armées, ou à entraver l'effort de guerre de la nation. Ce scénario concerne toutefois un cas de figure très précis, car pour être qualifiée comme telle, la publication, la diffusion ou la reproduction doit avoir été effectuée de mauvaise foi et avoir troublé ou risqué de troubler la paix publique. Ce dernier cas de figure met en évidence la nécessité de préciser la distinction entre les notions de fausses informations et de fausses nouvelles (*fake news*). Lors de l'examen de la proposition de loi relative à la lutte contre les fausses informations (adopté par la suite sous le nom de loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de

[346] Cour de cassation, décision n° 18-85.365 (non publiée au bulletin).

[347] *Le Monde* avec AFP, « Brigitte Macron se pourvoit en cassation après la relaxe en appel de deux femmes qui avaient propagé une infox transphobe », *Le Monde*, 14 juillet 2025.

l'information[348]), le Conseil d'État a jugé utile, dans un avis consultatif daté du 4 mai 2018, de clarifier la différence entre la notion de fausse information et celle de fausse nouvelle, déjà présente en droit français dans la loi sur la liberté de la presse, ainsi que dans le Code électoral[349]. Il relève ainsi qu'au vu de la jurisprudence de la Cour de cassation, la notion de « fausses nouvelles » se rattache « à un fait précis et circonstancié, non encore divulgué et dont le caractère mensonger est établi de façon objective », tandis que la notion de « fausses informations » présente un champ d'application plus large, en ce qu'elle « supprime la condition tenant à l'absence de divulgation préalable de l'information litigieuse ». De surcroît, le Conseil d'État recommande de limiter la notion de « fausses informations » aux cas où la diffusion de telles informations « procède d'une intention délibérée de nuire ».

3.3.3. Application en cas d'élections

Le contexte géopolitique de ces dernières années et la recrudescence des ingérences étrangères ont montré que la lutte contre la désinformation ne pouvait de toute évidence pas reposer uniquement sur la loi n° 2018-1202 relative à la lutte contre la manipulation de l'information. Ce constat a incité le législateur à prendre en 2024 de nouvelles dispositions pour atteindre cet objectif, en utilisant des techniques fondées sur le traitement algorithmique qui avait été mises en œuvre à titre expérimental dans le cadre de la loi relative au renseignement[350], afin d'identifier les menaces terroristes. Introduite à l'article L851-3 du Code de la sécurité intérieure[351], cette mesure a été renouvelée à deux reprises, avant d'être pérennisée par la loi relative à la prévention d'actes de terrorisme et au renseignement[352]. Destinée à prévenir les ingérences étrangères en France[353], cette loi a cherché à étendre cette mesure en autorisant le déploiement du traitement algorithmique pour identifier, à partir des données de connexion et des adresses des contenus internet consultés, toute ingérence étrangère ou tentative d'ingérence. En contrepartie, elle met en place des garanties procédurales, en exigeant une autorisation du Premier ministre respectant le principe de proportionnalité et en définissant précisément le traitement autorisé ; le gouvernement doit également présenter un rapport au parlement sur la mise en œuvre de cette disposition législative.

En complément de ce cadre juridique, la France a également adopté des mesures de nature opérationnelle, en se dotant d'un service de vigilance et de protection contre les ingérences numériques étrangères (VIGINUM). Investi d'une compétence nationale, celui-ci

[348] *Op. cit.*
[349] Conseil d'État, Lutte contre les fausses informations, avis consultatif, 4 mai 2018.
[350] Loi n° 2015-912 du 24 juillet 2015 relative au renseignement, JORF n° 0171 du 26 juillet 2015.
[351] Code de la sécurité intérieure.
[352] Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement, JORF n° 0176 du 31 juillet 2021.
[353] Loi n° 2024-850 du 25 juillet 2024 visant à prévenir les ingérences étrangères en France, JORF n° 0177 du 26 juillet 2024.

a été créé par le décret n° 2021-922 du 13 juillet 2021[354] et est rattaché au Secrétariat général de la défense et de la sécurité nationale (SGDSN). La mission de VIGINUM consiste à détecter et à caractériser les opérations d'ingérence numérique étrangères diffusées publiquement sur les plateformes en ligne, en particulier pendant les périodes électorales, lorsqu'elles sont de nature à altérer l'information des citoyens. Les menaces informationnelles ciblées concernent spécifiquement les opérations impliquant, de manière directe ou indirecte, un État étranger ou une entité non étatique étrangère, et visant à la diffusion artificielle ou automatisée, massive et délibérée, de fausses informations par l'intermédiaire d'un service de communication au public en ligne. En l'occurrence, la notion de fausses informations se réfère à la description qui est donnée de ces opérations à l'article R.*1132-3 du Code de la défense[355], à savoir des « allégations ou imputations de faits manifestement inexactes ou trompeuses de nature à porter atteinte aux intérêts fondamentaux de la nation ». Ajoutons enfin que VIGINUM apporte un soutien à plusieurs institutions françaises : assistance au SGDSN dans la coordination et la conduite des efforts interministériels de lutte contre les fausses nouvelles ; contributions aux efforts européens et internationaux en la matière ; fourniture d'informations à l'ARCOM et à la Commission nationale de contrôle de la campagne électorale en vue de l'élection présidentielle, dans leurs rôles respectifs visant à combattre ces menaces.

3.4. L'exemple de l'Ukraine

Dr *Dariia Opryshko, Human Rights Platform*

3.4.1. Cadre juridique national relatif aux plateformes

En Ukraine, les aspects relatifs aux plateformes en ligne et à la publication de contenus ont longtemps été réglementés par des dispositions générales réparties dans différents actes législatifs. La législation autorisait le blocage de contenus représentant des abus sexuels sur des enfants ou enfreignant le droit d'auteur et les droits voisins[356].

Les premières dispositions visant spécifiquement à réglementer les plateformes en ligne en Ukraine ont été introduites par la loi ukrainienne sur les médias[357] (LUM), adoptée le 13 décembre 2022 et entrée en vigueur le 31 mars 2023. Celle-ci fait la distinction entre les plateformes de partage de vidéos (VSP) et les plateformes dites « de partage d'accès à l'information[358] » (plateformes en ligne) ; elle ne réglemente toutefois que les VSP, et

[354] Décret n° 2021-922 du 13 juillet 2021 portant création, auprès du secrétaire général de la défense et de la sécurité nationale, d'un service à compétence nationale dénommé « service de vigilance et de protection contre les ingérences numériques étrangères », JORF nº 0162 du 14 juillet 2021.
[355] Code de la défense.
[356] D. Opryshko, chapitre « Ukraine », *in* Institut suisse de droit comparé (éd.), *Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content*, Lausanne, 2015 ; D. Opryshko, *Follow-up to the Comparative Study on "Blocking, Filtering and Take-Down of Illegal Internet Content, Report on Ukraine*, 2019.
[357] *Закон України Про медіа* (loi ukrainienne sur les médias) nº 2849-IX, 13 décembre 2022.
[358] Qui sont par exemple Telegram, Facebook, X, etc.

uniquement dans le cas où celles-ci relèvent de la compétence de l'Ukraine. En d'autres termes, les plateformes en ligne les plus appréciées des Ukrainiens (telles que Telegram, Facebook, Instagram, YouTube, Netflix, TikTok, etc.) ne sont pas tenues de se conformer à la LUM.

La loi ukrainienne sur les médias[359] impose aux VSP de respecter des exigences en matière de transparence de la propriété des médias[360] ; de prévoir dans leurs conditions d'utilisation l'interdiction de diffuser des informations contraires aux exigences de la LUM[361] (y compris au cours d'une agression armée et après un conflit[362]) et à la législation sur le droit d'auteur et les droits voisins ; de publier leurs conditions d'utilisation et de les porter à la connaissance des utilisateurs ; et enfin de prévoir dans leurs conditions d'utilisation une procédure permettant d'exercer un droit de réponse ou de réfutation en cas d'informations inexactes. Les VSP sont également tenues de vérifier l'âge de l'utilisateur avant de lui permettre d'accéder à des informations susceptibles de nuire au développement physique, mental ou moral des enfants ; de garantir la possibilité de recourir à un système de contrôle parental, afin de protéger les enfants contre de telles informations ; de mettre en place des mécanismes transparents et compréhensibles permettant le dépôt de plaintes (en particulier en cas de diffusion de contenus illicites), l'examen efficace de celles-ci et l'information des plaignants du résultat de cet examen, et de veiller à l'existence d'un mécanisme transparent, simple et efficace de recours contre les mesures prises par les fournisseurs de VSP après examen des plaintes d'utilisateurs ; de mettre en œuvre des mesures et des outils efficaces d'éducation aux médias, de sensibiliser les utilisateurs à ces mesures, entre autres.[363] Une plateforme de partage de vidéos qui manque à ses obligations au titre de la LUM peut se voir infliger des amendes par le Conseil national de la radio et de la télévision[364] (Conseil national).

Les utilisateurs des plateformes de partage de vidéos disposent de moyens de recours contre les décisions, actions et défauts d'action illicites de celles-ci auprès du

[359] Les obligations fixées par la LUM s'inspirent des dispositions correspondantes de la directive SMA, en particulier de l'article 28 *ter*, ainsi que d'autres articles.

[360] Articles 25, 26 et 120 de la LUM. Ces exigences visent à interdire toutes relations avec l'État agresseur, qu'il s'agisse de liens de propriété ou de financement. Pour de plus amples informations, voir D. Opryshko, « Regulation of Media in the Context of Armed Aggression », *in* O. Batura, B. Holznagel et J. C. Kalbhenn (éd.), *Disinformation in Europe. Challenges, Legal Instruments & Policy Recommendations*, Nomos, 2024, pp. 254-257.

[361] Ces restrictions concernent 14 grandes catégories de contenus (article 36 de la LUM), les informations susceptibles de nuire au développement physique, mental ou moral des enfants (article 42), ainsi que quatre types particuliers de contenus dont la diffusion est interdite tant que les dispositions du chapitre IX sont en vigueur (article 119).

[362] Les dispositions spéciales prévues au chapitre IX de la LUM ne peuvent concerner qu'un État agresseur officiellement reconnu comme tel par le Parlement ukrainien. L'application de ces dispositions est limitée dans le temps, valable jusqu'à révocation de ce statut et pendant les cinq ans qui suivent. En août 2025, l'Ukraine n'avait appliqué le statut d'« État agresseur » qu'à la Russie (en 2015), après l'occupation illégale par celle-ci d'une partie du territoire ukrainien.

[363] Article 23, partie 1, de la LUM.

[364] Article 114 et article 116, partie 19, de la LUM. En cas d'infraction grave, les fournisseurs de VSP sont passibles d'une amende comprise entre 5 et 25 fois le salaire minimum à la date de l'infraction. Afin de déterminer le montant de l'amende, le Conseil national doit tenir compte de la technologie utilisée pour fournir le service, du territoire sur lequel celui-ci est fourni, de la taille de l'audience et d'autres paramètres qui influent sur le degré de danger public que représente l'infraction commise. En août 2025, l'amende pouvait s'élever approximativement à un montant compris entre 870 et 4 350 EUR.

Conseil national et/ou d'un tribunal[365], tandis que les fournisseurs de VSP ont la possibilité de créer un organisme de corégulation[366].

S'agissant des interactions avec des plateformes en ligne ne relevant pas de la compétence de l'Ukraine, la législation ukrainienne ne prévoit que des mécanismes non contraignants. La LUM habilite à cet égard l'autorité de régulation des médias ainsi que d'autres organismes d'État à prendre des mesures pour établir une coopération avec ces plateformes, notamment sous forme d'accords ou de mémorandums d'entente pertinents[367]. Malgré le lancement, il y a environ un an, de négociations avec certaines entreprises telles que Meta et Google, aucun mémorandum d'entente ni aucun accord n'a été conclu à ce jour[368]. Fin 2024, il n'existait toujours aucun mécanisme juridique efficace pour agir sur les plateformes en ligne ne relevant pas de la compétence ukrainienne, mais opérant dans le pays[369]. En août 2025, la situation resté inchangée.

Cet état de fait constitue un enjeu pour l'Ukraine, compte tenu notamment des cyberattaques systémiques, à grande échelle et ciblées, menées par la Russie contre le pays et sa population. L'augmentation constante de la consommation d'informations et d'actualités via les plateformes sociales rend la situation plus alarmante encore[370].

Dans ce contexte, on notera qu'après le début de l'invasion russe à grande échelle en février 2022, Telegram est devenue la plateforme en ligne la plus utilisée en Ukraine. Elle permettait en effet un accès très facile à l'information, proposait des chaînes qui informaient la population de l'itinéraire des drones et roquettes lancés sur l'Ukraine, etc. De plus, de nombreux responsables gouvernementaux, y compris au plus haut niveau, y avaient créé leurs propres chaînes pour communiquer avec leurs concitoyens[371]. Telegram

---

[365] Article 23, partie 3, de la LUM.

[366] En vertu de la LUM, les organismes de corégulation sont créés par les représentants du secteur des médias et sont habilités, conjointement avec le Conseil national, à élaborer des codes (règles) concernant la création et la diffusion de certaines informations, les critères relatifs aux informations prohibées (notamment les discours de haine, la discrimination, l'incitation au terrorisme et la pédopornographie), les critères permettant d'identifier les acteurs du secteur des médias en ligne, et ceux permettant de qualifier une publicité de préjudiciable, etc. Ce mécanisme prévoit que les acteurs du secteur des médias s'engagent volontairement à respecter les codes (règles) qui les concernent, tandis que le Conseil national estime que ces exigences sont suffisantes pour garantir l'intérêt public (article 36, partie 2 ; article 90, partie 1, paragraphes 23, 24, 26 et 51, ainsi qu'article 90, partie 2 ; et article 92 de la LUM).

[367] Article 2, partie 15 ; article 90, partie 1, paragraphes 13 et 14 ; article 91, partie 1, paragraphes 3, 11 et 13 ; article 99, partie 3 ; et article 124, partie 5, de la LUM.

[368] D. Opryshko, « *Monitoring Media Pluralism the European Union: Preliminary Study to the Implementation of the Media Pluralism Monitor 2025 in Ukraine* », EUI, RSC, rapport de projet de recherche, Centre for Media Pluralism and Media Freedom (CMPF), 2025, p. 13 ; Conseil national de la télévision et de la radio, « *Регулювання платформ та хто фінансує компанії, які реєструють медіа: Національна рада провела зустріч з мериканською торговельною палатою* » (« Réglementation des plateformes et financement des sociétés d'enregistrement des médias : le Conseil national rencontre la Chambre de commerce des États-Unis »), communiqué de presse, 15 avril 2025.

[369] D. Opryshko, « *Monitoring Media Pluralism the European Union: Preliminary Study to the Implementation of the Media Pluralism Monitor 2025 in Ukraine* », EUI, RSC, rapport de projet de recherche, Centre for Media Pluralism and Media Freedom (CMPF), 2025.

[370] *Ibid*., p. 6.

[371] R. Horbyk, D. Dutsyk et S. Shalaysky, « *The Effectiveness of Countering Russian Disinformation in Ukraine in the Context of a Full-Scale War. Analytical report* », ONG Ukrainian Institute of Media and Communication, 2023, p. 7 et 50.

est ainsi resté la plateforme en ligne numéro un en Ukraine, au moins jusqu'à la fin de l'année 2024[372].

Dans le même temps, ce service est activement utilisé, dans le cadre d'opérations d'information hostiles menées par la Russie, pour lancer des cyberattaques, pour diffuser des messages de *phishing* (hameçonnage) et des logiciels malveillants, pour localiser géographiquement les utilisateurs et ajuster les frappes des missiles[373] ainsi que pour recruter des citoyens (y compris des mineurs) en vue de leur faire commettre des actes répréhensibles contre l'Ukraine (par exemple, faire exploser les organes de commandement militaire chargés de mettre en œuvre la législation ukrainienne sur les obligations militaires, le service national et la formation en vue de la mobilisation, ou encore endommager ou détruire les biens [tels que les voitures] du personnel militaire[374], etc.).

Cette situation a entraîné l'élaboration de plusieurs projets de loi visant à réglementer les plateformes en ligne, notamment un projet de loi modifiant certaines lois ukrainiennes relatives à la réglementation de l'activité des plateformes d'accès partagé à l'information, par lesquelles sont diffusées des informations de masse[375].

La note explicative accompagnant le texte indique que ce projet de loi a pour objectif de fournir aux autorités nationales les outils nécessaires pour répondre efficacement aux menaces que font peser sur la sécurité nationale les plateformes en ligne, et en particulier Telegram[376].

Les auteurs du projet ont cherché à incorporer dans la législation ukrainienne certaines composantes de l'approche du DSA en matière de régulation des plateformes en ligne. Ils ont par exemple proposé que les plateformes ne relevant pas de la compétence de l'Ukraine ou d'un État membre de l'Union soient tenues de désigner un représentant officiel en Ukraine, afin de faciliter la communication avec le Conseil national, les autres autorités publiques et les collectivités locales.

Les propositions de modifications apportées au projet n'offrent cependant pas une sécurité juridique suffisante. Ainsi, elles n'indiquent pas pourquoi les plateformes en ligne diffusant des informations de masse devraient bénéficier d'un traitement différent des autres plateformes en ligne, dans la mesure où ces deux types de plateformes permettent

---

[372] InMind, « *Ukrainian media, attitude and trust in 2024* », novembre 2024, p. 4 et 28.

[373] Le Conseil national de sécurité et de défense de l'Ukraine a décidé de restreindre l'utilisation de Telegram au sein des autorités gouvernementales, des formations militaires et des infrastructures critiques, voir https://www.rnbo.gov.ua/ua/Diialnist/6994.html.

[374] Administration militaire régional de Kharkiv, « *Cyber police warn: recruitment of teenagers to commit sabotage has increased on the Internet* », 19 février 2025 ; ministère ukrainien des Affaires intérieures, « *Enemy recruiting teenagers to commit sabotage: cyber police warn of dangers on the Internet* », 12 mars 2025 ; M. Patoka, « *The SSU revealed how many minors were arrested for collaborating with the Russian Federation* » (« Le SBU révèle le nombre de mineurs arrêtés pour collaboration avec la Fédération de Russie », 30 juin 2025.

[375] *Проект Закону про внесення змін до деяких законів України щодо регулювання діяльності платформ спільного доступу до інформації, через які поширюється масова інформація* (Projet de loi modifiant certaines lois ukrainiennes relatives à la réglementation de l'activité des plateformes d'accès partagé à l'information par lesquelles sont diffusées des informations de masse), n° 11115, 25 mars 2024.

[376] Note explicative accompagnant le projet de loi modifiant certaines lois ukrainiennes relatives à la réglementation de l'activité des plateformes d'accès partagé à l'information par lesquelles sont diffusées des informations de masse, n° 11115, 25 mars 2024, disponible sur : https://itd.rada.gov.ua/billinfo/Bills/Card/43884.

d'enregistrer et de diffuser des informations émanant des utilisateurs à un public illimité. Le projet ne précise pas non plus si les dispositions proposées réglementent uniquement les plateformes dont les activités ciblent l'Ukraine et sa population. En outre, on ignore selon quelles modalités précises les plateformes relevant de la compétence d'un ou de plusieurs États membres de l'UE devraient communiquer avec les autorités ukrainiennes au sujet des notifications, exigences, décisions, demandes, lettres ou autres qui leur seraient adressées par les organismes ukrainiens compétents.

Le projet de loi qualifie les fournisseurs de plateformes en ligne permettant la diffusion d'informations de masse d'acteurs du secteur des médias ; toutefois, contrairement au règlement européen sur la liberté des médias et au DSA, il ne tranche pas la question de leur responsabilité éditoriale[377]. Il ne prévoit pas non plus de recours judiciaires dans les affaires relatives aux restrictions d'accès à des contenus dont la diffusion enfreint les exigences de la LUM, sur la base de demandes émanant de l'autorité de régulation des médias, etc.

En août 2025, le projet de loi était toujours en cours d'examen par la commission parlementaire pour la politique humanitaire et l'information, et n'avait pas encore été présenté en première lecture à la Verkhovna Rada, le Parlement ukrainien.

Entre-temps, le Centre national de coordination de la cybersécurité (NCCC), qui dépend du Conseil national de sécurité et de défense de l'Ukraine (NSDC), a recommandé en septembre 2024 d'interdire l'installation et l'utilisation de Telegram sur les terminaux officiels des employés des autorités de l'État, du personnel militaire, des employés du secteur de la sécurité et de la défense, ainsi que des entreprises exploitant des infrastructures critiques[378] (à l'exception des personnes qui utilisent cette messagerie instantanée dans le cadre de leurs fonctions officielles). Cette recommandation a été suivie par un certain nombre d'autorités étatiques, d'universités publiques et d'autres entités.

En lien avec cette recommandation, le Conseil national a également annoncé l'instauration d'un régime spécial d'accès à Telegram. Les employés de l'instance de régulation des médias se sont vu interdire l'utilisation de Telegram sur leurs terminaux professionnels (afin de protéger les informations classées confidentielles). Dans le même temps, un segment de réseau distinct (séparé du réseau interne du Conseil national, mais connecté à l'internet externe) a été mis en place, afin d'analyser les activités des médias sur cette plateforme en ligne[379].

---

[377] En vertu du règlement européen sur la liberté des médias, les fournisseurs de très grandes VSP peuvent être qualifiés à la fois de fournisseurs de VSP, de fournisseurs de TGP et de fournisseurs de services de médias, dès lors qu'ils exercent un contrôle éditorial sur une ou plusieurs parties de leurs services (considérant 11). Les exemptions de responsabilité prévues par le DSA ne devraient notamment pas s'appliquer aux informations élaborées sous la responsabilité éditoriale du fournisseur du service intermédiaire proprement dit (considérant 18).

[378] Conseil national de sécurité et de défense, « The NCCC Has Decided to Restrict the Use of Telegram in Government Agencies, Military Formations, and Critical Infrastructure Facilities », communiqué de presse, 20 septembre 2024.

[379] Conseil national de la radio et télévision d'Ukraine, « The National Council Has Introduced a Special Procedure for Accessing Telegram », communiqué de presse, 9 octobre 2024.

3.4.2. Règles spécifiques en matière de désinformation

Un certain nombre de documents stratégiques ukrainiens ont pour objectifs la lutte contre la désinformation et les opérations d'information spéciales, ainsi que l'amélioration du niveau de compétence médiatique de la population[380].

En 2022, l'invasion à grande échelle de l'Ukraine par la Russie a conduit à l'instauration de la loi martiale[381] sur l'ensemble du territoire ukrainien, doublée de l'imposition de restrictions au droit à la liberté d'expression[382], et à la dérogation par l'Ukraine à ses obligations au titre de l'article 19 du Pacte international relatif aux droits civils et politiques[383] (PIDCP) et de l'article 10 de la Convention européenne des droits de l'homme[384]. Bien que le pays n'ait officiellement instauré aucune censure, la législation ukrainienne a été modifiée et prévoit désormais de nouvelles dispositions visant à lutter contre l'influence russe sur l'information.

Ainsi, une responsabilité pénale peut désormais être engagée en cas de justification, de négation ou de reconnaissance de la légalité de l'agression armée par la Fédération de Russie contre l'Ukraine, ainsi qu'en cas de glorification des participants à cette agression[385] ; les services de médias audiovisuels à la demande et les services des prestataires audiovisuels de l'État agresseur ont été temporairement bloqués sur le territoire ukrainien[386] ; enfin, les plateformes de partage de vidéos sont dorénavant tenues

[380] Ces éléments faisaient partie des priorités de la politique nationale ukrainienne en matière d'information définies notamment dans la doctrine de l'Ukraine concernant la sécurité de l'information (2017-2021), et des objectifs stratégiques de la stratégie pour la sécurité de l'information (2021), dont la mise en œuvre était prévue jusqu'en 2025. Voir, par ailleurs, la stratégie du ministère de la Culture et de l'Information de l'Ukraine pour le développement de l'éducation aux médias sur la période allant jusqu'en 2026, consultable ici.

[381] La loi martiale est un régime juridique spécial imposé en Ukraine ou dans certains territoires en cas d'agression armée, de menace d'agression ou de toute menace à l'indépendance de l'État ukrainien et à son intégrité territoriale. Elle confère aux autorités étatiques compétentes, au commandement des forces armées, aux administrations militaires et aux gouvernements locaux les pouvoirs nécessaires pour combattre la menace, pour repousser l'agresseur armé et assurer la sécurité nationale, pour éliminer la menace pesant sur l'indépendance de l'État et l'intégrité territoriale de l'Ukraine, ainsi que pour prévoir la restriction temporaire, en raison de la menace, des droits et libertés constitutionnels des personnes et des citoyens, et des droits et intérêts légitimes des personnes morales, en précisant la durée de ces restrictions (article 1, *Закон України Про правовий режим воєнного стану* [loi de l'Ukraine sur le régime juridique de la loi martiale], 12 mai 2015, nº 389-VIII).

[382] D. Opryshko, « Freedom of Expression during Military Conflict », *in* ORF (éd.), *Public Value Texte 25 – Why Independence Matters*, ORF, Vienne, 2022, pp. 45-53, et notamment p. 46.

[383] Pacte international relatif aux droits civils et politiques (adopté le 16 décembre 1966), 999 UNTS 171.

[384] D. Opryshko, « Monitoring Media Pluralism in the Digital Era: Application of the Media Pluralism Monitor in the European Union, Albania, Montenegro, the Republic of North Macedonia, Serbia and Turkey in the Year 2022. Preliminary Study to the Implementation of the Media Pluralism Monitor: Ukraine », EUI, RSC, Centre for Media Pluralism and Media Freedom, 2023, pp. 7-8.

[385] Voir *Закон України Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції* (loi de l'Ukraine relative aux modifications de certains actes législatifs ukrainiens concernant le renforcement de la responsabilité pénale pour la production et la diffusion de produits d'information interdits) du 3 mars 2022.

[386] Article 123 de la LUM. En août 2025, cette liste de services de médias audiovisuels à la demande et de services de prestataires de services audiovisuels de l'État agresseur compte 49 noms. Elle est disponible ici.

d'interdire, dans leurs conditions d'utilisation, la diffusion de quatre types de contenus spécifiques[387].

Il s'agit en l'occurrence 1) d'informations présentant l'agression armée contre l'Ukraine comme un conflit interne, un conflit civil ou une guerre civile ; 2) d'informations non fiables concernant l'agression armée et les actes perpétrés par l'État agresseur (État occupant), par ses représentants et par les personnes et organisations qu'il contrôle, dès lors que leur diffusion conduit à une incitation à l'hostilité ou à la haine[388]. En effet, la Russie pratique la désinformation, en recourant systématiquement à des éléments de langage tels que « conflit interne/conflit civil/guerre civile » ou « conduite d'une opération spéciale de dénazification/désatanisation » pour justifier ses agissements illégaux, mais aussi pour diviser et affaiblir la société ukrainienne[389].

En outre, afin de réduire l'effet amplificateur des discours de désinformation soutenus par certains artistes et musiciens russes[390], la loi ukrainienne sur les médias interdit la diffusion 3) de programmes et de contenus (à l'exception de ceux consacrés à l'information et à l'analyse) dans lesquels l'un des participants figure sur la liste des personnes représentant une menace pour la sécurité nationale[391] et 4) de phonogrammes, de vidéogrammes et de clips musicaux interprétés par des chanteurs qui sont citoyens de l'État agresseur (moyennant quelques exceptions), qui n'ont pas condamné l'agression russe contre l'Ukraine et figurent ainsi sur la liste correspondante[392].

3.4.3. Application en cas d'ingérence étrangère par la désinformation en temps de guerre

Les dispositions de la loi ukrainienne sur les médias concernant les VSP relevant de la compétence ukrainienne n'ont pas encore été appliquées. En effet, ces plateformes n'ont commencé à s'enregistrer en Ukraine qu'en 2025. En août 2025, il existait deux VSP relevant de la compétence ukrainienne[393].

Il est à noter que la LUM prévoit des approches réglementaires distinctes pour les plateformes en ligne et les médias qui ont enregistré leurs comptes sur ces plateformes en

[387] Bien que les dispositions du chapitre IX de la LUM soient en vigueur (cf. plus haut), ses dispositions spéciales ne s'appliquent qu'à un État agresseur officiellement reconnu comme tel par le Parlement ukrainien. Leur application est limitée dans le temps, jusqu'à la révocation du statut d'État agresseur et pour les cinq années qui suivent.
[388] Article 112, partie 4, paragraphes 7 et 8, et article 119, partie 1, paragraphes 1 et 2, de la LUM.
[389] D. Opryshko, « *Regulation of Media in the Context of Armed Aggression* », *in* O. Batura, B. Holznagel et J. C. Kalbhenn (éd.), *Disinformation in Europe. Challenges, Legal Instruments & Policy Recommendations*, Nomos, 2024, pp. 251-252.
[390] *Ibid.*, pp. 252-254 ; O. Batura et D. Opryshko, « *Kunstfreiheit und Propaganda aus Sicht des Völkerrechts* », *in* J. Crückeberg *et al.* (éd.), *Handbuch Kulturpolitik*, Springer VS, Wiesbaden, 2023.
[391] Cette liste comporte notamment de célèbres acteurs de théâtre et de cinéma, metteurs en scène, producteurs, compositeurs, chanteurs, présentateurs de télévision, etc. qui soutiennent publiquement la guerre menée par la Russie contre l'Ukraine. Elle est disponible ici.
[392] Article 119, partie 1, paragraphes 3 et 4, de la LUM.
[393] Liste des acteurs du secteur des médias au 1er août 2025, p. 6208, 6455, disponible ici.

tant que médias en ligne. Ces derniers doivent se conformer aux exigences de la législation ukrainienne, notamment aux règles relatives à la transparence en matière de propriété des médias, et peuvent être tenus pour responsables en cas d'infraction à la LUM. Il est nettement plus problématique de lutter contre la désinformation, la mésinformation et la propagande émanant de comptes et de chaînes anonymes. Ces dernières jouissent souvent d'une audience considérable (qui représente jusqu'à un tiers de la population ukrainienne en chiffres absolus[394]) et exercent par conséquent une forte influence sur la société. L'Ukraine ne peut toutefois pas leur appliquer sa législation, car ces plateformes en ligne ne relèvent pas de sa compétence.

En l'absence de mécanismes efficaces qui permettraient à l'État de peser sur les plateformes en ligne étrangères afin de protéger ses intérêts nationaux, un blocage généralisé a été appliqué à certains sites web et certaines plateformes en ligne. Cette mesure est principalement mise en œuvre en vertu de la loi ukrainienne sur les sanctions et pendant l'invasion de l'Ukraine par la Russie ; elle est également appliquée conformément aux instructions du Centre national de gestion opérationnelle et technique des réseaux de télécommunications (NCU). Ces deux mécanismes font l'objet de critiques nourries de la part d'avocats spécialisés dans les droits de l'homme, d'experts et d'organisations professionnelles, notamment en raison de leur manque de transparence et de prévisibilité[395].

Les premiers blocages de ressources web en vertu de la loi ukrainienne sur les sanctions sont intervenus en 2017. Ils portaient, entre autres, sur des plateformes en ligne russes telles que VKontakte et Odnoklassniki, le service de messagerie électronique Mail.ru, ainsi que le moteur de recherche et portail internet Yandex[396]. Ils ont été instaurés sur la base juridique de paragraphe 25 de partie 1 de l'Article 4, de la loi relative aux sanctions, lequel régit les « autres sanctions conformes aux principes d'application établis par la présente loi ». Cette façon de bloquer des ressources web a été critiquée, au motif qu'elle ne respecte pas les principes de légalité et de prévisibilité qu'impose l'article 10, paragraphe 2, de la Convention européenne des droits de l'homme. Toutefois, concernant la restriction de la diffusion de contenus préjudiciables, les experts estiment qu'un tel blocage constitue une mesure proportionnée pour la protection de la sécurité nationale, des données à caractère personnel, des droits d'auteur et des droits voisins, ainsi que pour

[394] K. Rodak, « *Trukha: true colours revealed. Who really stands behind the largest network of anonymous Telegram channels in Ukraine and how much it costs* », 5 septembre 2023 ; G. Sklyarevs'ka, « NGL.media: Trukha is owned by Volodymyr Lytvyn and earns hundreds of thousands of dollars a month from advertising » ; D. Opryshko, « *Media Ownership Transparency as a Shield against Foreign Interference: the Ukrainian Experience* », EMFA Observatory, EUI, 26 mars 2025.

[395] D. Opryshko, « Monitoring Media Pluralism the European Union: Preliminary Study to the Implementation of the Media Pluralism Monitor 2025 in Ukraine », EUI, RSC, rapport de projet de recherche, Centre for Media Pluralism and Media Freedom (CMPF), 2025, pp. 15-17.

[396] *Указ Президента України « Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій) »* (« Décret du Président de l'Ukraine relatif à la décision du Conseil national de sécurité et de défense de l'Ukraine du 28 avril 2017 sur l'application de mesures économiques spéciales et d'autres mesures restrictives [sanctions] »), 15 mai 2017, nº 133. Les décisions relatives au blocage des ressources en ligne en vertu de la loi ukrainienne sur les sanctions sont adoptées par le Conseil national de sécurité et de défense de l'Ukraine et promulguées par décret présidentiel (article 5, paragraphes 2 et 3, de la loi sur les sanctions).

la lutte contre les contenus piratés, et qu'il ne constitue pas une violation du droit à la liberté d'expression[397].

Un autre mécanisme de blocage des ressources web évoqué plus haut, qui comprend le blocage de l'accès aux adresses IP et aux systèmes autonomes (AS) et est appliqué dans le cadre de la loi martiale en Ukraine, passe par des ordonnances de blocage des ressources web émises par le NCU[398]. Leur non-respect peut entraîner l'exclusion des réseaux de communications électroniques et des fournisseurs de services du registre pertinent, et par conséquent la suspension de leurs activités pendant un an[399].

La restriction de l'accès aux adresses IP et aux AS entraîne des répercussions significatives, non seulement pour les acteurs qui diffusent des contenus préjudiciables, mais aussi pour d'autres ressources, non soumises à restriction[400]. Il devient dès lors impossible d'accéder à un grand nombre de ressources web qui coexistent avec des ressources de propagande hostile sur une même adresse numérique, sans que celles-ci soient liées à la guerre menée par la Russie contre l'Ukraine ou à la propagande russe. Les experts soulignent que le blocage des AS constitue une mesure unique, sans équivalent ailleurs dans le monde[401]. Quant au blocage des ressources web sur instruction du NCU, il manque de transparence et de prévisibilité, et garantit aucune protection contre les blocages arbitraires[402]. C'est la raison pour laquelle il a été critiqué, au motif qu'il ne respecte pas les normes européennes en matière de liberté d'expression.

---

[397] D. Opryshko, « Monitoring Media Pluralism the European Union: Preliminary Study to the Implementation of the Media Pluralism Monitor 2025 in Ukraine », EUI, RSC, rapport de projet de recherche, Centre for Media Pluralism and Media Freedom (CMPF), 2025, p. 15 et p. 20.

[398] Article 32, partie 8, *Закон України Про електронні комунікації* (loi de l'Ukraine relative aux communications électroniques).

[399] Voir, par exemple, la décision de la Commission nationale de régulation des communications électroniques, du spectre des radiofréquences et de la fourniture des services postaux (NKEK) du 30 mars 2022, n° 26, relative à l'exclusion de la société à responsabilité limitée NETASSIST du registre des opérateurs et fournisseurs de télécommunications, telle que modifiée par la décision de la NKEK du 1er juin 2022, n° 59.

[400] A. Belovolchenko, « "Надійно заблокувати щось в інтернеті неможливо". Як в Україні блокуються російські ресурси й чому це зачіпає легальні сайти » (« "Il est impossible de bloquer quoi que ce soit de manière fiable sur internet." Blocage des ressources russes en Ukraine et incidence sur les sites légaux »), DOU.ua, 13 janvier 2023.

[401] D. Opryshko, « *Monitoring Media Pluralism the European Union: Preliminary Study to the Implementation of the Media Pluralism Monitor 2025 in Ukraine* », EUI, RSC, rapport de projet de recherche, Centre for Media Pluralism and Media Freedom (CMPF), 2025, pp. 16-17.

[402] *Ibid.*, p. 17.

4. La Lutte contre les contenus à caractère terroriste

4.1. Mesures d'exécution à l'échelon de l'UE

Dr Mark D. Cole, directeur des affaires académiques à l'Institut européen des médias (EMR) et professeur en droit des médias et des télécommunications à l'université du Luxembourg

La dissémination de contenus à caractère terroriste en ligne n'a cessé de prendre de l'ampleur au fil des ans, les terroristes diffusant largement leurs messages à l'aide de plateformes qui hébergent des contenus téléversés par des tiers[403]. Ce phénomène est pris en compte dans la Directive Services de médias audiovisuels (SMA), qui souligne l'importance de protéger le grand public contre l'incitation au terrorisme[404]. La directive impose par conséquent aux États membres de prendre les mesures appropriées pour garantir que les services des fournisseurs de services de médias relevant de leur compétence ne contiennent aucune provocation publique à commettre une infraction terroriste[405] ; de même, les fournisseurs de plateformes de partage de vidéos (VSP) doivent prendre les mesures appropriées pour éviter la présence de tels contenus sur leurs plateformes[406]. Ces mesures prennent notamment la forme de mécanismes permettant d'indiquer ou de signaler des contenus, de systèmes de vérification de l'âge des utilisateurs, d'outils de contrôle parental, ainsi que de procédures transparentes de modération des contenus[407].

L'accessibilité des contenus à caractère terroriste a largement contribué à la radicalisation des individus[408]. Le règlement sur les contenus à caractère terroriste en

[403] Europol, *European Union Terrorism Situation and Trend report 2023*, Office des publications de l'Union européenne, Luxembourg, 2023, et Europol, *European Union Terrorism Situation and Trend report 2022*, Luxembourg, 2022.
[404] Voir le considérant 18 de la Directive SMA, motivant l'instauration d'une disposition à l'article 6 qui concerne spécifiquement l'interdiction de la diffusion de contenus à caractère terroriste.
[405] Article 6 de la Directive (UE) 2018/1808 du Parlement européen et du Conseil du 14 novembre 2018 modifiant la Directive 2010/13/UE visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels (Directive « Services de médias audiovisuels »), compte tenu de l'évolution des réalités du marché, *JOUE* L 303/69 du 28 novembre 2018.
[406] Article 28 *ter*, paragraphe 1, point c), de la Directive SMA.
[407] Article 28 *ter*, paragraphe 3, de la Directive SMA.
[408] Commission européenne, Proposition de règlement du Parlement européen et du Conseil relatif à la prévention de la diffusion de contenus à caractère terroriste en ligne, COM(2018) 640 final, 2018 (exposé des motifs) ; Commission européenne, Rapport de la Commission au Parlement européen et au Conseil sur la mise en œuvre du Règlement (UE) 2021/784 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne, COM(2024) 64 final, 2024.

ligne[409] (TERREG) vise ainsi expressément à pallier les limites des accords volontaires conclus dans le cadre du Forum de l'UE sur l'internet[410], une initiative multipartite lancée par la Commission européenne en décembre 2015. Le Forum de l'UE sur l'internet a certes suscité des réactions favorables sur le plan de l'amélioration de la coopération entre les acteurs du secteur, Europol et les autorités nationales, mais seul un nombre limité de fournisseurs de services d'hébergement y participent. En outre, « l'ampleur et la vitesse des progrès » accomplis par les hébergeurs ont été jugées insuffisantes pour remédier à l'accessibilité des contenus à caractère terroriste en ligne[411]. Le consensus atteint autour de la nécessité de renforcer l'action de l'UE contre ce type de contenus a débouché en 2018 sur une recommandation de la Commission[412]. Elle s'appuyait elle-même sur la communication adoptée par la Commission en 2017 pour lutter contre le contenu illicite en ligne[413] et sur les activités du Forum de l'UE sur l'internet, lesquelles ont permis de définir certaines mesures essentielles, notamment des mécanismes de notification et d'action. Les mesures proposées ont par la suite été intégrées dans le TERREG, qui fixe des règles harmonisées pour la suppression des contenus à caractère terroriste et est entré en application en juin 2022[414].

Le TERREG se fonde sur les définitions des infractions terroristes figurant dans la directive 2017/541 relative à la lutte contre le terrorisme[415] et précise en outre le matériel auquel s'applique la définition du contenu en ligne à caractère terroriste[416]. Dans cette optique, la notion générale de « contenu à caractère terroriste » recouvre non seulement les contenus qui incitent à la commission d'un acte de terrorisme, mais aussi des types de

---

[409] Règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne, *JOUE* L 172/79 du 17 mai 2021. Pour une vue d'ensemble, voir P. Voigt, E. Eschborn et H. Bastians, « *Weitreichende neue Pflichten für Host-Provider, Kurzanalyse der Verordnung zur Bekämpfung der Verbreitung terroristischer Online-Inhalte* », *MMR* 727, 2022.

[410] Commission européenne, « Forum de l'UE sur l'internet : réunir les gouvernements, EUROPOL et les entreprises du secteur de l'internet pour lutter contre les contenus à caractère terroriste et les discours de haine en ligne », communiqué de presse, 3 décembre 2015.

[411] Commission européenne, Rapport de la Commission au Parlement européen et au Conseil sur la mise en œuvre du Règlement (UE) 2021/784 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne, *op. cit.*

[412] Recommandation (UE) 2018/334 de la Commission du 1er mars 2018 sur les mesures destinées à lutter, de manière efficace, contre les contenus illicites en ligne, *JOUE* L 63/50, 2018.

[413] Commission européenne, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions – Lutter contre le contenu illicite en ligne – Pour une responsabilité accrue des plateformes en ligne, COM(2017) 555 final, 2017.

[414] Concernant la proposition de TERREG, voir M. D. Cole, C. Etteldorf et C. Ullrich, « *Cross-Border Dissemination of Online Content* », vol. 81 *Schriftenreihe Medienforschung*, Nomos, Baden-Baden, 2021, p. 149 et s.. Pour de plus amples informations concernant le TERREG dans sa version finale, voir V. H. Albus, « *Eyes Shut, Fingers Crossed: the EU's Governance of Terrorist Content Online under Regulation 2021/784* », *in* R. Gsenger et M.-T. Sekwenz (éd.), *Digital Decade: How the EU Shapes Digitalisation Research*, Nomos, Baden-Baden, 2025, p. 209 et s.

[415] Directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil, *JOUE* L 88/6 du 31 mars 2017.

[416] L'article 3 de la directive 2017/541 relative à la lutte contre le terrorisme définit un certain nombre d'actes qui doivent être érigés en infractions terroristes dans les législations nationales lorsqu'ils sont commis en vue d'intimider gravement une population, de contraindre indûment des pouvoirs publics ou une organisation internationale à accomplir ou à s'abstenir d'accomplir un acte quelconque, ou encore de gravement déstabiliser ou détruire les structures politiques, constitutionnelles, économiques ou sociales fondamentales d'un pays ou d'une organisation internationale.

matériel liés au recrutement, à la formation ou à la fourniture d'instructions, ainsi que ceux qui incitent à participer aux activités d'un groupe terroriste ou risquent d'encourager un individu à mener un acte de terrorisme[417]. La directive 2017/541 comporte une liste d'actes intentionnels définis comme des infractions en vertu du droit national, qui constituent des infractions terroristes, telles que les atteintes à la vie d'une personne pouvant entraîner la mort, les enlèvements ou les prises d'otage, etc. L'article 21 prévoit en outre un certain nombre de mesures à adopter en vue de lutter contre les contenus en ligne constituant une provocation publique à commettre une infraction terroriste.

Applicable à tous les fournisseurs de services d'hébergement proposant des services dans l'Union[418], l'article 3 du TERREG instaure des « injonctions de retrait », que les autorités compétentes peuvent émettre pour exiger des hébergeurs qu'ils retirent les contenus à caractère terroriste ou bloquent l'accès à ces contenus dans tous les États membres de l'UE. Ces injonctions de retrait peuvent prendre la forme d'une décision administrative ou judiciaire, selon l'autorité compétente désignée. Le TERREG entend raccourcir le temps de réaction et garantir le blocage ou le retrait des contenus à la source. En conséquence, l'injonction visant à supprimer un contenu à caractère terroriste ou à empêcher l'accès à celui-ci doit être exécutée dès que possible et, en tout état de cause, dans un délai d'une heure à compter de sa réception[419].

Pour assurer un traitement rapide, un modèle d'injonction figure à l'annexe I du TERREG et doit être utilisé par les autorités compétentes ; en outre, l'article 15 du règlement impose aux fournisseurs de services d'hébergement de désigner ou d'établir un point de contact pour la réception de ces injonctions par voie électronique. Un fournisseur de services d'hébergement dont l'établissement principal n'est pas situé dans l'Union doit désigner un représentant légal dans l'UE aux fins de la réception, du respect et de l'exécution des injonctions de retrait et des décisions. Avant d'émettre une injonction de retrait, les autorités compétentes doivent échanger des informations, se coordonner, et coopérer – entre elles et, le cas échéant, avec Europol –, de manière à éviter les efforts faisant double emploi et les interférences avec des enquêtes en cours[420]. Les signalements, qui constituent un mécanisme permettant d'avertir les fournisseurs de services d'hébergement de l'existence de potentiels contenus à caractère terroriste, afin qu'ils puissent examiner la compatibilité de ceux-ci avec leurs propres conditions générales[421], ne sont pas réglementés dans le cadre du TERREG. Ils n'en demeurent pas moins un moyen efficace et rapide pour sensibiliser davantage les hébergeurs à la mise à disposition de

[417] Article 2, paragraphe 7, du TERREG.
[418] Article premier, paragraphe 2, du TERREG.
[419] Article 3, paragraphe 3, du TERREG.
[420] Article 14 du TERREG. S'agissant du principe d'éviter les doublons, les États membres sont incités à recourir aux outils spécialisés mis au point par Europol, tels que la Plateforme européenne de retraits des contenus illégaux sur internet (PERCI) de l'unité chargée du signalement des contenus sur l'internet (voir Europol, *PERCI TCO Regulation Presentation* [7 novembre 2022]). La PERCI vise à centraliser, à coordonner et à faciliter la transmission des injonctions de retrait et des signalements ; elle aide les autorités compétentes des États membres à établir les injonctions de retrait ou les signalements et à les transmettre aux points de contact spécialisés.
[421] Voir TERREG, *op. cit.*, considérant 40.

contenus à caractère terroriste par l'intermédiaire de leurs services et pour leur permettre de prendre des mesures volontaires[422].

Concernant les injonctions de retrait transfrontières émises au sein de l'Union, le TERREG instaure une nouvelle procédure, qui exige notamment que l'État membre émetteur transmette une copie de l'injonction à l'autorité compétente[423] de l'État où le fournisseur d'hébergement a son établissement principal, afin de permettre à l'autorité destinataire de procéder à un examen approfondi de l'injonction. Si l'autorité destinataire doit pouvoir partir du principe qu'une injonction de retrait émise dans un autre État membre est licite, elle a la possibilité de déterminer par elle-même si l'ordre respecte les dispositions du TERREG et ne va pas à l'encontre des normes consacrées par la Charte des droits fondamentaux de l'Union européenne[424].

Le TERREG prévoit également des obligations de diligence raisonnable supplémentaires pour les hébergeurs identifiés comme des fournisseurs qui ont précédemment été exposés à des contenus à caractère terroriste[425], qui devront dès lors appliquer des mesures dites « spécifiques ». Ces dernières recouvrent notamment l'identification et le retrait préventif des contenus à caractère terroriste[426]. Les fournisseurs de services d'hébergement ne sont toutefois pas tenus d'avoir recours à des outils automatisés pour identifier ou retirer ces contenus, ce qui contreviendrait par ailleurs à l'interdiction d'obligation générale de surveillance énoncée à l'article 8 du Règlement sur les services numériques (DSA) et, antérieurement, dans la Directive sur le commerce électronique[427].

C'est à la Commission européenne qu'il incombe d'assurer un suivi étroit de la mise en œuvre du TERREG[428]. Afin de sensibiliser aux actions entreprises dans le cadre du règlement, un fournisseur de services d'hébergement qui a pris des mesures contre la diffusion de contenus à caractère terroriste, ou auquel il a été fait obligation de prendre des mesures en vertu du TERREG, doit mettre à la disposition du public des rapports de transparence concernant ces mesures[429]. Puisqu'il n'introduit pas de responsabilité civile pour les contenus hébergés, le TERREG s'appuie sur un système de sanctions. En vertu de son article 18, les États membres sont ainsi tenus d'adopter un régime de sanctions ; le non-respect systématique ou persistant des obligations de retrait des contenus est passible de sanctions financières pouvant atteindre jusqu'à 4 % du chiffre d'affaires mondial du fournisseur de services d'hébergement[430].

Malgré un champ d'application très limité, à la fois s'agissant du type de contenu concerné et parce qu'il ne concerne que les fournisseurs de services d'hébergement, le rapport sur la mise en œuvre du TERREG conclut que celui-ci a eu un effet positif, en

[422] *Ibid.*
[423] Voir le site dédié de la Commission européenne pour une liste des autorités nationales compétentes.
[424] TERREG, Article 4.
[425] *Ibid.*, l'article 5, paragraphe 4.
[426] *Ibid.*, Article 5.
[427] Union européenne, Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« Directive sur le commerce électronique »).
[428] *Ibid.*, Article 21.
[429] *Ibid.*, Article 7, paragraphe 2.
[430] *Ibid.*, Article 18, paragraphe 3.

limitant la diffusion de contenus terroristes en ligne[431]. Toutefois, à examiner de plus près ce rapport, il s'avère que les informations reçues par la Commission européenne ne portent que sur 349 injonctions de retrait émises par les autorités compétentes[432] de six États membres (l'Espagne, la Roumanie, la France, l'Allemagne, la Tchéquie et l'Autriche) entre juin 2022 et le 31 décembre 2023[433]. Le déploiement, le 3 juillet 2023, de l'outil technique PERCI, élaboré par Europol et devenu un nouveau canal de communication pour lutter contre les contenus illégaux, a entraîné une augmentation du nombre de signalements ; plus de 14 000 d'entre eux ont été traités entre ce lancement et la fin de l'année 2023[434]. La transmission des demandes de suppression, qui prennent désormais la forme d'injonctions de retrait, reste difficile lorsque les fournisseurs de services d'hébergement sont basés dans des pays tiers et n'ont pas désigné de représentant légal dans l'Union[435].

Parallèlement au TERREG et au suivi de sa mise en œuvre, la Commission européenne poursuit sa collaboration avec les États membres, Europol et les acteurs du secteur qui le souhaitent, notamment au sein du Forum de l'UE sur l'internet. Ainsi, un exercice de simulation a été organisé en 2024 dans le cadre du protocole de crise de l'UE, un mécanisme volontaire permettant une réaction rapide et coordonnée de la part des États membres et des plateformes en ligne face à la propagation de contenus à caractère terroriste en ligne en cas d'attaque terroriste[436]. Europol a en outre contribué à la mise en place d'une « base de données d'empreintes numériques » des contenus à caractère terroriste connus, afin de permettre le marquage électronique des contenus identifiés comme préjudiciables, dans le but d'empêcher leur réapparition[437].

Il convient de noter que le DSA s'applique sans préjudice des règles établies par le TERREG, c'est-à-dire que le régime de responsabilités de ce dernier prime sur les dispositions connexes du DSA en ce qui concerne, par exemple, l'exécution des injonctions de retrait[438]. Conformément à l'article 16, paragraphes 5 et 6, du DSA, les très grandes plateformes et les très grands moteurs de recherche (TGP et TGMR) doivent notifier dans les meilleurs délais aux particuliers ou entités concernés leurs décisions relatives à la modération des contenus, en leur fournissant des informations complémentaires sur les possibilités de recours ; autrement dit, ils doivent également informer les particuliers ou entités concernés lorsqu'ils agissent à la suite d'un signalement ou d'une injonction de retrait.

---

[431] Commission européenne, Rapport de la Commission au Parlement européen et au Conseil sur la mise en œuvre du règlement (UE) 2021/784 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne, *op. cit.*

[432] Voir le site dédié de la Commission européenne pour une liste des autorités nationales compétentes et des points de contact.

[433] Commission européenne, Rapport de la Commission au Parlement européen et au Conseil sur la mise en œuvre du règlement (UE) 2021/784 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne, *op. cit.*

[434] *Ibid.*

[435] *Ibid.*

[436] Europol, « *Tabletop Exercise Hosted by Europol to Disrupt Terrorist Content Online* », communiqué de presse, 7 mars 2024.

[437] Commission européenne, « Programme de lutte antiterroriste pour l'UE et mandat renforcé pour Europol : questions et réponses », communiqué de presse, 9 décembre 2020.

[438] DSA, Article 2, paragraphe 4, point *c*).

Il est à noter en outre que le DSA couvre un éventail de services plus large que le TERREG ; cependant, les TGP/TGMR présentent un intérêt particulier du point de vue des mesures visant à lutter contre la diffusion de contenus à caractère terroriste. En raison des risques systémiques inhérents aux TGP/TGMR, les fournisseurs de ces services doivent notamment procéder à une évaluation des risques liés à la diffusion de contenus illicites, y compris à caractère terroriste, et à leurs effets négatifs prévisibles sur les droits de l'homme, conformément au DSA. Les risques liés à la diffusion de contenus illicites doivent être identifiés, analysés et traités avec diligence[439]. L'exposition à des contenus à caractère terroriste varie considérablement d'une TGP ou d'un TGMR à l'autre, en raison de leur nature très diverse.

Dès lors qu'un risque systémique de diffusion et d'exposition à des contenus à caractère terroriste est identifié, les mesures d'atténuation imposent à la TGP ou au TGMR concerné de se coordonner et d'échanger avec différents acteurs. Toute mesure adoptée par les TGP/TGMR vis-à-vis de contenus à caractère terroriste doit être raisonnable et atténuer efficacement les risques systémiques spécifiques mis en évidence[440].

En revanche, en vertu du TERREG, un fournisseur de services d'hébergement n'est tenu de mettre en œuvre des « mesures spécifiques », visant notamment à réduire son degré d'exposition aux contenus à caractère terroriste, qu'une fois que son exposition à ces contenus a été formellement établie par son autorité compétente de référence. La décision de l'autorité compétente doit être fondée sur des éléments objectifs, tels que la réception de deux injonctions de retrait ou plus au cours d'une même année[441]. Il s'agit donc d'une forme d'atténuation réactive, tandis que le DSA exige que les TGP/TGMR se montrent proactifs pour procéder à une évaluation préventive des risques. S'il existe des codes de conduite pour d'autres domaines à risque, le TERREG prévoit déjà des mesures d'atténuation s'agissant des signalements, des injonctions de retrait et des « mesures spécifiques », dès lors qu'un hébergeur a été exposé à des contenus à caractère terroriste[442].

L'article 18 du DSA impose en outre aux hébergeurs qui ont connaissance d'informations conduisant à soupçonner qu'une infraction pénale présentant une menace pour la vie ou la sécurité d'une personne a été, est en train ou est susceptible d'être commise, d'en informer promptement les autorités répressives ou judiciaires et de leur fournir des informations pertinentes. Les infractions ne sont pas détaillées, toutefois le considérant 56 du DSA indique que sont visées ici les infractions définies dans la directive 2017/541 sur la lutte contre le terrorisme, telles que la provocation à commettre une infraction terroriste.

Faisant usage des pouvoirs d'enquête et d'exécution que lui confère le DSA, la Commission européenne a d'ores et déjà engagé des procédures formelles à l'encontre de certaines TGP – ainsi contre le réseau X, pour n'avoir pas évalué correctement le risque de diffusion de contenus à caractère terroriste[443] (en particulier dans le contexte des attentats terroristes menés par le Hamas contre Israël), en raison de la conception et du

[439] DSA, Considérants 53 et 55.
[440] Voir DSA, considérant 86.
[441] TERREG, Article 5, paragraphe 4.
[442] TERREG, Articles 3 à 5 et considérant 40.
[443] Commission européenne, « La Commission ouvre une procédure formelle à l'encontre de X au titre du Règlement sur les services numériques », communiqué de presse, 18 décembre 2023.

fonctionnement mêmes du service[444]. À l'avenir, les obligations de transparence et les rapports prévus par le TERREG et le DSA permettront d'en savoir plus sur l'exposition des intermédiaires aux contenus à caractère terroriste et sur les mesures prises pour empêcher la diffusion de ces contenus.

4.2. L'exemple de l'Allemagne

Dr Sandra Schmitz-Berndt, chercheuse associée, Institut du droit européen des médias (EMR)

4.2.1. Cadre juridique national concernant les plateformes

Dans le sillage de l'adoption du DSA, la réglementation applicable aux plateformes en Allemagne a connu plusieurs évolutions, notamment avec le vote de la *Digitale-Dienste-Gesetz*[445] (loi sur les services numériques – DDG) qui met en œuvre le DSA. Elle s'applique sauf mention contraire à l'ensemble des services numériques au sens de l'article 1, paragraphe 1, point *b*), du DSA. La nouvelle loi ressemble également au règlement dans sa structure et vient unifier en un seul texte législatif des réglementations intermédiaires antérieures, notamment les éléments pertinents de la transposition nationale de la Directive SMA et les exonérations de responsabilité pour les intermédiaires. La DDG vient compléter le DSA en octroyant des compétences ; elle fait ainsi du Bundeskriminalamt[446] (Office fédéral de la police judiciaire – BKA) l'autorité compétente pour la notification des soupçons d'infraction pénale en vertu de l'article 18 du DSA[447]. L'autorité compétente en matière de contrôle des fournisseurs de services intermédiaires et de mise en œuvre du DSA est la Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Agence fédérale des réseaux d'électricité, de gaz, de télécommunication, de poste et de chemin de fer – BNetzA), qui assure le rôle de coordinateur pour les services numériques (DSC) pour l'Allemagne. Le DSC agit en toute indépendance dans l'accomplissement des missions et dans l'exercice des pouvoirs qui lui incombent. La DDG détermine également le régime de sanctions applicable en cas d'infraction au DSA.

Bien que l'adoption du DSA ait entraîné des changements significatifs dans le cadre juridique national, il est intéressant d'examiner le paysage législatif antérieur, et notamment la *Netzwerkdurchsetzungsgesetz*[448] (loi d'application du droit sur les réseaux –

[444] Décision de la Commission d'ouvrir une procédure en vertu de l'article 66, paragraphe 1, du règlement (UE) 2022/2065 (en anglais), COM(2023) 9137 final, 2023.
[445] *BGBl* (Journal officiel), 2024 I, n° 149.
[446] Le BKA est l'Office fédéral de la police judiciaire en Allemagne.
[447] DDG, Article 13.
[448] Loi d'application du droit sur les réseaux (*Netzwerkdurchsetzungsgesetz* – NetzDG) du 1er septembre 2017, *BGBl*. I, p. 3 352. Une traduction anglaise en est disponible sur : https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf;jsessionid=798A2B22B939C8AEEA23B03619CC3544.2_cid289?__blob=publicationFile&v. Pour un aperçu de la version initiale de la NetzDG, voir S. Schmitz et C. Berndt, « *The German Act on Improving Law Enforcement on Social Networks (NetzDG): A Blunt Sword?* », *SSRN*, 2018.

NetzDG), qui a fait abondamment parler d'elle[449] tant en Allemagne qu'à l'étranger, et est considérée comme l'un des textes qui ont inspiré le DSA et, avant lui, le TERREG[450]. La NetzDG comportait une liste des infractions pénales constituant des « contenus illicites » et obligeait les fournisseurs de réseaux sociaux à mettre en place une procédure efficace et transparente pour traiter les plaintes relatives à ces contenus illicites[451]. Cette procédure imposait au fournisseur de supprimer les contenus manifestement illicites dans un délai de 24 heures en général[452]. Le fournisseur était également tenu de mettre en place une procédure efficace et transparente permettant à la fois au plaignant et à l'utilisateur dont le contenu avait été signalé de demander une révision de la décision de suppression de celui-ci. De surcroît, les réseaux sociaux relevant du champ d'application de la NetzDG devaient signaler au BKA tout « contenu illicite » constituant l'une des infractions énumérées à l'article 3*a* de la NetzDG ; le BKA avait mis en place une cellule centrale destinée à recueillir les signalements, la Zentrale Meldestelle für strafbare Inhalte im Internet (Cellule centrale de signalement des contenus répréhensibles sur internet – ZMI BKA). Parmi ces infractions figuraient la diffusion de matériel de propagande d'organisations terroristes, l'utilisation de symboles d'organisations terroristes et la formation d'organisations terroristes. En outre, la loi prévoyait l'obligation d'établir un rapport semestriel éclairant le traitement des plaintes ; celle-ci était complétée par une obligation de rendre compte des efforts déployés pour atténuer les « activités pénalement répréhensibles », par un mécanisme de signalement, par la mise en œuvre de mesures de modération des contenus, ainsi que par des précisions quant au processus de décision[453]. Les informations relatives aux pratiques de modération détaillaient également les qualifications professionnelles attendues des modérateurs de contenus humains, et notamment leurs compétences linguistiques, une exigence qui figure désormais également dans le DSA. Dans le sillage de l'entrée en vigueur du DSA, de vastes pans de la NetzDG ont été abrogés en 2024 ; seule demeure l'obligation de désigner un destinataire autorisé pour la signification des actes[454], tandis que les obligations incombant aux fournisseurs sont désormais intégrées dans la DDG, comme indiqué plus haut.

Concernant la responsabilité des fournisseurs de plateformes en matière de contenus tiers, il existe une abondante jurisprudence des tribunaux allemands, et notamment de la Bundesgerichsthof[455] (Cour fédérale de justice – BGH), qui examine principalement l'applicabilité de l'exonération de responsabilité prévue par le texte qui mettait précédemment en œuvre en droit allemand l'article 14 de la directive sur le commerce électronique (désormais remplacé par l'article 6 du DSA), la portée des obligations de retrait et de retrait définitif, ainsi que la notion allemande de *Störerhaftung*

---

[449] Au sujet de la controverse, voir W. Schulz., « *Regulating Intermediaries to Protect Privacy Online – the Case of the German NetzDG* », *in* W. Schulz, M. C. Kettemann et A. P. Heldt (éd.), « *Probleme und Potenziale des NetzDG – ein Reader mit fünf HBI-Expertisen* », *Arbeitspapiere des Hans-Bredow-Instituts*, 48, 2019, p. 13 et s.

[450] D. Holznagel, « *Chapter II des Vorschlags der EU-Kommission für einen Digital Services Act—Versteckte Weichenstellungen und ausstehende Reparaturen bei den Regelungen zu Privilegierung, Haftung & Herkunftslandprinzip für Provider und Online-Plattformen* », *Computer und Recht,* 2021, pp. 123-132 ; J. Kahl et S. Liepert, « *Digital Services Act: Was sich gegenüber dem NetzDG ändert* », *heise online*, 9 décembre 2022.

[451] NetzDG, Articles 1, 3.

[452] *Ibid*., Article 1, paragraphe 2.

[453] Ibid., Article 2.

[454] *Ibid*., Article 5.

[455] La BGH est la plus haute instance judiciaire allemande en matière civile et pénale.

(littéralement, « responsabilité de la personne causant un trouble »). Cette dernière désigne un régime de responsabilité stricte, dérivé du droit de la propriété, qui autorise un propriétaire à demander que toute atteinte préjudiciable à sa propriété cesse et soit interdite à l'avenir, même lorsqu'elle n'est pas directement causée par la personne à laquelle il adresse sa requête[456]. Dès lors qu'un fournisseur de plateforme a été informé d'une infraction, il doit non seulement concéder une mesure injonctive à la partie lésée, mais aussi prendre des mesures préventives.

Les textes juridiques de l'Union européenne ont de plus en plus tendance à remplacer et à modifier la législation nationale dans le domaine du numérique. Par conséquent, outre le DSA avec son régime de responsabilité et ses règles en matière d'atténuation des risques systémiques, les plateformes proposant des services en Allemagne comme dans tous les autres États membres sont désormais soumises aux règles d'application directe fixées par le RGPD, le DMA ou le TERREG.

4.2.2. Dispositions spécifiques concernant les contenus à caractère terroriste

Le *Strafgesetzbuch* (Code pénal allemand – StGB) définit différentes infractions pénales en matière de terrorisme, et notamment : la diffusion de matériel de propagande terroriste[457], l'utilisation de symboles d'organisations terroristes[458], le soutien à des organisations terroristes[459], la provocation publique à commettre des infractions criminelles et notamment des actes terroristes[460], enfin le fait de cautionner des actes terroristes[461/462].

Cependant, l'application du droit pénal national atteint souvent ses limites dans le cas des contenus diffusés en ligne. Celles-ci peuvent être de nature factuelle (par exemple, quand il est impossible d'identifier l'auteur de l'infraction), juridictionnelle (par exemple, en cas d'absence de lien territorial) ou pratique[463] (par exemple, s'il est difficile d'appliquer le droit pénal national à des acteurs étrangers). D'autres défis se posent également à l'égard

[456] *Bürgerliches Gesetzbuch* (Code civil allemand – BGB), Article 1004 ; voir BGH, *Internet-Versteigerung* (11 mars 2004), affaire nº I ZR 304/01 36 ; BGH, *Internet-Versteigerung II* (19 avril 2007), affaire nº I ZR 35/04 ; BGH, *Internet-Versteigerung III* (30 avril 2008), affaire nº I ZR 73/05. Dans le cadre de ce régime de responsabilité stricte, une personne peut être considérée comme (indirectement) responsable d'avoir permis ou facilité une activité illégale menée par autrui, même si elle n'a pas commis elle-même cet acte illégal ; il suffit pour l'établissement de la responsabilité que la personne ait joué un rôle dans le déclenchement de l'infraction ou contribué à la permettre. Ainsi, dans les jurisprudences citées, un fournisseur de site web d'enchères a pu être jugé responsable d'avoir contribué à une infraction, par exemple en fournissant la plateforme qui a permis la publication d'annonces illégales, dans la mesure où il avait ou aurait dû avoir connaissance de cette activité illégale et n'a pas agi, alors même qu'il avait la capacité technique d'arrêter ou d'empêcher l'infraction.
[457] StGB, Article 86, *op. cit.*.
[458] *Ibid.*, Article 86*a*.
[459] *Ibid.*, Articles 129*a* et 129*b*.
[460] *Ibid.*, Article 111.
[461] Ibid., Article 140.
[462] Ces infractions figuraient toutes dans la liste des contenus répréhensibles devant être supprimés rapidement en vertu de la NetzDG.
[463] Voir J. Ukrow J, « Introduction et aperçu », *in* M. Cappello (éd), *L'application du droit des médias sans frontières,* IRIS *Spécial*, Observatoire européen de l'audiovisuel, Strasbourg, 2018, p. 3 et s.

de certains comportements précis : ainsi, la négation de la Shoah constitue une infraction pénale en droit allemand[464], alors qu'elle est considérée comme légale dans d'autres États. Afin de garantir la prompte suppression des contenus à caractère terroriste sur les grandes plateformes de réseaux sociaux, la NetzDG traitait la négation de la Shoah dans une catégorie à part et avait instauré le régime de suppression décrit ci-dessus (voir XXXXXX). Le TERREG adopte une démarche similaire à celle de la NetzDG, consistant à viser principalement les fournisseurs de services d'hébergement qui proposent leurs services au sein de l'Union.

Avec l'adoption du TERREG et du DSA, de nouveaux niveaux de conformité ont été instaurés, et les obligations de retrait et de retrait définitif relèvent désormais directement du droit de l'Union harmonisé en vigueur. Toutefois, il était nécessaire d'adopter certaines mesures d'exécution en droit allemand, principalement concernant les autorités compétentes et l'application à l'échelon national.

Le BKA est l'instance désignée par l'Allemagne pour émettre les demandes de retrait conformément à l'article 3 du TERREG, ainsi que pour examiner les injonctions de retrait adressées aux fournisseurs de services d'hébergement allemands par les autorités d'autres États membres de l'Union. En complément, la BNetzA est l'autorité compétente qui chapeaute les mesures de protection techniques et inflige les sanctions. Elle supervise par conséquent la mise en œuvre de mesures spécifiques, telles que la modération des contenus conformément à l'article 5 du TERREG pour les fournisseurs de services d'hébergement établis en Allemagne, et prend en outre les décisions au titre de l'article 5, paragraphe 4, du TERREG, visant à déterminer si un fournisseur de services d'hébergement est exposé à des contenus à caractère terroriste en ligne[465]. C'est également à la BNetzA qu'incombe l'ensemble des procédures relatives aux amendes administratives infligées en vertu du TERREG. Le BKA constitue quant à lui le point de contact au sens de l'article 12, paragraphe 2, du TERREG, et a compétence pour recevoir des notifications au sujet de contenus présentant une menace imminente pour la vie au sens de l'article 14, paragraphe 5, du TERREG. Tant le BKA que la BNetzA doivent publier des informations et des rapports de transparence, entre autres, conformément à l'article 8 du TERREG[466]. Afin de faire respecter les injonctions évoquées plus haut, émises en vertu de l'article 3, paragraphe 1, et de l'article 5, paragraphe 6, du TERREG, une amende coercitive jusqu'à concurrence de 5 millions d'euros peut être infligée en vertu de la *Verwaltungsvollstreckungsgesetz*[467] (loi sur l'exécution par voie administrative – VwVG). En outre, un régime détaillé de sanctions figure à l'article 6 de la *Terroristische-Online-Inhalte-Bekämpfungs-Gesetz*[468] (loi visant à combattre les contenus à caractère terroriste en ligne – TerrOIBG), qui prévoit des amendes administratives pouvant atteindre 5 millions d'euros pour les personnes physiques et jusqu'à concurrence de 4 % du chiffre d'affaires annuel mondial pour les personnes morales.

---

[464] En vertu de l'article 130 du StGB. Voir M. Heger, « *Paragraph 130 StGB* », *in* K. Lackner et K. Kühl (éd.), *Strafgesetzbuch*, C. H. Beck, Munich, 31e édition, 2025, paragraphes 8 et s.

[465] Ce point est réglementé dans la loi de mise en œuvre du règlement, la *Terroristische-Online-Inhalte-Bekämpfungs-Gesetz* (loi visant à combattre les contenus à caractère terroriste en ligne - TerrOIBG).

[466] *Ibid*., Article 4.

[467] *Ibid*., Article 5.

[468] Loi de mise en œuvre du TERREG (TerrOIBG).

Outre ces différents cadres réglementaires, la ZMI BKA, qui a été créée pour centraliser les notifications de soupçons d'infractions pénales en vertu de la NetzDG et qui continue à assurer cette mission s'agissant des infractions pénales mettant en danger la vie humaine en vertu du DSA, a également noué une coopération avec les parties prenantes sur la base du volontariat, dans le but de lutter contre les crimes de haine. Si l'accent est mis sur ce type de crimes, son champ d'application ne se limite pas aux seuls discours de haine. Les utilisateurs peuvent signaler des contenus haineux ou extrémistes aux parties prenantes ; ces dernières les évaluent et, s'ils relèvent du droit pénal, transmettent la notification à la ZMI BKA qui procède à une évaluation synthétique plus approfondie et identifie l'auteur potentiel de l'infraction. Le fait que certains partenaires de coopération possèdent le statut de signaleur de confiance au titre du DSA n'a aucune incidence sur l'évaluation ; il signifie simplement que les notifications réalisées par les signaleurs de confiance auprès des hébergeurs doivent être traitées en priorité par ces derniers. À ce jour, cette coopération réunit notamment le *Land* de Hesse[469], une fondation[470], les autorités de régulation des médias des *Länder* allemands, ainsi que les bureaux du procureur[471]. Ces canaux de signalement visent à fournir un service facile d'accès, venant compléter le dépôt d'une plainte pénale auprès d'une autorité chargée de l'application de la loi. L'intérêt du travail de la ZMI BKA, dans le cas des contenus à caractère terroriste en ligne, réside dans le fait que la cellule doit coopérer avec les autorités de régulation des médias afin d'engager des procédures de suppression des contenus illégaux. En vertu du *Jugendmedienschutz-Staatsvertrag* (Traité inter-*Länder* sur la protection des mineurs dans les médias – JMStV), ces autorités ont compétence pour faire supprimer tout un éventail de contenus illégaux[472] recouvrant également les infractions terroristes, et comprenant notamment la représentation d'actes de violence cruels ou inhumains à l'encontre de personnes d'une manière qui glorifie ou banalise cette violence[473]. Les pouvoirs d'exécution recouvrent des amendes ainsi que d'autres mesures coercitives relevant du droit administratif.

Les autorités de régulation des médias disposent également de pouvoirs d'exécution pour lutter contre les contenus relevant du droit pénal en vertu du *Medienstaatsvertrag* allemand (Traité inter-*Länder* sur les médias – MStV), qui s'applique aussi aux intermédiaires internet. Ces pouvoirs d'exécution s'étendent aux fournisseurs d'accès, dès lors que le fournisseur de contenu ou l'hébergeur ne se conforme pas à une première injonction de supprimer le contenu illégal concerné. Ainsi, une autorité de

[469] Le *Land* de Hesse a mis en place la *Meldestelle HessenGegenHetze* qui recueille les signalements de discours de haine et de contenus à caractère extrémiste.

[470] La fondation Jugendstiftung beim Demokratiezentrum Baden-Württemberg a créé REspect!, un portail permettant de signaler les discours de haine.

[471] Ainsi, le bureau du procureur de Göttingen, autorité centrale de lutte contre les crimes de haine en ligne dans le *Land* de Basse-Saxe, dispose d'un outil de notification sur un site dédié.

[472] Voir l'article 4 de la JMStV, ainsi que J. Ukrow, « *Paragraph 4 JMStV* », *in* M. D. Cole, J. Oster et E. E. Wagner (éd.), *Medienstaatsvertrag, Jugendmedienschutz-Staatsvertrag (HK-MstV)*, C. F. Müller, Heidelberg, 104e éd. supp., septembre 2025.

[473] Voir l'article 20 de la JMStV. L'article 5*b* de la JMStV prévoit aussi l'obligation, pour les fournisseurs de plateformes de partage de vidéos, de mettre en œuvre une procédure de notification des contenus illégaux. Cette obligation a été critiquée au motif qu'elle serait contraire au droit de l'UE, dans la mesure où elle ne tiendrait pas compte de l'effet d'harmonisation totale du DSA, et elle n'a jusqu'à présent eu aucune incidence dans la pratique, voir M. Liesching, « *Paragraph 5*b *JMStV* », *in* M. Liesching (éd.), *BeckOK Jugendschutzrecht*, C. H. Beck, Munich, 5e édition, 2025, paragraphe 2.

régulation des médias a adopté en dernier recours une décision de blocage à l'encontre de grands fournisseurs d'accès allemands, afin d'empêcher l'accès aux plateformes pornographiques[474].

4.2.3. Application à la suite de l'attaque terroriste d'octobre 2023 perpétrée par le Hamas en Israël

Dans le sillage de l'attaque terroriste perpétrée par le Hamas en Israël le 7 octobre 2023, les internautes ont été exposés dans des proportions inédites à des contenus à caractère terroriste. Au cours de l'attaque, le Hamas a spécifiquement exploité les technologies internet, notamment en diffusant en direct ses atrocités à l'aide de téléphones portables et de caméras corporelles, sur des plateformes telles que Telegram et Facebook[475]. Des contenus montés en temps réel ont également été diffusés sur les plateformes de réseaux sociaux[476]. Par la suite, les réseaux sociaux ont en outre été exposés à des discours haineux présentés sous des *hashtags* tels que *#freepalestine*. Contrairement à la plupart des autres États membres de l'Union, les autorités de régulation allemandes ont réagi rapidement en s'appuyant activement sur le TERREG. Si l'Allemagne s'est emparée sans tarder des possibilités offertes par le règlement, c'est d'abord parce que le pays possède une sensibilité historique et juridique particulière aux questions d'antisémitisme et de terrorisme ; par ailleurs, les autorités allemandes avaient acquis une certaine expérience avec la ZMI BKA, cellule centrale de signalement qui joue dans le cadre actuel de l'article 18 du DSA le même rôle que précédemment sous le régime de la NetzDG, à savoir celui de l'autorité compétente pour recevoir les notifications de soupçons d'infractions pénales. L'exemple de l'attaque du Hamas et de ses suites, marquées par une augmentation significative de la quantité de contenus illégaux, de désinformation et de discours de haine sur les réseaux sociaux[477], illustre bien le fonctionnement du régime de retrait du TERREG dans la pratique.

Ainsi qu'on l'a indiqué plus haut, 349 injonctions de retrait au titre du TERREG ont été émises par les autorités compétentes de six États membres entre juin 2022 et le 31 décembre 2023. Elles émanaient d'Allemagne pour la grande majorité d'entre elles[478] (pas moins de 249). Toutes ces injonctions étaient destinées à des hébergeurs situés hors du pays et ont été respectées. En revanche, seules deux injonctions de retrait ont été émises par les autorités compétentes d'un autre État membre à l'encontre de fournisseurs d'hébergement allemands. S'agissant de l'émission d'injonctions et de l'évaluation des demandes transfrontières, le BKA peut coopérer avec les autorités nationales de régulation des médias des *Länder* allemands. Le Landesanstalt für Medien (office régional des médias)

---

[474] Voir S. Schmitz-Berndt, « Le Verwaltungsgericht de Berlin rejette le recours en référé de plateformes pornographiques contre la décision de blocage de la LMA compétente », *IRIS* 2025-6:1/18, Observatoire européen de l'audiovisuel, 2025.
[475] E. Cortellessa, « *The Oct. 7 Massacre Revealed a New Hamas Social Media Strategy* », *TIME*, 31 octobre 2023.
[476] D. Loucaides, « *How Telegram Became a Terrifying Weapon in the Israel-Hamas War* », *WIRED*, 31 octobre 2023.
[477] Bundesministerium des Inneren (ministère fédéral allemand de l'Intérieur), « *Wellen des Hasses stoppen* » (« Mettre fin aux déferlements de haine »), communiqué de presse, 13 février 2024.
[478] BKA, *Umsetzung der TCO-Verordnung im Bundeskriminalamt – Transparenzbericht für das Jahr 2023*, 2024.

de Rhénanie-du-Nord-Westphalie, dans son rôle de représentant de l'ensemble des autorités chargées des médias, est ainsi régulièrement sollicité.

Au 21 novembre 2023, la plupart des injonctions émises concernaient l'attaque d'octobre 2023 menée par le Hamas contre Israël et étaient adressées à Telegram[479]. De fait, entre le 7 octobre et le 21 novembre 2023, le BKA a émis 153 injonctions de retrait à l'encontre de Telegram et de X, visant la propagande du Hamas et du Jihad islamique palestinien[480]. Si ce chiffre semble modeste, c'est parce qu'avant d'émettre une injonction de retrait, le BKA a couramment recours à l'instrument du « signalement » ou de la demande de retrait, un appel à agir adressé aux hébergeurs qui leur donne l'occasion d'intervenir de leur plein gré.

En 2023, le BKA a transmis 7 240 signalements ; 5 762 d'entre eux ont conduit à la suppression du contenu visé ou au blocage de l'accès à celui-ci. En raison de leur caractère non contraignant, ces signalements n'ont pas à être traités dans un délai déterminé. Toutefois, le BKA s'assure que le contenu a été supprimé ou désactivé après deux jours ouvrables[481]. Ce délai répond à l'exigence d'agir « promptement » associée à l'exonération de responsabilité de l'article 6, paragraphe 1, du DSA applicable aux hébergeurs. Lorsqu'un hébergeur ne réagit pas dans ce délai, le BKA émet au besoin une injonction de retrait. Celle-ci peut également être émise directement, sans demande préalable de retrait volontaire. Dans les faits, en réponse aux contenus évoqués plus haut, diffusés par le Hamas et le Jihad islamique palestinien en octobre 2023, le BKA a d'abord envoyé des signalements, puis émis des injonctions de retrait, les premiers n'ayant pas été suivis d'effet.

En 2023, la BNetzA a estimé que le premier fournisseur allemand de services d'hébergement était « exposé à des contenus à caractère terroriste » et lui a enjoint de prendre les mesures nécessaires pour qu'il cesse de mettre ces contenus à la disposition du public, conformément à l'article 5 du TERREG[482]. Cette qualification s'appuyait sur la grande quantité de demandes de signalement du BKA et sur les deux injonctions de retrait dont avait fait l'objet l'hébergeur concerné[483]. Le fournisseur a par la suite renforcé les mesures techniques et organisationnelles existantes pour lutter contre la diffusion de contenus terroristes en ligne.

La BNetzA et le BKA estiment que les mesures prises par le fournisseur d'hébergement concerné ont globalement permis de réduire efficacement la diffusion de contenus à caractère terroriste en ligne ; des améliorations notables ont été relevées au cours de la période de référence 2024. Une évaluation est en cours concernant les capacités indépendantes d'identification et de réaction du fournisseur. Une enquête menée auprès des fournisseurs d'hébergement a permis d'identifier un certain nombre de mesures qui ont été adoptées : mesures organisationnelles (par exemple, liées aux conditions d'utilisation), mesures techniques (par exemple, détection automatisée des combinaisons d'émoticônes

[479] Voir Deutscher Bundestag, « *Antwort der Bundesregierung auf die kleine Anfrage der Fraktion der CDU/CSU – Drucksache 20/9299 – Social-Media-Terrorismus* », 2023, *BT-Drs.* 20/9688.
[480] Les injonctions de retrait ont été émises à l'encontre de X (10 injonctions) et de Telegram (143), voir *ibid.*
[481] BNetzA, *Transparency Report as per Article 8 of the Terrorist Content Online Regulation and Section 4 of the Act Addressing Terrorist Content Online and Monitoring Report as per Article 21(1) of the Regulation and Section 3 of the Act*, 2024, p. 7.
[482] *Ibid.*
[483] *Ibid.*, p. 8.

extrémistes, restriction de certains noms d'utilisateur, d'URL et des comptes bloqués) et procédures manuelles[484] (par exemple, équipes de modération des contenus, évaluation des tendances et des tactiques de contournement). En 2023, ce sont en tout 15 766 éléments de contenu qui ont été retirés par le fournisseur de services d'hébergement considéré comme exposé à des contenus terroristes, en raison de mesures spécifiques prises conformément à l'article 5 du TERREG[485]. Dans 100 cas, les utilisateurs ont déposé une plainte pour contester la suppression de leur contenu, ce qui a conduit dans neuf cas à la restauration de celui-ci[486].

En 2023, les fournisseurs de services d'hébergement ont reçu de la part des autorités compétentes 139 demandes d'accès à des données[487], en lien avec des contenus ou des activités terroristes, contre seulement quatre en 2024[488]. Cette évolution met en évidence la nécessité d'un mécanisme de suppression rapide, parallèlement aux enquêtes pénales, compte tenu notamment de l'augmentation des demandes de signalement et de suppression. À noter qu'en 2024, le BKA a émis 482 injonctions de retrait, atteignant ainsi un taux de conformité de 95,9 %[489]. Le BKA a également examiné 11 injonctions de retrait émises par d'autres États membres, dont aucune n'a été contestée, et a relayé 17 045 signalements aux fournisseurs de services d'hébergement[490] (87,4 % d'entre eux ont conduit au retrait ou à la désactivation du contenu).

Outre le cadre mis en place par le TERREG, la ZMI BKA s'appuie sur son mécanisme de coopération volontaire avec certains portails internet permettant de signaler des discours de haine. Entre le 7 octobre et le 20 novembre 2023, le BKA a ainsi reçu de cette façon un total de 139 notifications qui portaient sur des contenus relevant du pénal, car constitutifs d'incitation à la haine ou à la violence contre certaines parties de la population (article 130 du StGB) et en lien avec le conflit au Proche-Orient[491].

Le BKA a également reçu des notifications de contenus par des fournisseurs de plateformes au titre de l'article 18 du DSA. Entre octobre et décembre 2023, 16 notifications seulement ont été effectuées, ce qui s'explique principalement par le fait que les obligations ne concernaient que les TGP/TGMR désignés comme tels et que la disposition n'a commencé à s'appliquer aux autres intermédiaires qu'au 17 février 2024. Sur

[484] BNetzA, *Transparency Report as per Article 8 of the Terrorist Content Online Regulation and Section 4 of the Act Addressing Terrorist Content Online and Monitoring Report as per Article 21(1) of the Regulation and Section 3 of the Act*, 2025, p. 8 et s.
[485] BNetzA, *Transparency Report as per Article 8 of the Terrorist Content Online Regulation and Section 4 of the Act Addressing Terrorist Content Online and Monitoring Report as per Article 21(1) of the Regulation and Section 3 of the Act*, 2024, p. 8.
[486] *Ibid.*
[487] *Ibid.*
[488] BNetzA, *Transparency Report as per Article 8 of the Terrorist Content Online Regulation and Section 4 of the Act Addressing Terrorist Content Online and Monitoring Report as per Article 21(1) of the Regulation and Section 3 of the Act*, 2025, p. 9.
[489] BKA, « *Transparenzbericht 2024 zur Bekämpfung terroristischer Online-Inhalte veröffentlicht* », communiqué de presse, 2025.
[490] *Ibid.*, p. 1.
[491] Voir Deutscher Bundestag, *Antwort der Bundesregierung auf die kleine Anfrage der Fraktion der CDU/CSU – Drucksache 20/9299 – Social-Media-Terrorismus*, 2023, *BT-Drs.* 20/9688, p. 5.

1 773 notifications enregistrées en 2024, 1 244 étaient de nature pénale, et seules neuf d'entre elles étaient spécifiquement liées au terrorisme[492].

Il est difficile d'isoler le nombre exact d'injonctions de retrait, de demandes de signalement et de notifications autres ou encore de suppressions effectives liées à l'attaque du Hamas. En février 2024, le ministre de l'Intérieur a déclaré que plus de 3 500 demandes de signalement avaient été formulées au total entre le 7 octobre 2023 et le 6 février 2024 concernant des contenus à caractère terroriste relatifs à l'attaque du Hamas[493]. Elles avaient donné lieu à 290 injonctions de retrait[494].

Les chiffres cités plus haut le montrent : les volumes sont significatifs et indiquent que la recrudescence des contenus à caractère terroriste s'est accompagnée d'une forte augmentation des mesures de retrait. Cette réponse rapide tient surtout à la mise en place, avant l'entrée en vigueur du TERREG, d'une infrastructure et d'un cadre institutionnel adaptés ; elle est aussi le fruit de l'expérience antérieure engrangée par les parties prenantes concernées. Les normes strictes intégrées dans la NetzDG, désormais abrogée, ont peut-être également contribué à sensibiliser les fournisseurs à la nécessité de réagir sans délai aux demandes de retrait.

4.3. L'exemple de la Türkiye

Dr Mehmet Bedii Kaya, professeur associé en droit des technologies de l'information, université Bilgi d'Istanbul

4.3.1. Cadre juridique national concernant les plateformes

La République de Türkiye est membre du Conseil de l'Europe et de l'Organisation pour la sécurité et la coopération en Europe, ainsi que candidate à l'adhésion à l'Union européenne. La pénétration d'internet est particulièrement élevée dans sa population. D'après l'institut statistique national, l'usage d'internet est passé de 27 % en 2004 à environ 97 % en 2024, soit une multiplication par un facteur de 3,6 en deux décennies. Les habitudes d'utilisation révèlent que WhatsApp, Instagram et YouTube sont actuellement les plateformes de réseaux sociaux les plus plébiscitées. Parmi elles, YouTube domine du point de vue de la consommation de données, représentant 46,1 % du trafic internet total, suivi par Instagram (13 %) et par Netflix[495] (5,9 %). Ces chiffres indiquent que le comportement des utilisateurs

[492] Parmi les contenus relevant du pénal, 1 046 éléments concernaient des contenus pédopornographiques. Les contenus considérés comme ne relevant pas du pénal concernaient principalement des annonces de suicide, qui ne constituent pas une infraction pénale, mais représentent une menace grave pour la vie. Voir Bundesregierung, « *Bericht der Bundesregierung gemäß § 13 Satz 2 des Digitale-Dienste-Gesetzes* », 27 août 2025.
[493] Bundesministerium des Inneren, « *Wellen des Hasses stoppen* », *op. cit.*
[494] *Ibid.*
[495] Pour tous les chiffres, voir Bilgi Teknolojileri ve İletişim Kurumu (Autorité turque pour les technologies de l'information et de la communication), *Türkiye Elektronik Haberleşme Sektörü, Üç Auylik Pazar Verileri Raporu* (Secteur des communications électroniques, rapport trimestriel sur les données du marché), 2025, pp. 54-56.

tend fortement à s'orienter vers les contenus vidéo, sachant que les plateformes de réseaux sociaux représentent une part importante du trafic internet global en Türkiye.

La Constitution de la République de Türkiye consacre certaines libertés publiques fondamentales, notamment la liberté d'expression, la liberté de la presse et la protection de l'intégrité tant physique que mentale des personnes. Bien que ses cadres juridiques nationaux s'inspirent souvent des normes de l'Union européenne, la Türkiye, en sa qualité de pays non membre, a adapté ces normes à ses priorités nationales et à son contexte sociopolitique. Aucune des dispositions de la Constitution ne concerne spécifiquement les technologies. Il convient cependant de noter qu'une modification importante du texte adoptée en 2010 a permis d'introduire une disposition relative à la protection des données à caractère personnel. L'article 20, paragraphe 3, de la Constitution reconnaît ainsi explicitement le droit à la protection de ces données.

La Türkiye a mis en place une infrastructure réglementaire complète destinée à préserver l'ordre public dans l'univers physique comme numérique. Au fil du temps, ces mesures réglementaires se sont accentuées et ont acquis une portée plus large, ce qui témoigne d'une évolution vers des contrôles de plus en plus stricts.

Le principal instrument législatif encadrant les activités sur internet en Türkiye est la loi n° 5651 *İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun*[496] (loi relative à la réglementation de la radiodiffusion sur internet et à la lutte contre les infractions commises dans le cadre d'une radiodiffusion en ligne – loi relative à internet).

La loi relative à internet régit principalement trois domaines réglementaires[497] :

1) les responsabilités juridiques, pénales et administratives des principaux acteurs d'internet, notamment des fournisseurs de contenu, des hébergeurs, des fournisseurs de services internet (FSI), des fournisseurs d'accès public à internet et des fournisseurs de réseaux sociaux[498] ;
2) les procédures de restriction d'accès en réaction à des infractions pénales spécifiques, et tout particulièrement les interventions d'urgence ;
3) la mise en œuvre de mécanismes de filtrage et de pratiques de surveillance d'internet.

Depuis son adoption, la loi relative à internet a connu plusieurs modifications, notamment en 2014, 2020 et 2022, qui reflètent des changements de priorités politiques et les avancées technologiques. Outre les réformes législatives, les interprétations jurisprudentielles, en particulier certaines décisions de la Cour constitutionnelle de Türkiye

[496] *5651 İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun*, JO du 23 mai 2007/26530. Pour une traduction intégrale en anglais de la loi turque relative à internet, voir cette page.

[497] Les dispositions protégeant les droits de la personnalité ont été annulées par la Cour constitutionnelle turque. Les nouvelles règles destinées à les remplacer n'ont pas encore été adoptées.

[498] Pour un examen exhaustif de la loi turque relative à internet, voir M. B. Kaya, « *The regulation of Internet intermediaries under Turkish law: Is there a delicate balance between rights and obligations?* », *Computer Law & Security Review* 32, 2016, p. 759 et s.

concernant des plateformes telles que Twitter et YouTube, ont contribué de manière significative à faire évoluer la compréhension et l'application de la loi[499].

Si la loi relative à internet était à l'origine le principal instrument réglementaire s'agissant de la gouvernance d'internet en Türkiye, le paysage législatif a depuis évolué et de nombreuses institutions se sont vu octroyer des pouvoirs en la matière dans le cadre de leurs missions officielles respectives. En conséquence, un large éventail d'organismes publics dispose désormais du pouvoir d'identifier, de supprimer et de bloquer les contenus illégaux en ligne. Cette décentralisation a conduit à une fragmentation du cadre juridique et institutionnel. Malgré la prolifération de dispositions législatives complémentaires abordant des questions connexes, la loi relative à internet demeure cependant le texte fondamental qui réglemente les contenus en ligne et les responsabilités des intermédiaires du numérique.

Ainsi qu'on l'a signalé plus haut, la loi relative à internet s'applique principalement à quelques catégories précises d'acteurs, notamment les fournisseurs de contenu, les hébergeurs, les fournisseurs de services internet (FSI), les fournisseurs d'accès public à internet et les fournisseurs de réseaux sociaux. Parmi ces intervenants, les hébergeurs occupent une place centrale. Conformément à l'article 2, paragraphe 1, point *m*), de la loi relative à internet, cette catégorie recouvre « des personnes physiques ou morales proposant des systèmes qui hébergent des services et des contenus ».

Les dispositions réglementaires applicables aux hébergeurs concernent un vaste éventail de plateformes dont les fonctions, les modèles opérationnels et les architectures techniques sont variés. Il s'agit notamment de services d'hébergement web traditionnels, tels que l'hébergement mutualisé, l'hébergement sur le *cloud*, les serveurs privés virtuels (VPS), les serveurs dédiés, les services de colocation et les réseaux privés virtuels (VPN), mais aussi des plateformes proposant l'hébergement de fichiers, d'images, de vidéos, de blogs et de messageries électroniques. Le champ d'application s'étend également aux réseaux sociaux, aux moteurs de recherche, aux plateformes d'enchères en ligne, aux places de marché numériques et à d'autres fournisseurs de plateformes en ligne[500].

La loi relative à internet n'a pas la portée nécessaire pour réglementer de manière adéquate toute la diversité des fournisseurs d'hébergement, dont les modèles d'exploitation peuvent varier considérablement. Elle dispose en particulier que les fournisseurs d'hébergement peuvent être classés en fonction de la nature de leurs services et se voir attribuer des droits et obligations différents, sur la base de principes et de procédures établis dans la législation dérivée. Cette disposition a été intégrée en 2014 dans la loi relative à internet[501] ; toutefois, aucune classification de ce type n'a été mise en œuvre à ce jour dans la législation dérivée. Par conséquent, c'est la même règle juridique qui s'applique actuellement à l'ensemble des plateformes en ligne.

En vertu de l'article 5 de la loi relative à internet, il n'est du ressort des hébergeurs ni de contrôler les contenus qu'ils hébergent ni de déterminer l'existence d'éventuelles

[499] Cour constitutionnelle de la République de Türkiye, *Affaire Twitter*, requête nº 2014/3986, 2 avril 2014 ; *Affaire YouTube*, requête nº 2014/4705, 29 mai 2014 ; voir également *Affaire loi relative à internet*, affaire nº 2014/87, décision nº 2015/112, 8 décembre 2015.
[500] Voir A. Işık, *İnternet Aktörleri ve Egemenliğin Değişen Boyutları*, On İki Levha Publishing, 2023.
[501] Modification par la loi nº 6518, JO du 19 février 2014/28918.

activités illicites. Leur responsabilité se limite à la suppression des contenus illégaux dès qu'ils sont informés de leur existence, conformément au mécanisme de notification et de retrait prévu par la loi relative à internet. Ils sont ainsi tenus de supprimer promptement les contenus illicites, afin de les rendre inaccessibles au public.

La question centrale nécessitant des éclaircissements concerne l'étendue de cette obligation de suppression. Il s'agit plus précisément de savoir si elle exige la suppression définitive du contenu incriminé des serveurs ou s'il suffit pour y satisfaire de restreindre l'accès à ce contenu pour les utilisateurs en Türkiye (ou pour le trafic provenant de Türkiye). Cette ambiguïté constitue l'un des aspects les plus controversés de la loi relative à internet. Aux termes de l'article 2 de la loi, on entend par « suppression du contenu », « la suppression du contenu des serveurs ou du contenu hébergé, par les fournisseurs de contenu ou d'hébergement ». En conséquence, si un fournisseur utilise des mesures techniques telles que le géoblocage ou applique des restrictions de contenus spécifiques à un pays, il peut encore être tenu pour responsable en vertu des dispositions de la loi relative à internet.

La loi relative à internet prévoit en outre toute une palette de sanctions judiciaires et administratives pour les fournisseurs d'hébergement qui ne respectent pas les injonctions des tribunaux ou les directives administratives, ou qui négligent de coopérer avec les autorités pertinentes.

Outre les hébergeurs, la seule catégorie de plateformes en ligne qui est définie explicitement dans le cadre de la loi relative à internet est celle des fournisseurs de réseaux sociaux[502]. Cette désignation a été introduite en 2022, à l'occasion d'une révision législative largement inspirée de la NetzDG allemande[503].

L'article 2, paragraphe 1, point *s*), de la loi relative à internet définit comme suit les fournisseurs de réseaux sociaux : « des personnes physiques ou morales permettant aux utilisateurs de créer, de consulter ou de partager des données textuelles, visuelles, audio, géolocalisées ou de nature similaire à des fins d'interaction sociale. » Les fournisseurs de réseaux sociaux sont considérés comme une sous-catégorie distincte des hébergeurs. Il est important de noter que l'application de dispositions spécifiques aux fournisseurs de réseaux sociaux n'exempte pas ces derniers des obligations et responsabilités qui leur incombent par ailleurs en leur qualité de fournisseurs d'hébergement en vertu de la loi relative à internet.

Conformément à l'article 4 additionnel de la loi relative à internet, les fournisseurs des réseaux sociaux étrangers recevant plus d'un million de visites par jour en Türkiye sont tenus de nommer au moins un représentant légal dans le pays. Les fournisseurs étrangers et nationaux de réseaux qui dépassent ce seuil doivent répondre aux demandes de notification et de retrait dans un délai de 48 heures, tout refus devant s'accompagner d'une explication motivée.

---

[502] Modification par la loi nº 7253, JO du 31 juillet 2020/31202.

[503] Pour une vue d'ensemble de la réglementation applicable aux réseaux sociaux, voir M. B. Kaya et M. F. Akıncı, « *Social Media Regulation* », *in* M. Eroğlu, M. Finger et E. Köksal (éd.), *The Economics and Regulation of Digitalisation: The Case of Türkiye*, Routledge, Abingdon, 2024. Voir également ci-dessus chapitre 4.2.1f concernant la NetzDG.

L'article 4 additionnel impose également à ces fournisseurs de remettre des rapports semestriels en turc, contenant des données statistiques et catégorielles relatives à l'exécution des décisions de suppression et de blocage des contenus. Le non-respect de ces obligations peut entraîner des amendes administratives, les sanctions pour les fournisseurs étrangers étant susceptibles d'atteindre un million de livres turques.

Dans le cadre de la loi relative à internet, la décision de bloquer l'accès aux contenus illicites en ligne et de les supprimer constitue le principal instrument mis en œuvre pour lutter contre ceux-ci. La méthode incontournable pour contrer ces infractions consiste à supprimer les contenus déclarés illégaux par décision de justice ou, sous certaines conditions, par les autorités administratives. Faute de suppression, l'accès à l'URL spécifique hébergeant le contenu illicite est bloqué ; en cas d'impossibilité technique, c'est l'accès à l'ensemble du site web qui peut être restreint.

La loi relative à internet définit un cadre général en vue de lutter contre différents types de contenus illégaux, notamment :

1) Article 8 – lutte contre certaines infractions pénales spécifiques ;
2) Article 8/A – autorisation de restrictions d'accès en cas d'urgence.

L'Autorité turque des technologies de communication et d'information (BTK) joue un rôle central dans la gestion des infrastructures de communication en Türkiye, ainsi que dans l'exécution des décisions de blocage d'accès adoptées en vertu de la loi relative à internet.

L'article 8 de la loi fixe une procédure spécifique permettant d'imposer des restrictions d'accès aux sites web présentant des contenus illicites[504]. Il n'autorise pas l'application de ces restrictions en réponse à toutes les infractions pénales, les réservant à une liste exhaustive d'infractions qu'il détaille. En d'autres termes, l'accès à un site web ne peut être bloqué que si les faits relèvent d'une infraction pénale expressément définie dans la loi. Les infractions concernées par l'article 8 sont les suivantes :

3) incitation au suicide ;
4) abus sexuels sur enfants ;
5) facilitation de la consommation de substances narcotiques ou stimulantes ;
6) fourniture de substances dangereuses pour la santé ;
7) obscénité ;
8) prostitution ;
9) mise à disposition de locaux ou de matériel destinés aux jeux d'argent ;
10) infractions visées par la loi n° 5816 *Atatürk Aleyhine İşlenen Suçlar Hakkında Kanun* (loi relative aux infractions commises au détriment de Kemal Atatürk) ;
11) paris illégaux ;
12) infractions régies par l'article 27, paragraphes 1 et 2, de la loi n° 2937 *Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu* (loi sur les services de renseignement de l'État et le bureau national de renseignement).

[504] Voir également L. Keser, « Les rapports sur les expériences pratiques d'une sélection de pays – Turquie », *in* M. Cappello (éd), *L'application du droit des médias sans frontières,* IRIS *Spécial*, Observatoire européen de l'audiovisuel, Strasbourg, 2018, p. 92.

La décision de blocage d'accès peut être rendue par un procureur lors de la phase d'enquête ou par un tribunal lors de la phase des poursuites. Il est important de relever que le terrorisme et les infractions liées à celui-ci ne figurent pas parmi les infractions pénales énumérées à l'article 8 de la loi relative à internet.

En 2015, cette loi a fait l'objet d'une réforme, qui a introduit dans le texte une disposition très controversée à l'article 8/A[505].

Dans les domaines liés à la protection de la vie et des biens, à la sécurité nationale, à l'ordre public, à la prévention de la criminalité ou à la santé publique, un juge peut rendre une décision visant à bloquer l'accès à un contenu en ligne ou à le supprimer. En cas d'urgence, cette autorité peut également être exercée par le Président de la République ou par les ministères pertinents. Dans ce cas, la décision finale de bloquer l'accès ou de supprimer le contenu revient au président de la BTK.

En vertu de l'article 8/A, dès lors qu'est rendue une décision de supprimer un contenu ou d'en bloquer l'accès pour l'un des motifs énumérés dans cette même disposition, les hébergeurs et les fournisseurs de réseaux sociaux sont tenus de s'exécuter dans les quatre heures suivant la notification officielle de la mesure.

Bien que les interventions sur la disponibilité des contenus en ligne reposent principalement sur des décisions de justice, une décision du Président ou d'un ministre concerné peut également imposer des restrictions d'accès. Selon l'article 8/A, lorsqu'une telle décision est prise sur demande du Président de la République ou d'un ministère compétent, le président de la BTK est tenu de la soumettre dans les 24 heures à la cour pénale de paix pour obtenir l'approbation d'un juge. Celui-ci doit rendre sa décision sous 48 heures, sans quoi la décision devient automatiquement nulle.

Il est devenu courant en Türkiye de prendre des mesures administratives visant à restreindre l'accès à des contenus sur internet. L'article 8/A, en particulier, en est venu à servir de base juridique générale pour la régulation des contenus en ligne. Cette disposition est de plus en plus utilisée à la manière d'un mécanisme général de blocage. Au fil du temps, elle a servi de fondement à des décisions visant à restreindre l'accès à diverses plateformes de réseaux sociaux, notamment X, Wattpad, TikTok et Instagram[506].

Sous le régime de la loi relative à internet, les décisions de blocage d'accès sont mises en œuvre grâce au ciblage d'éléments précis du contenu illicite, tels que la publication, une partie de celle-ci ou l'adresse URL. Toutefois, s'il s'avère impossible techniquement de restreindre l'accès uniquement au contenu illicite ou à ses composants connexes, les autorités peuvent décider de bloquer le site web dans son intégralité.

Le chiffrement généralisé du trafic web a rendu le blocage par URL pratiquement inefficace. Par conséquent, lorsqu'un fournisseur de services ne parvient pas à supprimer le contenu visé, c'est l'accès à l'ensemble du site web qui est généralement restreint. Cette façon de procéder est devenue une pratique de régulation admise de longue date. Elle a pu

[505] Voir *ibid*., p. 93.

[506] Voir également R. Michaelson, « *The Internet's Sewer: Why Turkey Blocked Its most Popular Social Site* », *The Guardian,* 1er mars 2023 ; « *Ekşi Sözlük'e 'milli güvenlik ve kamu düzeninin korunması' gerekçesiyle yine erişim engeli getirildi* » (« L'accès à Ekşi Sözlük bloqué à nouveau au nom de la "protection de la sécurité nationale et de l'ordre public" »), *BBC*, 14 décembre 2023.

conduire à empêcher l'accès à des plateformes entières telles que Google Sites, YouTube ou Wikipédia. Ce type de blocage généralisé a fait l'objet de plusieurs arrêts de la Cour européenne des droits de l'homme contre la Türkiye[507].

Le pays a adopté une stratégie de contrôle des contenus en ligne qui passe principalement par des méthodes de restriction reposant sur les adresses IP et les DNS. En appui à cette approche, la Türkiye a considérablement amélioré son infrastructure internet, afin d'empêcher l'accès aux contenus jugés illicites par les autorités compétentes. Un système exhaustif et avancé d'« inspection approfondie des paquets » (*deep packet inspection* – DPI) a été déployé sur tous les points d'accès du pays. Néanmoins, la prépondérance croissante des technologies de chiffrement et, en particulier, le chiffrement généralisé du trafic réduisent l'efficacité de ces systèmes de contrôle. En raison de ces limites technologiques, la Türkiye a été contrainte de réévaluer son modèle de « censure d'internet ». Ce changement a coïncidé avec un bouleversement de la gouvernance d'internet, sous l'impulsion de l'expansion rapide des réseaux sociaux, qui jouent désormais un rôle central dans les domaines social et économique.

La nouvelle approche adoptée par la Türkiye en matière de régulation entend prendre en charge à la racine la gestion des contenus sur les plateformes de réseaux sociaux. Plutôt qu'une simple limitation d'accès, elle vise la suppression complète, directement à la source, des contenus illicites ou préjudiciables. Conformément à cette évolution, la législation dans sa version révisée prévoit que les entreprises de réseaux sociaux nomment un représentant local afin de faciliter une collaboration directe avec les autorités turques. Ces plateformes sont également tenues de répondre promptement aux demandes des utilisateurs, de remettre des rapports de transparence détaillant leurs activités au chapitre de la modération des contenus, de stocker les données à caractère personnel à l'intérieur des frontières turques, de renforcer leur capacité de lutte contre les activités criminelles et de prendre des mesures proactives pour protéger les mineurs et les jeunes utilisateurs. Les dispositions réglementaires révisées concernant les réseaux sociaux, contenues dans l'article 4 additionnel de la loi relative à internet introduit en 2022, ont mis en place une structure de responsabilité unique, adaptée aux grands objectifs poursuivis par la Türkiye. Afin de garantir leur application effective, la loi relative à internet a été complétée par de nouveaux mécanismes de sanction. Les plateformes de réseaux sociaux qui ne respectent pas leurs obligations légales s'exposent à des sanctions telles que l'interdiction de la publicité, la réduction de leur bande passante, le partage de responsabilité civile pour les contenus illicites, ainsi que des amendes administratives substantielles.

4.3.2. Dispositions particulières concernant les contenus à caractère terroriste

Confrontée à de nombreux attentats terroristes au fil des ans, la Türkiye est de longue date engagée dans la lutte contre ce phénomène. Elle s'y emploie tant par des mesures

[507] Voir *Ahmet Yildirim c. Turquie*, requête n° 3111/10 (CEDH, 18 décembre 2012) et *Cengiz et autres c. Turquie*, requête n^{os} 48226/10 et 14027/11 (CEDH, 1er décembre 2015).

opérationnelles que par des instruments juridiques. S'agissant des aspects juridiques du terrorisme, une loi spécifique intitulée *Terörle Mücadele Kanunu* (loi relative à l'antiterrorisme) a été adoptée en 1991, afin d'établir le cadre juridique nécessaire pour faire face à ces menaces[508].

Ce texte apporte un cadre exhaustif, en ce qu'il définit le terrorisme, désigne les personnes responsables d'actes terroristes, décrit les infractions commises dans une intention terroriste, caractérise les organisations terroristes et fixe des procédures et des sanctions distinctes applicables à ces crimes.

La loi relative à l'antiterrorisme donne la définition suivante du terrorisme :

> *Est qualifié de terrorisme tout acte commis par une ou plusieurs personnes membres d'une organisation ayant pour objet de modifier les caractéristiques fondamentales de la République, telles qu'elles sont définies par la Constitution, ainsi que son ordre politique, juridique, social, laïque et économique ; tout acte ayant pour objet de porter atteinte à l'entité indivisible que forme l'État avec son territoire et sa nation ; tout acte ayant pour objet de mettre en danger l'existence de l'État et de la République turcs, d'affaiblir ou de détruire ou de se saisir de l'autorité de l'État, d'anéantir les droits et libertés fondamentaux ou de porter atteinte à la sécurité intérieure et extérieure de l'État, à l'ordre public ou à la santé publique, en recourant à la contrainte, à la force et à la violence, à la terreur, à l'intimidation ou à la menace.*

Dans la définition qu'en donne la loi relative à l'antiterrorisme, le terrorisme peut être le fait d'individus ou de groupes.

Sont considérées comme des crimes terroristes les infractions commises en lien avec les activités d'une organisation terroriste. Lorsqu'un acte est qualifié d'infraction terroriste, la sanction encourue est aggravée et des règles de procédure distinctes s'appliquent, en vertu du cadre juridique en vigueur.

Depuis sa promulgation, cette loi fait l'objet de débats juridiques et politiques, ses détracteurs estimant qu'elle impose des restrictions disproportionnées aux droits et libertés fondamentaux. Au fil du temps, son champ d'application et ses dispositions ont connu d'importantes modifications.

4.3.3. Application en vue de bloquer l'accès à des contenus à caractère terroriste

Les technologies numériques n'étaient pas prédominantes au moment de son adoption, aussi la loi relative à l'antiterrorisme ne contient-elle naturellement aucune mention explicite d'internet ou des domaines technologiques connexes. Néanmoins, ses définitions fondamentales ont continué à orienter et à façonner les cadres réglementaires plus récents qui régissent l'environnement numérique.

[508] Pour une traduction intégrale en anglais de la loi relative à l'antiterrorisme, voir cette page.

Contrairement à l'article 8 de la loi relative à internet, qui n'autorise le blocage de l'accès et la suppression de contenus que pour certaines infractions pénales, son article 8/A autorise le blocage de l'accès et la suppression de contenus pour toute infraction pénale ou atteinte à l'ordre public. En particulier, le terrorisme et les infractions liées à ce dernier peuvent relever du champ d'application de l'article 8/A, car les notions générales de sécurité nationale, d'ordre public et de prévention de la criminalité confèrent un pouvoir discrétionnaire important en matière de réglementation d'internet.

La BTK ne tient pas de statistiques sur le nombre de sites web bloqués pour des motifs liés au terrorisme et ne publie pas de données exhaustives sur ce sujet. Néanmoins, des communiqués de presse ont indiqué à plusieurs reprises que des contenus liés au terrorisme avaient déjà fait l'objet de mesures de blocage en vertu de l'article 8/A de la loi relative à internet[509].

Il convient de noter dans ce contexte que la lutte contre le terrorisme demeure l'une des priorités les plus immédiates pour la Türkiye et que le pays s'emploie à combattre activement les contenus à caractère terroriste en ligne. Bien que la loi relative à internet, principal cadre juridique turc pour la régulation d'internet, ne mentionne pas explicitement les contenus à caractère terroriste, des mesures continuent d'être prises à l'encontre de ces derniers. L'article 8/A de la loi tient lieu de disposition générale permettant une intervention et un blocage de l'accès à un large éventail de contenus illicites.

On peut ainsi considérer que l'article 8/A de la loi relative à internet sert de disposition « fourre-tout » pour contrôler les contenus en ligne, quels qu'ils soient. Dans les faits, cela signifie notamment que le délai très bref de quatre heures applicable au retrait vise en réalité l'ensemble des contenus à caractère terroriste provenant de toutes les plateformes, y compris les réseaux sociaux.

[509] Voir « *6 bin 500 habere engel 5 bin habere sansür! » (« 6 500 articles d'actualité bloqués, 5 000 supprimés ! »)*, *Cumhuriyet*, 16 octobre 2023 ; A. Uludag, « *AYM kararına rağmen engellenen içeriklerin sayısı artıyor » (« Malgré la décision de la Cour constitutionnelle, le nombre de contenus bloqués est en hausse »)*, *Deutsche Welle*, 4 août 2023.

5. La lutte contre les propos diffamatoires, le discours de haine et l'incitation à la violence

5.1. Les normes applicables au niveau de l'Union européenne

Dr Mark D. Cole, directeur des affaires académiques de l'Institut européen du droit des médias (EMR) et professeur en droit des médias et des télécommunications à l'université du Luxembourg

De nombreux facteurs, et notamment une succession de crises économiques et sociales, la pandémie de COVID-19, les enjeux migratoires et la numérisation croissante, ont contribué à la prolifération sur internet de propos à caractère diffamatoire et de discours d'incitation à la haine et à la violence[510]. Les mesures réglementaires récemment adoptées par l'Union européenne pour lutter contre ce type de discours sont en constante évolution.

Afin de favoriser une application harmonisée de la réglementation, à l'instar de ce qui a été fait en matière de contenus à caractère terroriste (voir plus haut, le point 4.1), l'Union européenne a encouragé ses États membres à harmoniser leur définition des propos qui sont pénalement répréhensibles et, par conséquent, illicites. Par exemple, les discours de haine illicites sont définis dans une décision-cadre relative à la lutte contre certaines formes et manifestations de racisme et de xénophobie au moyen du droit pénal[511] comme une incitation publique à la violence ou à la haine fondée sur certaines caractéristiques, notamment la race, la couleur de peau, la religion, l'ascendance et l'origine nationale ou ethnique[512]. Bien que cette décision-cadre sur la lutte contre le racisme et la xénophobie concerne uniquement les discours à caractère raciste et xénophobe, la majorité des États membres ont étendu leur législation nationale afin de sanctionner les discours de haine fondés sur d'autres motifs, tels que l'orientation sexuelle, l'identité de genre et le handicap. Cette approche transparaît également dans la Directive SMA consolidée qui, à l'article 6 de manière générale et à l'article 9(1)*c*)ii) pour les communications commerciales, fait référence à une liste plus étendue de motifs de discrimination illicites, parmi lesquels figurent le sexe, l'origine raciale ou ethnique, la nationalité, la religion ou les convictions, le handicap, l'âge ou l'orientation sexuelle, et s'apparente ainsi à l'article 21 de la Charte

[510] Voir F. Faloppa et autres, *Étude sur la prévention et la lutte contre le discours de haine en temps de crise*, Conseil de l'Europe, CDADI, Strasbourg, novembre 2023.
[511] Union européenne, Décision-cadre 2008/913/JAI du Conseil du 28 novembre 2008 sur la lutte contre certaines formes et manifestations de racisme et de xénophobie au moyen du droit pénal, *JOUE* L 328/55, 6 décembre 2008.
[512] L'Union européenne a également adopté plusieurs directives qui interdisent la discrimination fondée sur divers motifs, tels que la race et l'origine ethnique. Compte tenu de l'objet du présent rapport *IRIS*, ces directives ne sont pas examinées.

des droits fondamentaux de l'Union européenne, auquel il est clairement fait référence à l'article 6 (1)[513].

Confrontée à la fragmentation du droit matériel, d'une part, et à la forte augmentation des discours et des infractions à caractère haineux en Europe, d'autre part[514], la Commission européenne a adopté en 2021 une communication qui souligne la nécessité d'une décision du Conseil visant à compléter l'actuelle liste des « infractions pénales de l'Union » mentionnée à l'article 83(1) du TFUE[515] afin d'y faire figurer les discours et les infractions à caractère haineux[516]. Toutefois, comme cette extension de la liste n'a pas encore été officiellement finalisée, le Parlement européen et le Conseil ne disposent d'aucune base juridique pour adopter une réglementation fixant des exigences minimales pour la définition des infractions pénales relatives aux discours de haine et des sanctions correspondantes encourues[517]. Indépendamment de ces limites, la directive sur la lutte contre la violence à l'égard des femmes et la violence domestique[518] érige en infraction pénale les discours de haine à l'égard des femmes ainsi que d'autres formes de

[513] Dans la mesure où les dispositions de la Charte des droits fondamentaux de l'Union européenne doivent être interprétées de la même manière que celles de la Convention européenne des droits de l'homme, la jurisprudence de la Cour européenne concernant l'article 17 de la Convention précise le seuil minimal européen en matière de droits de l'homme pour les discours de haine pénalement répréhensibles. Ce seuil a été défini au paragraphe 11 de la Recommandation du Comité des ministres du Conseil de l'Europe sur la lutte contre le discours de haine, CM/Rec/(2022)16, qui comprend : *a*) l'incitation publique à commettre un génocide, des actes de violence ou de discrimination ; *b*) les menaces racistes, xénophobes, sexistes et LGBTI-phobes ; *c*) les insultes publiques à caractère raciste, xénophobe, sexiste et LGBTI-phobe dans des conditions telles que celles énoncées spécifiquement pour les insultes en ligne par le Protocole additionnel à la Convention sur la cybercriminalité relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (STE n° 189) ; *d*) la négation, la banalisation et l'apologie publiques du génocide, des crimes contre l'humanité ou des crimes de guerre ; et *e*) la diffusion intentionnelle de matériel contenant de telles expressions de discours de haine (énumérées aux points *a*) à *e*) ci-dessus), y compris des idées fondées sur la supériorité d'une race ou sur la haine raciale.

[514] Pour ce dernier point, voir les rapports annuels de la Commission européenne contre le racisme et l'intolérance (ECRI) de 2019 et 2020 : ECRI, Rapport annuel sur les activités de l'ECRI couvrant la période du 1er janvier au 31 décembre 2019, Strasbourg, mars 2020 et ECRI, Rapport annuel sur les activités de l'ECRI couvrant la période du 1er janvier au 31 décembre 2020, Strasbourg, mars 2021. Voir également l'étude commandée par le département thématique Droits des citoyens et des affaires constitutionnelles du Parlement européen, *Hate speech and hate crime in the EU and the evaluation of online content regulation approaches* (Discours et crimes de haine dans l'Union européenne et évaluation des stratégies pour la réglementation des contenus en ligne), juillet 2020, en anglais.

[515] Les domaines de criminalité énumérés à l'article 83(1) du TFUE sont les suivants : le terrorisme, la traite des êtres humains et l'exploitation sexuelle des femmes et des enfants, le trafic illicite de drogues, le trafic illicite d'armes, le blanchiment d'argent, la corruption, la contrefaçon de moyens de paiement, la criminalité informatique et la criminalité organisée.

[516] Commission européenne, Communication de la Commission au Parlement européen et au Conseil, Une Europe plus inclusive et plus protectrice : extension de la liste des infractions de l'UE aux discours de haine et aux crimes de haine, COM(2021) 777 final, 2021.

[517] Conformément à l'article 83(1) du TFUE, le Parlement européen et le Conseil peuvent, au moyen de directives adoptées conformément à la procédure législative ordinaire, établir des règles minimales relatives à la définition des infractions pénales et des sanctions dans les domaines de la criminalité particulièrement grave revêtant une dimension transfrontière résultant du caractère ou des incidences de ces infractions ou d'un besoin particulier de les combattre sur des bases communes. En ce qui concerne l'état d'avancement des propositions visant à étendre la liste des infractions pénales de l'UE à toutes les formes de délits et discours de haine, voir le site web dédié du Parlement européen consacré au programme train législatif, disponible en anglais ici.

[518] Directive (UE) 2024/1385 , 24 mai 2024.

cyberviolence fondée sur le genre, au motif que la violence à l'égard des femmes porte atteinte au principe fondamental de l'UE d'égalité entre les femmes et les hommes, en invoquant comme bases juridiques les articles 82(2) et 83(1) du TFUE.

Parallèlement, plusieurs stratégies ont fait leur apparition sous forme de droit primaire, dérivé et non contraignant de l'UE afin de lutter contre les discours de haine en précisant les éléments constitutifs d'un tel discours[519]. La lutte contre les discours d'incitation à la haine en ligne a été renforcée puisqu'ils sont désormais jugés contraires aux valeurs fondamentales de l'UE telles qu'énoncées à l'article 2 du Traité sur l'Union européenne (TUE)[520]. Parmi les nombreuses initiatives et campagnes de sensibilisation visant à lutter contre la haine en ligne et hors ligne[521], le présent chapitre met l'accent sur la diffusion de ces contenus sur les plateformes en ligne. Ces plateformes comportent en effet des risques particuliers en raison de leurs systèmes algorithmiques qui amplifient la diffusion de certains types de discours et peuvent ainsi avoir de graves répercussions négatives sur les potentielles victimes.

Il en va de même pour les propos diffamatoires, dont l'effet est similaire à celui des discours de haine, puisque la diffusion et la réplication instantanées de ces contenus en ligne exposent leurs victimes à des insultes et à d'autres risques de préjudice. Néanmoins, contrairement aux discours de haine, qui peuvent être soumis à des restrictions en vertu de l'article 10 de la Convention européenne[522] ou de l'article 11 de la Charte des droits fondamentaux de l'Union européenne, la question des propos diffamatoires n'est pas aussi clairement définie. En effet, la diffamation n'est pas toujours explicitement contraire à la loi, et les propos insultants peuvent toujours bénéficier de la protection de la Convention européenne des droits de l'homme et de la Charte des droits fondamentaux de l'Union européenne[523]. Le caractère juridiquement illicite des propos diffamatoires est apprécié selon la législation nationale. L'application des normes impose en général une évaluation de l'exactitude des faits, ainsi qu'une prise en compte du contexte, de l'intérêt général et de l'intention. Ces mêmes difficultés se posent également pour les discours qui incitent à la violence.

---

[519] Voir E. Nave et L. Lane, « *Countering Online Hate Speech: How Does Human Rights Due Diligence Impact Terms of Service* », *Computer Law & Security Review* 51, 2023, 105884. En termes de mesures politiques, la Commission européenne a créé en 2016 un groupe de haut niveau sur la lutte contre le discours de haine et les crimes de haine qui a notamment publié des lignes directrices sur la coopération entre les autorités répressives et les organisations de la société civile, et qui sert à faciliter l'échange de bonnes pratiques (voir Commission européenne, *Informal Commission Expert Group "High Level Group on Combating Hate Speech and Hate Crime", Terms of Reference*, en anglais, 2016).

[520] Voir Commission européenne, Communication conjointe au Parlement européen et au Conseil, « Pas de place pour la haine: une Europe unie contre toute forme de haine », JOIN(2023) 51 final, 2023 (en réponse aux commentaires publiés en ligne sur l'attaque du Hamas contre Israël le 7 octobre 2023).

[521] Pour une vue d'ensemble des axes de travail et des ressources au niveau de l'UE, voir le site web dédié de la Commission « *Combating Hate Speech and Hate Crime* », disponible en anglais sur : https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/combating-hate-speech-and-hate-crime_en.

[522] Soit pour abus de droit (article 17 de la CEDH) soit pour atteinte aux valeurs fondamentales de la Convention (les restrictions étant jugées nécessaires au titre de l'article 10(2) de la CEDH). Pour une brève présentation de la jurisprudence de la Cour européenne des droits de l'homme en matière de discours de haine, voir CEDH, Unité de la presse, « Fiche thématique – Discours de haine », 23 novembre 2023.

[523] *Handyside c. Royaume-Uni*, requête n° 5493/72 (Cour européenne des droits de l'homme, 7 décembre 1976).

Malgré les difficultés inhérentes au fait de déterminer la nature d'un discours donné, le DSA instaure au niveau de l'UE un cadre de responsabilités à plusieurs niveaux applicable aux plateformes en ligne. Le DSA impose notamment aux fournisseurs de très grandes plateformes en ligne (VLOP) et de très grands moteurs de recherche en ligne (VLOSE) de prévenir et de limiter les risques associés à la diffusion de contenus illicites, conformément aux obligations spécifiques qui leur incombent en vertu de la section 5 du chapitre III du DSA. Cette obligation supplémentaire s'ajoute à l'exigence générale imposée à l'ensemble des fournisseurs de services d'hébergement de mettre en place un système de notification et d'action, et de procéder dans les meilleurs délais au retrait des contenus illicites qui leur sont signalés. Ils doivent par ailleurs faire preuve de transparence au sujet du fonctionnement de leurs algorithmes et systèmes de recommandation, et traiter les risques liés à l'amplification des contenus illicites par ces systèmes.

S'agissant des discours de haine, ces obligations, y compris celles relatives à une action rapide, découlent du Code de conduite sur la lutte contre les discours haineux illégaux en ligne[524], lequel se concentre sur les discours illicites d'incitation à la haine tels que définis dans la décision-cadre précitée. Ce code de conduite était à l'origine un accord volontaire conclu en 2016 entre la Commission européenne et, dans un premier temps, *Facebook*, *Microsoft*, *Twitter* et *YouTube*, auxquels se sont joints par la suite d'autres fournisseurs de plateformes[525]. Le code de conduite sur la lutte contre les discours de haine illégaux en ligne visait à lutter contre la propagation en ligne de ces discours, dans le respect des législations européenne et nationales, et *notamment* en accélérant le contrôle et la suppression de ce type de discours, et en fixant un délai de réaction de 24 heures pour la plupart des notifications, ainsi qu'en encourageant la transparence et la coopération entre les plateformes et les autorités de l'Union européenne. Le 20 janvier 2025, le code de conduite a été révisé et intégré dans l'architecture de corégulation du DSA sous l'appellation de « Code de conduite sur la lutte contre les discours de haine illégaux en ligne+ »[526]. En mettant l'accent sur la prévention et l'anticipation des menaces, ce code de conduite renforce et améliore la manière dont les plateformes luttent contre les discours illicites afin de respecter les législations nationales et européennes, et contribue à une application effective du DSA. Le respect du Code de conduite sur la lutte contre les discours de haine illégaux en ligne + pourrait constituer une mesure pertinente d'atténuation des risques pour les signataires qui répondent aux critères applicables aux fournisseurs de très grandes plateformes en ligne (VLOP) et de très grands moteurs de recherche en ligne (VLOSE).

Avant l'intégration du code dans le DSA, la Commission européenne a engagé une procédure officielle à l'encontre de X en vertu de l'article 66(1) du DSA (voir ci-dessus, point 4.1). Cette procédure faisait état d'une violation des articles 34 et 35 du DSA en matière d'évaluation et d'atténuation des risques, du fait d'une évaluation insuffisante par X de la conception et du fonctionnement de son dispositif « *Freedom of Speech Not Freedom of*

[524] Code de conduite sur la lutte contre les discours de haine illégaux en ligne, 30 juin 2016 en anglais.
[525] Voir le site web dédié de la Commission, disponible ici.
[526] Code de conduite sur la lutte contre les discours de haine illégaux en ligne +, en anglais, 20 janvier 2025. Le code se compose de cinq engagements et de deux annexes. Les engagements portent, entre autres, sur l'examen de la plupart des signalements de discours de haine dans un délai de 24 heures, conformément aux articles 16 et 22 du DSA, par des « rapporteurs de contrôle » spécialisés dans les discours de haine.

Reach » (liberté d'expression et non liberté d'accès) dans l'Union européenne[527]. En 2023, X a notamment réduit ses effectifs chargés de la modération des contenus[528], s'est désengagé du Code de bonnes pratiques contre la désinformation[529] et a dissous son groupe consultatif consacré aux discours de haine[530]. La Commission européenne a notamment estimé que

> *les dimensions régionales et linguistiques des politiques de X concernant les « entités violentes et haineuses », les « discours violents », les « contenus incitant à la haine » et les « médias sensibles » au sein de l'Union européenne, ainsi que les moyens de modération des contenus et autres dispositifs mis en place par TIUC et X Holdings Corp. pour mettre en œuvre ces politiques, semblaient insuffisants pour réduire efficacement et de manière cohérente les risques de diffusion de contenus illicites*[531].

Une analyse complémentaire des données communiquées en novembre 2023 à la base de données transparente du DSA a révélé que la modération des contenus de X est effectivement limitée par rapport à d'autres plateformes de réseaux sociaux[532]. En janvier 2025, la Commission européenne a émis une ordonnance conservatoire dans le cadre de l'enquête en cours, en exigeant de X que des informations supplémentaires lui soient transmises au moyen de mesures techniques d'enquête relatives au système de recommandation de la plateforme[533]. La Commission européenne a demandé l'accès à certaines interfaces de programmation d'applications (API) commerciales, et en particulier aux interfaces techniques des contenus de X qui permettent de vérifier directement la modération des contenus et la viralité des comptes. La durée de l'enquête témoigne de la complexité de l'évaluation des risques systémiques et de leur atténuation au regard de l'autorité de contrôle. En septembre 2025, X faisait toujours l'objet d'une enquête de la Commission européenne sur ses pratiques de modération des contenus et ses obligations de transparence. Si la Commission constate que X ne respecte pas ses obligations au titre du DSA, elle peut alors lui infliger des sanctions (voir le point 2.2.2.2).

S'agissant des obligations de notification et d'action prévues par le DSA, certaines difficultés déjà rencontrées dans le cadre de la Directive sur le commerce électronique risquent de persister, notamment la question du retrait et du maintien du retrait en cas de violations répétées du même type. À l'instar des dispositions de la Directive sur le commerce électronique, le DSA n'impose aucune obligation générale de surveillance aux fournisseurs de services d'hébergement. Cependant, les parties qui estiment être victimes

---

[527] Décision de la Commission du 18 décembre 2023 relative à l'ouverture d'une procédure en vertu de l'article 66(1) du règlement (UE) 2022/2065, COM(2023) 9137 final, point 9, 2023.

[528] Reuters, *« Twitter further Cuts Staff Overseeing Global Content Moderation, Bloomberg Reports »*, *Reuters*, 7 janvier 2023.

[529] Voir la publication de Thierry Breton sur X « *Twitter leaves EU voluntary Code of Practice against disinformation* » du 26 mai 2023, en anglais.

[530] Associated Press, *« Musk's Twitter Has Dissolved its Trust and Safety Council »*, *npr*, 12 décembre 2022.

[531] *Ibid*., point 10. TIUC désigne *Twitter International Unlimited Company*, le principal établissement du fournisseur de X dans l'UE. *X Holdings Corp*. est la société qui contrôle le groupe de personnes morales auquel appartient TIUC.

[532] R. Kaushal et autres, « *Automated Transparency: A Legal and Empirical Analysis of the Digital Services Act Transparency Database* », *FAccT '24: Compte rendu de la conférence ACM 2024 sur l'équité, la responsabilité et la transparence*, ACM, 2024, pp. 1121-1132.

[533] Commission européenne, *« Commission Addresses Additional Investigatory Measures to X in the ongoing Proceedings under the Digital Services Act »*, communiqué de presse, 17 janvier 2025, en anglais.

d'une violation de leurs droits en raison de contenus hébergés par les fournisseurs ont toutes les raisons de vouloir mettre un terme à cette infraction et empêcher la poursuite ou la répétition de la diffusion de contenus illicites. Elles peuvent donc demander au juge de rendre une ordonnance visant à garantir que le contenu concerné soit retiré sans délai par les fournisseurs et, par la même occasion, qu'il soit définitivement supprimé et ne réapparaisse plus[534]. Cette suppression définitive nécessite l'intervention du fournisseur de services d'hébergement, par exemple au moyen d'une modération ou d'un filtrage des contenus[535].

Alors que la question des obligations spécifiques en matière de filtrage a également fait l'objet d'un vaste débat en matière de droit d'auteur et de droits voisins, notamment en ce qui concerne l'article 17 de la directive relative au droit d'auteur dans le marché unique numérique[536/537], la notion de retrait et de suppression définitive suscite encore de nombreuses interrogations lorsqu'il s'agit de contenus à caractère diffamatoire ou calomnieux ; en effet, le caractère illicite d'un contenu n'est pas nécessairement imputable à l'utilisation de certains termes ou expressions (par exemple ceux considérés comme insultants), mais au fait que la déclaration dans son ensemble puisse être considérée comme diffamatoire[538]. Pour garantir une protection effective des droits de la partie lésée, il faudrait que l'injonction prononcée par un tribunal s'applique non seulement aux termes utilisés dans le contenu jugé illicite, mais également aux « informations dont le contenu, tout en véhiculant essentiellement le même message, est formulé de manière légèrement différente, en raison du choix des mots ou de leur combinaison », comme l'a souligné la Cour de justice de l'Union européenne (CJUE) dans une affaire dont elle avait été saisie par une juridiction autrichienne[539]. La CJUE a considéré que le concept d'« informations ayant une signification équivalente » était admissible dans le cadre d'une injonction émise par une juridiction nationale, à condition qu'il ne nécessite pas une évaluation indépendante par le fournisseur et une obligation de blocage généralisé de ce type d'informations[540]. Cette conclusion reconnaît que les fournisseurs, en raison de la quantité d'informations stockées, recourent généralement à des outils et technologies de recherche automatisés lors de la

[534] Voir, au sujet des droits de propriété intellectuelle : C-324/09 *L'Oréal SA et autres c. eBay International et autres* (CJUE, 12 juillet 2011) ECLI:EU:C:2011:474 ; et C-70/10 *Scarlet Extended SA c. SABAM* (CJUE, 24 novembre 2011) ECLI:EU:C:2011:771.

[535] Voir T. Enarsson, « *Navigating Hate Speech and Content Moderation under the DSA : Insights from ECtHR case law* », *Information & Communications Technology Law* 33(3), 2024, pp. 384-401.

[536] Directive (UE) 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE, *JOUE* L 130/92, 17 mai 2019.

[537] Voir, par exemple, C. Geiger et BJ. Jütte, « *Platform Liability under Article 17 of the Copyright in the Digital Single Market Directive, Automated Filtering and Fundamental Rights : An Impossible Match* », *GRUR International* 70(6), 2021, pp. 517-543 ; N. Rauer et A. Bibi, « *Grundrechtskonformität des Art. 17 DSM-RL – Ende gut alles gut?* », *Zeitschrift für Urheber- und Medienrecht*, 2022, pp. 585-672.

[538] *C-18/18 Glawischnig-Piesczek c. Facebook* (CJUE, 3 octobre 2019) ECLI:EU:C:2019:821, point 40.

[539] Ibid., point 41.

[540] Ibid., point 46 et suivants.

modération et du filtrage des contenus[541], qui ne permettent toutefois pas de procéder à un contrôle préalable de chaque contenu publié.

5.2. L'exemple de l'Irlande

Dr Roderick Flynn, professeur agrégé, directeur du département des sciences de la communication, Faculté des sciences de la communication, université de Dublin

5.2.1. Le cadre législatif national applicable aux plateformes

L'adoption de la dernière version (2018) de la Directive SMA et du DSA en 2022, ainsi que l'obligation de transposer ou d'intégrer ces deux textes dans le droit irlandais, ont donné lieu à une série de modifications importantes de la loi irlandaise relative à la radiodiffusion de 2009[542]. Ces modifications portent sur la réglementation des discours de haine et l'incitation à la violence en ligne, mais n'ont que peu de rapport avec la diffamation, qui reste réglementée par la loi irlandaise relative à la diffamation de 2009[543].

L'une des conséquences directes de la transposition et de l'intégration de la Directive SMA et du DSA a été la création d'une nouvelle autorité de régulation des médias, la *Coimisiún na Meán* (CnaM). La CnaM a remplacé l'Autorité irlandaise de la radiodiffusion (*Broadcasting Authority of Ireland* – BAI), dont le domaine de compétence se limitait principalement aux radiodiffuseurs et aux services à la demande. L'extension significative de la réglementation aux contenus en ligne, induite par la Directive SMA et le DSA, a exigé la mise en place de nouvelles structures de régulation, dont l'expression institutionnelle s'est traduite par la création de la CnaM le 15 mars 2023. L'ensemble des fonctions précédemment dévolues à la BAI ont été transférées à la CnaM, ainsi que les obligations réglementaires supplémentaires découlant de la Directive SMA et du DSA. Cette réorganisation a conduit l'autorité de régulation à s'installer dans de nouveaux locaux mieux adaptés à la nouvelle taille de l'organisation, dont les effectifs sont passés de moins de 50 à plus de 350 personnes. La CnaM est donc désormais chargée de veiller à ce que les plateformes en ligne utilisent des mécanismes permettant de protéger efficacement leurs utilisateurs contre les contenus préjudiciables, notamment les discours d'incitation à la haine et à la violence.

L'intégration des dispositions de la Directive SMA et du DSA dans le droit irlandais a été grandement facilitée par deux textes législatifs nationaux : la loi relative à la sécurité en ligne et à la régulation des médias (*Online Safety and Media Regulation Act* – OSMR)[544]

---

[541] Voir *ibid*., point 46. Pour un commentaire à ce sujet, voir M. Rojszczak, « *Online Content Filtering in EU Law – A Coherent Framework or Jigsaw Puzzle?* », *Computer Law & Security Review* 47, 2022, 105739.

[542] *Loi relative à la radiodiffusion de 2009.*

[543] *Loi relative à la diffamation de 2009.*

[544] *Loi relative à la sécurité en ligne et à la régulation des médias de 2022.*

de 2022 et la loi irlandaise relative aux services numériques (*Irish Digital Services Act*)[545] de 2024. Ces deux textes ont été incorporés à la loi relative à la radiodiffusion de 2009 déjà en vigueur. À ce jour, aucune version consolidée officielle de la législation n'a été publiée, malgré le fait que l'*Irish Law Society* (association des juristes irlandais) dispose d'une version en ligne qui englobe tous les ajouts apportés depuis 2009 à la « loi principale », c'est-à-dire le texte original de la loi relative à la radiodiffusion de 2009)[546].

En février 2024, la Cour de justice de l'Union européenne a infligé une amende de 2 500 000 EUR à l'Irlande au motif qu'elle n'avait pas pleinement transposé la Directive SMA[547]. La Cour a en effet estimé que, même si l'OSMR comprenait des dispositions permettant l'adoption (obligatoire) de codes de conduite applicables aux plateformes de partage de vidéos, ces codes n'avaient début 2024 toujours pas été élaborés. Ce problème a finalement été résolu en octobre 2024, lorsque la CnaM a publié le code de sécurité en ligne[548]. Ce document présenté en détail ci-dessous définit brièvement en quoi consiste un contenu préjudiciable et mentionne spécifiquement l'incitation à la violence ou à la haine à l'encontre d'un groupe de personnes ou d'un membre d'un groupe pour l'un des motifs visés à l'article 21 de la Charte des droits fondamentaux de l'Union européenne, à savoir le sexe, les convictions politiques, le handicap, l'appartenance à une minorité ethnique, la religion et la race. Il précise également les obligations qui incombent aux fournisseurs de services de plateformes de partage de vidéos au regard des contenus qu'ils hébergent. Le code impose par ailleurs aux fournisseurs de ces plateformes « d'inclure, dans les conditions générales et les obligations associées au service, des restrictions interdisant aux utilisateurs :

- de télécharger ou de partager des contenus vidéo soumis à des restrictions, au sens du présent code, et
- de télécharger ou de partager des contenus générés par les utilisateurs et soumis à des restrictions, selon la définition du présent code »[549].

Le code de sécurité en ligne prévoit également que lorsque les utilisateurs ont régulièrement enfreint ces conditions générales, le fournisseur de la plateforme est tenu de suspendre leur compte[550]. Conformément au code, la CnaM a pour mission d'identifier les services de plateformes de partage de vidéos qui relèvent de la compétence irlandaise et de les désigner comme tels, ce qui s'est produit pour la première fois en décembre 2023 et a permis de constater que la plupart des principaux services de plateformes de partage de vidéos actifs en Europe étaient concernés[551].

---

[545] Loi relative aux services numériques de 2024.

[546] Voir Commission de réforme législative, Loi relative à la radiodiffusion de 2009 (dernière mise à jour le 1er juin 2025).

[547] S. Collins, « *Ireland fined €2.5m by EU courts for delays to online safety law* », *Irish Independent*, 29 février 2024.

[548] *Coimisiún na Meán*, Code de sécurité en ligne, octobre 2024.

[549] *Ibid*., article 12.1.

[550] *Ibid*., article 12.6.

[551] Compte tenu du fait qu'un nombre important de plateformes et d'entreprises technologiques ont établi leur siège européen en Irlande, la CnaM a désigné en décembre 2023 dix services de plateformes de partage de vidéos comme relevant du Code de sécurité en ligne, qui n'avait pas encore été publié à cette date. Il s'agissait de *Facebook*, *Instagram*, *YouTube*, *Udemy*, *TikTok*, *LinkedIn*, *X/Twitter*, *Pinterest*, *Tumblr* et *Reddit*.

Les services *Reddit* et *Tumblr* ont contesté leur désignation devant la Haute Cour irlandaise en 2024. *Reddit* soutenait qu'en sa qualité de société américaine, la plateforme ne devait pas relever de la compétence de l'État irlandais, tandis que *Tumblr* affirmait que la quantité de contenus vidéo sur sa plateforme était relativement faible et ne répondait donc pas aux critères requis pour lui attribuer le statut de plateforme de partage de vidéos. En juin 2024, la Haute Cour irlandaise a catégoriquement rejeté les deux recours, et a déclaré que la CnaM avait correctement désigné les deux services en question[552]. Cependant, en mai 2025, la CnaM a annulé la désignation du service *Reddit*, après le transfert par la société mère de ce dernier de son siège social européen aux Pays-Bas[553].

5.2.2. Les dispositions spécifiques applicables aux propos diffamatoires, au discours de haine et à l'incitation à la violence

Le présent rapport n'aborde que brièvement la question de la diffamation, dans la mesure où le code de sécurité en ligne ne comporte aucune référence explicite à la diffamation écrite ou verbale. Cela ne signifie pas pour autant que les discours de haine ou l'incitation à la violence ne peuvent pas également constituer des actes de diffamation. Cependant, dans la pratique, la diffamation en ligne est considérée sur le plan juridique de la même manière que la diffamation contenue dans des publications imprimées ou des contenus audiovisuels. À ce titre, la diffamation en ligne relève des dispositions de la loi de 2009 relative à la diffamation. Il a toutefois été observé que la diffamation en ligne soulève des difficultés particulières, notamment en ce qui concerne l'identification de la personne responsable de la publication de contenus diffamatoires sur une plateforme en ligne. Il convient de mentionner à cet égard les dispositions du projet de loi relative à la diffamation de 2024, qui a été adopté par la chambre basse du Parlement irlandais et qui est actuellement (octobre 2025) en cours d'examen par la commission de la chambre haute du Parlement[554]. Compte tenu de la difficulté potentielle d'identifier les personnes qui publient des propos diffamatoires en ligne, la partie 9, article 22, du projet de loi propose de modifier la loi relative à la diffamation de 2009 afin de permettre aux particuliers de solliciter auprès du tribunal itinérant (*Circuit Court*) une ordonnance à l'encontre de la plateforme en ligne concernée (« fournisseur de services d'information ») exigeant que cette plateforme communique l'identité de la personne à l'origine de la publication du contenu diffamatoire. Les demandeurs d'une telle divulgation d'identité doivent convaincre le tribunal itinérant

[552] A. O'Faolain, « *High Court dismisses Reddit and Tumblr challenges over new online safety code* », *Irish Times*, 20 juin 2024.
[553] *Coimisiún na Meán*, *Revocation of Designation Notice*, 22 mai 2025.
[554] Chambre de l'*Oireachtas*, projet de loi relative à la diffamation de 2024 (modification), projet de loi n° 67 de 2024.

de l'existence du délit de diffamation et, en outre, de la probabilité de succès d'une action en justice pour diffamation[555].

S'agissant des contenus illicites et préjudiciables, au sens de l'article 7(2)(*d*) de la loi relative à la radiodiffusion de 2009 (telle que modifiée), la CnaM doit s'efforcer de veiller à ce que ses dispositions réglementaires « traitent les programmes, les contenus générés par les utilisateurs et autres contenus préjudiciables ou illicites ». L'article 139K(3) de la loi relative à la radiodiffusion impose spécifiquement à la CnaM de créer un code de sécurité en ligne applicable aux fournisseurs de services de plateformes de partage de vidéos, comme évoqué ci-dessus.

L'article 139A de la loi relative à la radiodiffusion de 2009 (telle que modifiée) définit les catégories de contenus en ligne préjudiciables auxquels s'applique le code de sécurité en ligne. L'article 139A(2)(*a*) renvoie à l'annexe 3 de la législation qui énonce les « catégories de contenus en ligne spécifiques à certaines infractions ». L'article 4 de l'annexe 3 définit les discours incitant à la haine et à la violence comme « des contenus en ligne au moyen desquels une personne publie ou diffuse des documents écrits, ou un enregistrement d'images ou de sons, qui sont contraires à l'article 2(1) de la loi relative à l'interdiction de l'incitation à la haine de 1989 (documents, images ou sons qui ont un caractère menaçant, injurieux ou insultant et qui ont pour objectif ou, compte tenu de l'ensemble des circonstances, sont de nature à susciter des sentiments de haine) ». En vertu de l'article 5 de l'annexe 3, les contenus préjudiciables englobent également les programmes diffusés qui sont « contraires à l'article 3(1) de la loi de 1989 relative à l'interdiction de l'incitation à la haine (images ou sons de nature menaçante, injurieuse ou insultante dont la diffusion est destinée ou, compte tenu de toutes les circonstances, est susceptible d'attiser la haine) ».

Le recours à la loi de 1989 relative à l'interdiction de l'incitation à la haine[556] peut s'avérer problématique dans la mesure où, comme nous le verrons ci-dessous, cette loi est jugée imparfaite, même si elle interdit en effet l'incitation à la haine à l'encontre d'un groupe de personnes en raison de leur « race, couleur de peau, nationalité, religion, origine ethnique ou nationale, appartenance à la communauté des gens du voyage ou orientation sexuelle ».

Bien que cette loi de 1989 érige en infraction pénale l'incitation à la haine, elle est principalement considérée comme une disposition relative aux discours de haine. L'incitation englobe la publication, la diffusion et la préparation de documents, et l'application de la loi de 1989 ne se limite pas aux comportements hors ligne, puisqu'elle s'étend aux propos tenus, aux comportements ou aux documents affichés « en tout lieu autre qu'à l'intérieur d'une résidence privée »[557].

---

[555] Il convient également de rappeler qu'en mars 2022, quatre députés irlandais ont parrainé le « projet de loi sur la responsabilité des plateformes de médias sociaux (modification relative à la diffamation) », qui aurait permis de prononcer des jugements pour diffamation à l'encontre des plateformes de médias sociaux sur lesquelles des propos diffamatoires avaient été tenus, dans les situations où la plateforme en question n'était pas en mesure de révéler l'identité de la personne ayant tenu ces propos. Toutefois, en tant que projet de loi d'initiative parlementaire, le texte proposé n'a pas obtenu le soutien du gouvernement et n'a pas été adopté par le Parlement irlandais.

[556] Loi relative à l'interdiction de l'incitation à la haine de 1989.

[557] *Ibid.*, article 2(1)(*b*)(i).

La loi de 1989 relative à l'interdiction de l'incitation à la haine est toutefois jugée insuffisante : un rapport publié en 2016 par la commission pour la réforme législative sur les communications préjudiciables et la sécurité numérique souligne que « la loi de 1989 a fait l'objet de nombreuses critiques en raison de son inefficacité apparente, comme en témoigne le nombre limité de poursuites engagées au titre de cette loi »[558]. De même, dans ses observations sur l'Irlande, le Comité des Nations Unies pour l'élimination de la discrimination raciale s'est déclaré préoccupé par le fait que la loi de 1989 relative à l'interdiction de l'incitation à la haine s'est avérée inefficace dans la lutte contre les discours de haine à caractère raciste, en particulier les discours de haine à caractère raciste en ligne[559]. Certains universitaires ont déclaré que la loi de 1989 était « manifestement inadaptée à la lutte contre les délits motivés par la haine » et qu'elle devait être réformée afin de tenir compte du contexte particulier des délits motivés par la haine dans le cyberespace[560].

Afin de remédier à ces lacunes, le Gouvernement de l'époque a décidé en 2021 de remplacer la loi de 1989 relative à l'interdiction de l'incitation à la haine par une législation instaurant de nouvelles infractions aggravées, notamment un nouveau délit d'incitation. Le projet de loi avait été publié en avril 2021 et promettait d'ériger en infraction pénale spécifique le fait de commettre une infraction motivée par la haine sur la base de la couleur de peau, de l'orientation sexuelle ou du genre d'une personne, y compris son expression ou son identité de genre. Parmi les autres « caractéristiques protégées » figuraient la race, la nationalité, la religion, l'origine ethnique et nationale de la victime, ainsi que toute forme de handicap[561]. Une version révisée du projet de loi avait été publiée en octobre 2022 sous l'intitulé « *Criminal Justice (Incitement to Violence or Hatred and Hate Offences) Bill* » (projet de loi relative à la justice pénale (incitation à la violence ou à la haine et infractions motivées par la haine))[562].

Cette nouvelle législation visait à ériger en infraction pénale toute communication ou tout comportement intentionnel ou imprudent susceptible d'inciter à la violence ou à la haine à l'encontre d'une ou de plusieurs personnes en raison de leur appartenance à l'une des catégories protégées énumérées ci-dessus. Elle définissait également de nouvelles formes aggravées de certaines infractions pénales existantes, lorsque celles-ci étaient motivées par la haine à l'encontre d'une caractéristique protégée.

Malgré les controverses suscitées par le texte, la nouvelle législation a été approuvée en 2023 par la chambre basse du Parlement[563]. Elle a toutefois été bloquée à la

---

[558] Commission de réforme législative, « *Harmful Communications and Digital Safety* », Rapport LRC 116-2016, Dublin 2016.

[559] Comité pour l'élimination de la discrimination raciale, « Observations finales concernant le rapport de l'Irlande valant cinquième à neuvième rapports périodiques », UN, CERD/C/IRL/CO/5-9, Genève, 23 janvier 2020.

[560] A. Haynes et J. Schweppes, « *Lifecycle of a hate Crime : Country Report for Ireland* », Conseil irlandais des libertés civiles, Dublin, 2017, en anglais.

[561] Ministère de la Justice, des Affaires intérieures et des Migrations, « *New Bill to tackle hate crime and hate speech includes clear provision to protect freedom of expression* », communiqué de presse, 27 octobre 2022, en anglais.

[562] Conseil irlandais des libertés civiles, « *Better engagement with impacted communities paramount as hate crime and extreme hate speech legislation advances at the Oireachtas* », communiqué de presse, 27 octobre 2022 (Dublin: ICCL), en anglais.

[563] *Public Interest Law Alliance*, « *New Bill to tackle hate crime and hate speech is currently before the Seanad* », communiqué de presse, 17 mai 2023.

chambre haute après avoir été critiquée par des députés d'arrière-ban et certains sénateurs. Finalement, en octobre 2024, alors que la législature touchait à sa fin (des élections générales avaient lieu en novembre 2024), le ministre de la Justice de l'époque a décidé que la solution la plus pragmatique était de supprimer toute référence dans la législation à l'incitation à la violence ou à la haine, ainsi qu'à la décision-cadre de l'UE sur la lutte contre le racisme et la xénophobie[564]. En conséquence, la législation de 1989 reste le fondement de la définition des discours de haine et des discours incitant à la violence.

5.2.3. L'application du Code de sécurité en ligne

Lors de la présentation du cadre de sécurité en ligne de l'Irlande, la CnaM a souligné qu'en sa qualité d'autorité de régulation des médias irlandais, elle ne dispose pas du pouvoir de supprimer directement des contenus publiés sur internet. Son rôle consiste davantage à veiller à ce que les plateformes en ligne (et les radiodiffuseurs) qui relèvent de sa compétence mettent en place des mesures visant à empêcher la diffusion de contenus illicites ou préjudiciables. La responsabilité première en matière de lutte contre les contenus préjudiciables, parmi lesquels les discours de haine et les discours incitant à la violence, incombe par conséquent aux plateformes elles-mêmes. La CnaM rappelle que les plateformes ont l'obligation légale d'appliquer leurs propres normes en matière de contenu et de mettre en place des mécanismes permettant aux utilisateurs de signaler tout contenu qui enfreint ces normes.

Dans ce contexte, il revient à la CnaM d'intervenir lorsque ces mécanismes de signalement ne fonctionnent pas comme ils le devraient. La CnaM conseille aux utilisateurs qui rencontrent des difficultés pour signaler un contenu à une plateforme, ou qui estiment qu'une plateforme n'a pas suivi les procédures appropriées pour traiter un signalement, d'en informer la CnaM.

Lorsqu'un utilisateur signale un contenu illicite à une plateforme et qu'il ne parvient pas à obtenir de réponse dans un délai raisonnable et/ou que le contenu n'est pas supprimé, la CnaM invite les utilisateurs à lui signaler ce problème. Elle leur précise toutefois que ses pouvoirs sont limités : « Notre centre de conseil vous remerciera pour votre signalement, vous fournira des conseils et prendra note de vos préoccupations. Nous ne sommes malheureusement pas en mesure de supprimer ce contenu pour vous ».

Dans le meilleur des cas, la CnaM peut transmettre le signalement à son équipe de surveillance des plateformes, « qui s'efforcera de veiller à ce que les plateformes améliorent leurs systèmes ». S'il s'agit d'un problème plus urgent, tel qu'une menace directe en ligne pour la sécurité physique d'une personne, la CnaM conseille aux utilisateurs de contacter directement les services de la police irlandaise. Là encore, la CnaM rappelle que son rôle se limite à enquêter sur les risques systémiques inhérents aux plateformes plutôt que sur des incidents spécifiques.

[564] Décision-cadre 2008/913/JAI du Conseil du 28 novembre 2008 sur la lutte contre certaines formes et manifestations de racisme et de xénophobie au moyen du droit pénal, *JOUE* L 328/55, 6 décembre 2008.

À cet égard, bien qu'il ne soit pas directement lié à l'article 28 *ter* de la Directive SMA, l'article 34 du DSA exige des fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne désignés qu'ils identifient, analysent et évaluent « tout risque systémique [...] découlant de la conception ou du fonctionnement de leurs services et de leurs systèmes connexes, y compris des systèmes algorithmiques, ou de l'utilisation faite de leurs services.».

Les 10 fournisseurs de très grandes plateformes en ligne (VLOP) et de très grands moteurs de recherche en ligne (VLOSE) dont le siège social est situé en Irlande ont soumis à la Commission européenne des évaluations des risques systémiques conformément à l'article 34 du DSA[565]. Celles-ci comportent des parties consacrées au discours de haine. Après examen des premières évaluations communiquées, les 10 plateformes ayant leur siège en Irlande reconnaissent le risque inhérent que leurs services soient utilisés pour diffuser des discours de haine, mais affirment que les mesures internes qu'elles ont mises en place pour atténuer ce risque permettent de le maintenir à un niveau relativement faible. Aucune plateforme n'a en effet intérêt à donner l'impression qu'elle présente un risque significatif en matière de propos illicites.

Compte tenu de la récente mise en place du cadre général de sécurité en ligne et du code qui y est associé, il semble prématuré de procéder à une évaluation objective de son efficacité. Il convient de noter qu'en juin 2025, la CnaM s'est vue contrainte d'émettre une notification d'information réglementaire à l'encontre de la plateforme X au motif que celle-ci n'avait pas fourni suffisamment d'informations pour permettre à la CnaM de déterminer si elle prenait des mesures suffisantes pour se conformer à la partie du code relative à la protection des mineurs[566]. La plateforme X avait en décembre 2024 contesté devant la justice les obligations qui lui étaient imposées par le code de sécurité en ligne, qui constituaient selon elle un « excès de réglementation »[567] qui va au-delà des exigences de l'article 28 *ter* de la Directive SMA. Cette action a été rejetée par la Haute Cour irlandaise en juillet 2025 et, le même mois, X a mis en place de nouvelles mesures de vérification de l'âge afin de répondre aux préoccupations de la CnaM en matière de sécurité des mineurs[568].

Il convient également de noter les conclusions d'une étude publiée par la CnaM en septembre 2025, qui présente en détail l'expérience en ligne des candidats aux élections locales et générales irlandaises de 2024[569]. Bien que les élections locales de juin 2024 aient précédé la publication du code de sécurité en ligne, ce dernier était en vigueur avant les élections générales de novembre 2024. L'étude a révélé que 48 % des candidats aux élections locales ont été victimes de propos choquants, injurieux ou haineux en ligne, de comportements violents ou intimidants en ligne ou encore d'usurpation d'identité en

[565] Base de données Tremau relative au Règlement sur les services numériques. Consultée à l'adresse : https://tremau.com/resources/dsa-database/, 31 octobre 2025. Voir également : *DSA : Risk Assessment & Audit Database*, en anglais.
[566] *Coimisiún na Meán*, « *Coimisiún na Meán issues statutory information notice to X* », communiqué de presse, 17 juin 2025.
[567] Voir F. Gallagher, « *X Loses High Court Challenge Brought against Coimisiún na Meán Safety Code* », *The Irish Times*, 29 juillet 2025, en anglais.
[568] *X Internet UnLtd Company v. Coimisiún na Meán* [2025] IEHC 442
[569] *Coimisiún na Meán*, « *On the digital campaign trail: Election candidates' online experiences in the 2024 elections* », (Dublin: CnaM), en anglais.

ligne[570]. Ce chiffre est passé à 59 % des candidats lors des élections générales de novembre 2024. L'étude précise que 24 % des candidats aux élections locales et 21 % des candidats aux élections générales qui « utilisaient les réseaux sociaux et ont été victimes de comportements en ligne de ce type ont fait l'objet de menaces en ligne visant à *les tuer ou à les agresser violemment* pendant leur campagne électorale »[571] (l'italique est ajouté par l'auteur).

En outre, 58 % des candidats aux élections locales et 69 % des candidats aux élections générales qui ont été victimes de tels agissements ne les ont pas signalés aux plateformes en ligne concernées[572]. Les raisons invoquées de cette absence de signalement étaient notamment le fait de ne pas savoir comment procéder, l'impossibilité de trouver la fonction de signalement sur la plateforme et la trop grande ampleur des contenus violents ou haineux pour pouvoir tous les signaler. Toutefois, la raison la plus fréquemment invoquée (par 59 % des candidats aux élections locales et 72 % des candidats aux élections générales) était la conviction que le signalement ne serait pas traité de manière efficace[573]. Une simple « conviction » ne constitue pas nécessairement un motif suffisant pour conclure à l'inefficacité du cadre général irlandais de sécurité en ligne, mais les résultats de cette étude doivent néanmoins être jugés préoccupants.

5.3. L'exemple de l'Autriche

Dr Clara Rauchegger, université d'Innsbruck

5.3.1. Cadre juridique national concernant les plateformes

5.3.1.1. La loi autrichienne sur les plateformes de communication

Le législateur autrichien a adopté en 2020 une série de mesures législatives en vue de combattre les discours de haine, la diffamation, le cyberharcèlement, ainsi que d'autres comportements illégaux sur les plateformes en ligne. Elles avaient pour objectif commun la lutte contre « la haine sur internet[574] ». Le *Hass im Netz-Bekämpfungsgesetz* (paquet législatif relatif à la lutte contre la haine sur internet) est entré en vigueur en janvier 2021.

Au centre de cet ensemble de mesures figurait notamment la nouvelle *Bundesgesetz über Maßnahmen zum Schutz der Nutzer auf Kommunikationsplattformen*[575] (loi fédérale portant

[570] *Ibid.*, p. 5.
[571] *Ibid.*, p. 6.
[572] *Ibid.*, p. 81.
[573] *Ibid.*, p. 86.
[574] *Bundesgesetz, mit dem das Kommunikationsplattformen-Gesetz, das E-Commerce-Gesetz, das Mediengesetz, das Strafgesetzbuch, die Strafprozessordnung, das Einführungsgesetz zu den Strafgesetzen, das Allgemeine Bürgerliche Gesetzbuch und die Zivilprozessordnung geändert werden (Hass im Netz-Bekämpfungsgesetz)*, *BGBl.* I nº 151/2020.
[575] *Bundesgesetz über Maßnahmen zum Schutz der Nutzer auf Kommunikationsplattformen* (*Kommunikationsplattformen-Gesetz* – KoPl-G), *BGBl.* I nº 151/2020.

mesures de protection des utilisateurs de plateformes de communication – KoPl-G). À l'instar de la loi allemande d'application du droit sur les réseaux[576] (NetzDG), ce texte instaurait un certain nombre d'obligations pour les grandes plateformes en ligne. Celles-ci étaient tenues de mettre en place un système de notification, permettant le signalement par les utilisateurs des contenus illégaux, et de supprimer ou de bloquer ces contenus dans un délai de 24 heures, en cas d'illégalité manifeste, ou de sept jours, en cas de nécessité de procéder à une évaluation détaillée pour en établir l'illégalité[577]. Les plateformes devaient en outre publier des rapports de transparence[578] et nommer un représentant responsable en Autriche[579].

5.3.1.2. Arrêt de la CJUE invalidant la loi sur les plateformes de communication

Dans son arrêt dans l'affaire *Google Ireland c. KommAustria*[580], la CJUE a estimé que la KoPl-G était incompatible avec la Directive sur le commerce électronique[581]. Plus précisément, elle a constaté une violation du principe du pays d'origine consacré par la directive.

En vertu de ce principe, les fournisseurs de services de la société de l'information ne sont généralement tenus de respecter que les dispositions nationales de leur pays d'origine, c'est-à-dire de l'État membre dans lequel ils sont établis[582]. Les pays de destination, autrement dit les États membres dans lesquels les services sont proposés, ne peuvent imposer leurs propres règles juridiques à des prestataires établis dans un autre État membre[583]. Le principe du pays d'origine s'étend au « domaine coordonné », défini comme suit : « les exigences prévues par les systèmes juridiques des États membres et applicables aux prestataires des services de la société de l'information ou aux services de la société de l'information, qu'elles revêtent un caractère général ou qu'elles aient été spécifiquement conçues pour eux[584]. »

Lors de l'adoption de la Directive sur le commerce électronique en 2000, une harmonisation exhaustive de la législation applicable aux services de la société de l'information semblait irréaliste au sein de l'UE[585]. Dans le même temps, cette dernière souhaitait soutenir le développement de ces services, afin de favoriser l'innovation et la

---

[576] Loi d'application du droit sur les réseaux (*Netzwerkdurchsetzungsgesetz*, NetzDG) du 1er septembre 2017, *BGBl.* I, p. 3352. Une traduction en anglais est disponible sur : https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf;jsessionid=798A2B22B939C8AEEA23B03619CC3544.2_cid289?__blob=publicationFile&v. Pour un aperçu de la version initiale de la NetzDG, voir S. Schmitz et C. Berndt, « The German Act on Improving Law Enforcement on Social Networks (NetzDG): A Blunt Sword? », *SSRN*, 14 décembre 2018.

[577] Article 3 de la KoPl-G.

[578] Article 4 de la KoPl-G.

[579] Article 5 de la KoPl-G.

[580] C-376/22 *Google Ireland c. KommAustria* (CJUE, 9 novembre 2023) ECLI:EU:C:2023:835.

[581] Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, *JOUE* L 178 du 17 juillet 2000.

[582] Article 3, paragraphe 1, de la Directive sur le commerce électronique.

[583] Article 3, paragraphe 2, de la Directive sur le commerce électronique.

[584] Définition du « domaine coordonné » à l'article 2, point *h*), de la Directive sur le commerce électronique.

[585] B. Raue, « *Case Note on CJEU,* Google Ireland and Others, C-376/22 », *Neue Juristische Wochenschrift*, 2024, p. 201-205, p. 204.

croissance économique, et de « renforcer la compétitivité des entreprises européennes[586] ». En l'absence de législation harmonisée dans les domaines concernés, le principe du pays d'origine visait à supprimer les « obstacles résid[ant] dans la divergence des législations ainsi que dans l'insécurité juridique des régimes nationaux applicables à ces services[587] », l'idée étant que la règle selon laquelle les « services de la société de l'information doivent être soumis en principe au régime juridique de l'État membre dans lequel le prestataire est établi[588] » devait permettre de lever ces obstacles. Ils sont « réglementés dans le seul État membre sur le territoire duquel les prestataires de ces services sont établis[589] », la Directive sur le commerce électronique autorisant des dérogations à ce principe moyennant certaines conditions[590]. La libre circulation des services de la société de l'information peut notamment être restreinte si cela s'avère nécessaire pour des raisons d'ordre public, de protection de la santé publique, de sécurité publique ou de protection des consommateurs[591]. Une telle mesure doit être prise « à l'encontre d'un service de la société de l'information » donné, ce qui constitue une condition de fond essentielle à la validité de la dérogation[592]. Dans l'affaire *Google Ireland c. KommAustria*, l'interrogation centrale portait sur le fait de savoir si des mesures générales et abstraites, applicables de manière globale à certaines catégories de services de la société de l'information, relevaient de la notion de « mesures prises à l'encontre d'un service donné de la société de l'information », et pouvaient par conséquent justifier des dérogations au principe du pays d'origine[593]. Dans son arrêt, la CJUE a estimé que tel n'était pas le cas. La possibilité de déroger au principe du pays d'origine ne saurait s'étendre à des mesures générales et abstraites, telles que celles prévues par la KoPl-G. Par conséquent, cette dernière a été adoptée en violation de la Directive sur le commerce électronique.

Pour parvenir à cette conclusion, la CJUE s'est livrée à une interprétation littérale, systématique et téléologique. Du point de vue de la formulation, la CJUE a souligné que la disposition dérogatoire faisait référence à un service donné de la société de l'information (en anglais « *a given information society service* »). L'emploi du singulier et de l'adjectif « donné » tend à indiquer que la dérogation ne saurait s'appliquer à des mesures générales et abstraites visant globalement une catégorie de services de la société de l'information[594]. Dans son interprétation systématique, la CJUE a invoqué les modalités procédurales qui s'imposent aux États membres lorsqu'ils souhaitent déroger au principe du pays d'origine[595]. Enfin, d'un point de vue téléologique, la CJUE a souligné que la directive sur le commerce électronique visait à garantir la liberté des services de la société de l'information, objectif poursuivi par le biais des principes de contrôle dans l'État membre d'origine et de la reconnaissance mutuelle[596]. Ces principes seraient remis en question si les États membres étaient autorisés à adopter des mesures générales et abstraites visant une catégorie de

[586] Considérant 2 de la Directive sur le commerce électronique.
[587] Considérant 5 de la Directive sur le commerce électronique.
[588] Considérant 22 de la Directive sur le commerce électronique.
[589] C-376/22 *Google Ireland c. KommAustria* (CJUE, 9 novembre 2023), paragraphe 42. ECLI:EU:C:2023:835.
[590] Article 3, paragraphe 4, de la Directive sur le commerce électronique.
[591] Article 3, paragraphe 4, point *a*), i), de la Directive sur le commerce électronique.
[592] Article 3, paragraphe 4, point *a*), ii), de la Directive sur le commerce électronique.
[593] Voir C-376/22 *Google Ireland c. KommAustria*, *op. cit.*, paragraphe 25.
[594] *Ibid.*, paragraphe 27.
[595] Article 3, paragraphe 4, point *b*), C-376/22 *Google Ireland c. KommAustria*, *op. cit.*, paragraphes 35-38.
[596] Voir C-376/22 *Google Ireland c. KommAustria*, *op. cit.*, paragraphes 39-59.

services de la société de l'information dans le domaine coordonné[597]. La CJUE a dans l'ensemble opté pour une interprétation du principe du pays d'origine favorable au marché intérieur[598]. Renforçant ce principe, elle a limité la liberté des États membres d'adopter des législations telles que la KoPl-G ou la NetzDG en Allemagne[599/600]. Ainsi que l'a formulé un commentateur, la CJUE a dans les faits assorti d'un point d'exclamation le principe du pays d'origine[601].

5.3.1.3. Pertinence de l'arrêt pour l'interprétation du DSA

Dans le sillage des conclusions de la CJUE, la KoPl-G a été abrogée en 2024 par le *DSA-Begleitgesetz*[602] (paquet législatif d'accompagnement du DSA – DSA-BegleitG). Ce dernier introduisait par ailleurs un certain nombre de modifications dans la législation autrichienne existante et comportait en outre la nouvelle *Koordinator-für-Digitale-Dienste-Gesetz*[603] (loi relative au coordinateur pour les services numériques – KDD-G).

L'article 49 du DSA impose aux États membres de nommer à l'échelon national un coordinateur pour les services numériques (DSC). En Autriche, c'est la *Kommunikationsbehörde Austria* (Autorité des communications – KommAustria) qui a été désignée pour assurer ce rôle[604]. KommAustria[605], qui est l'organisme de régulation et de surveillance de la radiodiffusion et des médias audiovisuels électroniques, aurait également été chargée de faire appliquer la KoPl-G (invalidée par la CJUE, ainsi qu'on l'a expliqué). Elle est épaulée, pour assurer les missions qui lui incombent au titre du DSA, par une filiale de l'autorité de régulation organisée sous la forme d'une société privée détenue à 100 % par l'État[606].

La KDD-G énumère en outre une longue liste d'infractions administratives commises par les fournisseurs de services intermédiaires lorsqu'ils contreviennent aux dispositions du DSA[607]. Ces infractions sont punies d'une amende infligée par KommAustria, pouvant atteindre jusqu'à 1 % du chiffre d'affaires mondial annuel du fournisseur de services au

---

[597] *Ibid*., paragraphe 60.

[598] L. Knoke, H. Krüger et C. Sachs, « *EuGH stärkt Herkunftslandprinzip: Zugleich Besprechung von EuGH Urt. v. 9.11.2023 – C-376/22, EuZW 2024, 137 – Google Ireland u.a.* », *European Journal of Business Law*, 2024, pp. 957-961, p. 958.

[599] Concernant la NetzDG allemande, voir aussi le chapitre 4.2.1.

[600] M. Liesching, « *Das Herkunftslandprinzip limitiert Alleingänge nationaler Gesetzgeber: Anmerkung zu EuGH, Urteil vom* 9.11.2023 – C-376/22 », *Zeitschrift für Urheber- und Medienrecht*, 2024, pp. 205-207, p. 207 ; N. Wimmer et C. Teetzmann, « *Anmerkung zu Google Ireland and Others*, C-376/22 », *MMR - Zeitschrift für das Recht der Digitalisierung, Datenwirtschaft und IT*, 2024, pp. 157-162, p. 162.

[601] R. Mantz, « *Herkunftslandprinzip versus NetzDG – Wie geht es weiter mit den Pflichten von Diensteanbietern? Zugleich Besprechung von EuGH "Google Ireland u.a."* », *Gewerblicher Rechtsschutz und Urheberrecht*, 2024, pp. 34-37, p. 37.

[602] Article 10, paragraphe 1, de la *Koordinator-für-digitale-Dienste-G*, *BGBl.* I, nº 182/2023 ; pour une traduction en anglais de la loi, voir : RIS - ERV_2023_1_182 - *Austrian Laws*.

[603] Pour un aperçu en allemand, voir H. Wittmann, « *Das DSA-Begleitgesetz: Neue Instrumente zur Bekämpfung von 'Hass-im-Netz'* », *Medien und Recht*, 2023, pp. 298-301.

[604] Article 2, paragraphe 1, de la *Koordinator-für-digitale-Dienste-G*, *BGBl.* I, nº 182/2023.

[605] Voir « *Die Kommunikationsbehörde Austria (KommAustria) | RTR* ».

[606] *Koordinator-für-digitale-Dienste-G*, Article 2, paragraphe 2 ; RTR Media | RTR.

[607] *Koordinator-für-digitale-Dienste-G*, Article 5.

cours de l'exercice financier précédent (pour défaut de fourniture d'informations ou de soumission à une inspection) voire jusqu'à 6 %[608] (pour toutes les autres infractions). Si les conditions prévues par l'article 51, paragraphe 3, point *b*), du DSA sont réunies, KommAustria peut demander au Bundesverwaltungsgericht (Cour fédérale administrative) d'ordonner des restrictions temporaires d'accès au service ou, en cas d'impossibilité technique, à son interface en ligne[609].

5.3.2. Latitude pour la régulation des contenus illégaux en ligne après l'arrêt de la CJUE dans *Google Ireland c. KommAustria*

L'arrêt de la CJUE dans l'affaire *Google Ireland c. KommAustria* conserve sa pertinence sous l'empire du DSA, « dans la mesure où ce règlement n'abroge ni le principe du pays d'origine ni la faculté de déroger à ce principe[610] ». L'article 2, paragraphe 3, du DSA dispose que ce règlement n'a pas d'incidence sur l'application de la Directive sur le commerce électronique, laquelle demeure en vigueur. Il s'ensuit que le principe du pays d'origine reste d'application[611].

En vertu du considérant 9 du DSA, de surcroît, il est possible pour les États membres de réglementer les services intermédiaires moyennant deux conditions. D'une part, ces mesures nationales ne doivent pas relever du champ d'application du DSA. D'autre part, si elles se situent hors du champ d'application du DSA, elles doivent néanmoins respecter le principe du pays d'origine consacré par la Directive sur le commerce électronique. Par conséquent, une réglementation nationale qui vise les fournisseurs d'autres États membres, qui se trouve en dehors du champ d'application du DSA, mais qui relève du domaine coordonné par la Directive sur le commerce électronique, n'est admissible que si elle se justifie à titre de dérogation autorisée au principe du pays d'origine (et si elle ne relève pas d'une autre législation harmonisée de l'Union européenne).

L'arrêt rendu dans *Google Ireland c. KommAustria* restera également pertinent pour l'interprétation du DSA, qui favorise lui aussi le principe du contrôle par l'État membre d'origine[612]. En vertu de son article 56, paragraphe 1, c'est généralement l'État membre dans lequel se situe l'établissement principal du fournisseur de services intermédiaires qui dispose des pouvoirs exclusifs pour surveiller et faire respecter le DSA. Comme la Directive sur le commerce électronique, le DSA considère les législations nationales divergentes en

[608] *Koordinator-für-digitale-Dienste-G*, Article 6.
[609] *Koordinator-für-digitale-Dienste-G*, Article 4.
[610] *Google Ireland c. KommAustria*, conclusions de l'avocat général Szpunar présentées le 8 juin 2023, ECLI:EU:C:2023:467, paragraphe 8 ; M. Liesching, *op. cit.*, pp. 205-207.
[611] L. Mischensky et S. Denk, « *Digital Services Act und das Herkunftslandprinzip der E-Commerce-Richtlinie* », *Ecolex*, 2024(3), pp. 226 et s., p. 227.
[612] Voir W. Schroeder et L. Reider, « *Der rechtliche Kampf gegen Hass im Netz - Nationale Spielräume unter dem DSA* », *Österreichische Jurist:innenzeitung*, 2024(8), pp. 465 et s., p. 467.

matière de services intermédiaires comme des menaces à la libre circulation de ces services[613].

Au sein de son champ d'application, le DSA harmonise pleinement les règles applicables aux services intermédiaires dans le marché intérieur (considérant 9 du DSA). En conséquence, ces règles sont déterminées non plus par l'État membre d'origine, mais par l'Union européenne[614]. Le règlement met notamment en place, conformément à son article 1, paragraphe 2, un cadre pour l'exemption conditionnelle de responsabilité des fournisseurs de services intermédiaires, des obligations de diligence spécifiques, adaptées à certaines catégories de fournisseurs de services intermédiaires, ainsi que des règles de mise en œuvre et d'exécution du DSA. À l'inverse, les États membres sont libres de réglementer les questions qui ne relèvent pas du DSA. Ce dernier est donc sans préjudice de la législation nationale en ce qui concerne les contenus illégaux en ligne[615]. En particulier, le DSA ne définit pas ce qui est illégal en ligne, laissant ce soin aux États membres[616]. En outre, les dispositions adoptées à l'échelon national en matière de contenus illégaux en ligne peuvent être admissibles si elles poursuivent d'autres objectifs d'intérêt public légitimes que ceux poursuivis par le DSA ou si elles mettent en œuvre un texte de droit dérivé de l'Union sur lequel le DSA n'a aucune incidence[617].

5.3.3. Application en matière de cyberharcèlement et d'atteintes sexuelles par l'image

L'ensemble de mesures législatives adopté en vue de lutter contre la haine sur internet a également apporté des modifications à plusieurs lois existantes, et notamment au *Strafgesetzbuch* autrichien (code pénal – StGB). En dehors de la KoPl-G, la législation relative à la haine sur internet reste pour l'essentiel en vigueur.

Parmi les nouvelles infractions pénales ainsi introduites figure celle de cyberharcèlement persistant[618]. On entend par cyberharcèlement soit une atteinte à l'honneur de la victime, soit la diffusion d'informations ou d'images de la victime relevant de la sphère la plus intime sans son consentement. Cette conduite est punissable, dès lors qu'elle est de nature à porter déraisonnablement atteinte au mode de vie de la victime et qu'elle est perceptible par un grand nombre de personnes sur une longue période. Le cyberharcèlement persistant est passible d'une amende ou d'une peine d'emprisonnement pouvant aller jusqu'à un an. Cette durée monte à trois ans si l'infraction a entraîné le suicide ou une tentative de suicide de la victime, ou si elle est commise de façon continue pendant une période supérieure à un an ou reste perceptible pour la victime pendant plus d'un an.

[613] Voir les considérants 2, 4 et 9 du DSA.
[614] L. Mischensky et S. Denk, *op. cit.*, pp. 226 et s., p. 227.
[615] W. Schroeder et L. Reider, *op. cit.*, pp. 465 et s., p. 467.
[616] *Ibid.*, p. 468.
[617] *Ibid.*, p. 467. Voir le considérant 9, dernière phrase, ainsi que l'article 2, paragraphe 4, du DSA.
[618] StGB, Article 107*c* ; *Hass im Netz-Bekämpfungsgesetz*, *BGBl.* I nº 151/2020, Article 8.

Autre modification importante apportée au StGB : l'instauration d'un délit de captation d'images impudiques[619] (« *upskirting* »). Le terme désigne la pratique consistant à photographier ou à enregistrer les parties intimes d'une personne sans son consentement, généralement en pointant un appareil photo sous une jupe ou une robe. Ce délit est désormais passible d'une peine d'emprisonnement pouvant aller jusqu'à six mois ou d'une amende, que les images captées aient ou non été publiées.

En outre, l'incitation à la violence et à la haine est désormais érigée en infraction, même si elle ne vise pas l'ensemble d'un groupe de population, mais un individu appartenant à ce groupe[620]. Une infraction supplémentaire a été introduite dans le StGB à une date plus récente – c'est-à-dire non pas dans la *Hass im Netz-Bekämpfungsgesetz*, mais à l'occasion d'une autre initiative législative en 2025[621] : l'envoi non sollicité d'images représentant des organes génitaux humains exposés est désormais une infraction pénale, passible d'une peine pouvant aller jusqu'à six mois d'emprisonnement ou d'une amende.

Outre ces changements au sein du StGB, d'autres champs juridiques ont été révisés dans le sens d'un renforcement de la lutte contre la haine sur internet, notamment grâce à des modifications du droit procédural civil et pénal.

Une modification apportée au *Zivilprozessordnung* (Code de procédure civile – ZPO) vise ainsi à faire supprimer rapidement les contenus en ligne portant atteinte à la dignité humaine d'une personne[622]. Si la demande est suffisamment étayée, la juridiction compétente doit rendre une ordonnance d'injonction à la demande du plaignant, sans audience préalable et sans entendre le défendeur auparavant.

Plusieurs modifications ont en outre été apportées au *Strafprozessordnung* (code de procédure pénale – StPO). La première concerne l'enquête portant sur la personne accusée. En Autriche, l'insulte et la diffamation relèvent de poursuites privées engagées par la victime elle-même, autrement dit c'est cette dernière qui doit le plus souvent enquêter sur les auteurs de l'infraction, ce qui peut occasionner des frais considérables. La nouvelle procédure vient faciliter l'action des victimes[623]. De plus, celles-ci ne supportent plus les risques liés aux frais de justice en cas d'acquittement du mis en cause[624]. Elles bénéficient également d'un soutien psychosocial et juridique renforcé au cours de la procédure[625].

[619] StGB, Article 120*a* ; *Hass im Netz-Bekämpfungsgesetz*, *op. cit.*
[620] StGB, Article 283; *Hass im Netz-Bekämpfungsgesetz*, *op. cit.*
[621] StGB, Article 218, paragraphe 1b, instauré par le *BGBl.* I nº 45/2025.
[622] ZPO, Article 549, introduit par l'article 3 de la *Hass im Netz-Bekämpfungsgesetz*, *op. cit.*
[623] StPO 1975, Article 71; *Hass im Netz-Bekämpfungsgesetz*, *op. cit, A*rticle 10.
[624] StPO 1975, Article 390, paragraphe 1a du 1975 ; *Hass im Netz-Bekämpfungsgesetz*, *op. cit.*
[625] StPO, Article 66b; *Hass im Netz-Bekämpfungsgesetz*, *op. cit.*

5.4. L'exemple de l'Italie

Dr Giovanni de Gregorio, Professor in Law and Technology, Católica Global School of Law and Católica Lisbon School of Law

5.4.1. Le cadre législatif national applicable aux plateformes

La prise de conscience croissante des dangers que posent les contenus illicites et la désinformation a influencé la réglementation italienne en matière de contenus en ligne. Bien que le cadre législatif italien soit conforme au droit européen, notamment au regard du DSA, son application repose principalement sur des mécanismes nationaux. Ceux-ci comprennent à la fois des instances administratives et judiciaires, qui jouent un rôle essentiel dans la lutte contre les contenus illicites et préjudiciables, comme les discours de haine et la désinformation. Ce système repose non seulement sur les tribunaux, mais également sur des autorités administratives, notamment l'*Autorità per le Garanzie nelle Comunicazioni* (AGCOM) et d'autres organismes de réglementation qui peuvent être amenés à intervenir dans des affaires spécifiques relevant de domaines tels que la protection des données ou les systèmes d'intelligence artificielle.

Le DSA a remplacé l'ensemble disparate de dispositions relatives à la responsabilité des intermédiaires que les États membres avaient élaborées dans le cadre de la Directive sur le commerce électronique[626]. En Italie, la mise en place du DSA a entraîné l'abrogation partielle du décret-loi[627] qui codifiait l'ancien « régime d'exonération de responsabilité » de l'Union européenne avec les exemptions prévues par la directive sur le commerce électronique. En vertu du nouveau régime instauré par le DSA, les obligations qui incombent aux intermédiaires en ligne en Italie, qui vont des procédures de notification des contenus illicites et d'action au renforcement des mesures de transparence et de responsabilité pour les VLOP, sont directement applicables, à l'instar d'autres instruments réglementaires tels que le Règlement sur les contenus terroristes[628], le Règlement sur la publicité à caractère politique[629] et le Règlement européen sur la liberté des médias (EMFA)[630].

L'Italie a par ailleurs réformé sa législation nationale relative aux médias en adoptant le *Testo Unico sui Servizi di Media Audiovisivi* (Code consolidé des services de

[626] Union Européenne, Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, *JOUE* L 178, 17 juillet 2000.

[627] *Decreto legislativo 9 aprile 2003, n. 70, Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio ellettronico* (Décret-loi n° 70/2003).

[628] Règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne, *JOUE* L 172/79, 17 mai 2021.

[629] Règlement (UE) 2024/900 du Parlement européen et du Conseil du 13 mars 2024 relatif à la transparence et au ciblage de la publicité à caractère politique, *JOUE* L 2024/900, 20 mars 2024.

[630] Règlement (UE) 2024/1083 du Parlement européen et du Conseil du 11 avril 2024 établissant un cadre commun pour les services de médias dans le marché intérieur et modifiant la directive 2010/13/UE (Règlement européen sur la liberté des médias), *JOUE* L 2024/1083, 17 avril 2024.

médias audiovisuels – TUSMA)[631]. Le TUSMA met en œuvre la Directive SMA révisée et étend les obligations réglementaires aux « *fornitori di Servizi di piattaforma per la condivisione di video* » (fournisseurs de services de plateformes de partage de vidéos), ce qui englobe les services comparables à *YouTube*. Ces services sont désormais soumis à des exigences en matière de contenus, et notamment à des obligations relatives aux discours de haine, à la protection des mineurs et à l'incitation à la violence. Ces plateformes sont tenues d'adopter des mesures visant à limiter la diffusion de contenus à caractère haineux ou susceptibles d'être préjudiciables au public, par exemple en proposant des systèmes de signalement et de notification, en veillant à la transparence des conditions d'utilisation ou en proposant des outils de contrôle parental.

5.4.2. Les dispositions spécifiques en matière de propos diffamatoires, de discours de haine et d'incitation à la violence

Les dispositions applicables aux discours de haine et à la désinformation ne se limitent pas à la réglementation des plateformes, mais relèvent également du droit pénal et du droit civil. Plus précisément, en vertu du code pénal italien (*Codice Penale*)[632], le délit de diffamation est constitué lorsqu'une personne porte atteinte à la réputation d'une autre par des propos tenus devant au moins deux personnes[633], avec des peines aggravées si l'acte est commis par voie de presse ou par tout autre moyen de publicité. Les juridictions italiennes ont toujours considéré qu'internet, et notamment les réseaux sociaux, constituait un tel moyen, faisant ainsi de la diffamation en ligne une forme d'infraction aggravée[634]. Les sanctions peuvent aller d'une amende à une peine d'emprisonnement maximale de trois ans, même si l'emprisonnement est de plus en plus fréquemment remplacé par des sanctions pécuniaires. Le code pénal aborde également la question de l'incitation à commettre un délit et de l'apologie de la criminalité[635]. Il évoque l'incitation publique à commettre des délits et la glorification d'actes criminels.

Plus précisément, des dispositions visant les propos discriminatoires ont vu le jour à mesure de l'évolution du code pénal italien, dans le cadre de la « loi *Mancino* »[636], qui complète la législation antifasciste et antiraciste précédemment adoptée en Italie. L'article 604-*bis* du code pénal réprime la propagande fondée sur la supériorité ou la haine de groupes raciaux, ethniques, nationaux ou religieux, ainsi que l'incitation à la discrimination

[631] *Decreto legislativo 8 novembre 2021, n. 208, attuazione della direttiva (UE) 2018/1808 del Parlamento europeo e del Consiglio, del 14 novembre 2018, recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri, concernente il testo unico per la fornitura di servizi di media audiovisivi in considerazione dell'evoluzione delle realtà del mercato* (Décret-loi n° 208/2021 – TUSMA).
[632] *Codice Penale* (Code pénal approuvé par le décret royal n° 1398 du 19 octobre 1930, tel que modifié jusqu'au décret-loi n° 63 du 11 mai 2018).
[633] Code pénal italien, Article 595.
[634] Voir, par exemple, Cour suprême italienne, arrêt 3453/2023 ; Cour suprême italienne, arrêt 45680/2022.
[635] Code pénal italien, Article 414.
[636] Code pénal italien, Articles 604-*bis* et 604-*ter*.

ou à la violence à l'encontre de ces groupes. L'article 604-*ter* établit une circonstance aggravante, qui alourdit les peines encourues lorsque des infractions ordinaires sont commises avec l'intention de discriminer. Ces dispositions sont principalement inspirées du droit international en matière de droits de l'homme et de la législation européenne contre la discrimination afin de lutter contre les propos racistes et xénophobes en ligne. D'autres exemples législatifs pertinents figurent dans le décret-loi n° 215/2003[637], qui transpose la directive 2000/43/CE[638] et met en œuvre le principe de l'égalité de traitement entre les personnes sans distinction d'origine raciale ou ethnique, ainsi que dans la loi n° 115/2016 contre le génocide et les crimes contre l'humanité[639].

La désinformation n'est en revanche pas soumise à une réglementation spécifique en Italie. Les tentatives de légiférer contre la désinformation en ligne, notamment un projet de loi visant à ériger la désinformation en infraction pénale[640], se sont soldées par un échec. En conséquence, bien que la lutte contre les discours de haine trouve davantage de fondements juridiques dans le droit pénal et soit renforcée par les cadres réglementaires de l'UE et d'autres pays, la désinformation ne fait l'objet que de mesures indirectes, sous la forme de réglementations applicables aux plateformes, d'obligations imposées par la législation relative aux médias ou, dans certains cas, de recoupements avec des infractions déjà existantes comme la diffamation ou l'incitation à la haine.

5.4.3. L'application de la réglementation contre les propos diffamatoires, les discours de haine et l'incitation à la violence

5.4.3.1. L'application des normes administratives et le rôle de l'AGCOM

En Italie, l'application administrative des dispositions relatives aux contenus relève de la compétence de l'AGCOM. Initialement chargée de réglementer les télécommunications et la radiodiffusion, ainsi que de garantir le pluralisme, la concurrence et la protection des mineurs[641], son mandat s'est progressivement étendu aux environnements en ligne, d'abord par la publication de codes de conduite non contraignants et la mise en place d'observatoires et de mécanismes de contrôle, puis par sa désignation en qualité de coordinateur des services numériques de l'Italie au titre du DSA. Ces mesures ont contribué

[637] *Decreto Legislativo 9 luglio 2003, n. 215, Attuazione della direttiva 2000/43/CE per la parità di trattamento tra le persone indipendentemente dalla razza e dall'origine etnica* (Décret-loi n° 215/2003).
[638] Directive 2000/43/CE du Conseil du 29 juin 2000 relative à la mise en œuvre du principe de l'égalité de traitement entre les personnes sans distinction de race ou d'origine ethnique, 2000, *JOUE* L 180/22.
[639] *Legge 16 giugno 2016, n. 115, modifica all'articolo 3 della legge 13 ottobre 1975, n. 654, in materia di contrasto e repressione dei crimini di genocidio, crimini contro l'umanità e crimini di guerra, come definiti dagli articoli 6, 7 e 8 dello statuto della Corte penale internazionale* (Loi n° 115/2016).
[640] Projet de loi n° 2688.
[641] *Legge 31 luglio 1997, n. 249, Istituzione dell'Autorità per le garanzie nelle comunicazioni e norme sui sistemi delle telecomunicazioni e radiotelevisivo* (Loi n° 249/1997).

à faire passer l'AGCOM du statut de « sentinelle des communications » à celui de principale autorité institutionnelle de gouvernance des contenus en ligne en Italie.

La compétence de l'AGCOM se limite à son mandat national. Bien que la Commission européenne conserve des prérogatives exclusives sur les très grandes plateformes en matière de risques systémiques, l'AGCOM contribue à veiller au respect de la réglementation et des droits des utilisateurs à l'échelle nationale. Elle participe également au Comité européen des services numériques, au sein duquel les autorités nationales échangent des informations et élaborent des positions communes. L'AGCOM est notamment chargée d'enquêter sur les violations du DSA, de certifier les mécanismes extrajudiciaires de règlement des litiges et d'assurer la coordination avec les autres organismes de réglementation nationaux et européens.

L'AGCOM jouait déjà un rôle particulièrement actif avant l'adoption du DSA. Elle a en effet adopté un règlement relatif à la protection de la dignité humaine, au principe de non-discrimination et à la lutte contre les discours de haine[642], qui fixe les normes applicables à l'ensemble des médias afin de lutter contre les contenus discriminatoires et choquants et, en ce qui concerne les fournisseurs de services audiovisuels, encourage l'adoption de codes de conduite, identifie les formes de corégulation ainsi que les mécanismes de contrôle et de surveillance des différentes activités. Cet instrument a ensuite été complété par un autre règlement[643] visant à protéger les droits fondamentaux individuels. Ce dernier a renforcé les pouvoirs de l'AGCOM en matière de lutte contre les discours de haine et établit notamment des critères contraignants auxquels doivent se conformer les fournisseurs de services de médias audiovisuels, y compris les services de partage de vidéos, afin de prévenir toute forme d'incitation à la violence et à la haine. Ce règlement instaure par ailleurs un mécanisme de sanction spécifique, qui permet à l'AGCOM d'imposer des sanctions pécuniaires lorsqu'elle constate une violation de l'interdiction d'incitation à la violence ou à la haine à l'encontre d'une personne ou d'un groupe de personnes pour les motifs énumérés à l'article 21 de la Charte des droits fondamentaux de l'Union européenne, ou en violation de l'article 604-*bis* du code pénal italien.

La désinformation est une question encore plus complexe. La législation italienne étant limitée dans ce domaine, la désinformation est traitée indirectement, à travers différentes approches, notamment la diffamation et le droit des consommateurs, la protection des consommateurs, l'application des droits d'auteur ou encore des mesures administratives. L'AGCOM a préféré promouvoir l'éducation aux médias, la transparence de la publicité à caractère politique et la coopération avec les plateformes plutôt que de recourir au droit pénal. Ce cadre réglementaire peut en effet également s'appliquer aux situations dans lesquelles la désinformation est associée à des incitations à la haine concernant le même contenu. De fait, les campagnes de désinformation exploitent bien souvent les préjugés ou les propos discriminatoires, ce qui amplifie les stéréotypes ou attise l'hostilité à l'égard de groupes spécifiques.

L'AGCOM s'est également engagée dans une application progressive de la loi par le biais de rapports, de lignes directrices et de forums multipartites. Depuis 2017, elle coordonne le *Tavolo per il pluralismo e la correttezza dell'informazione sulle piattaforme*

[642] AGCOM, *Delibera* 157/19/CONS.
[643] AGCOM, *Delibera* 37/23/CONS.

digitali, une table ronde qui rassemble des institutions, des médias, des plateformes et la société civile afin de lutter contre la désinformation. Dans le cadre de ces activités, l'AGCOM a mené une enquête de terrain sur les plateformes numériques et le système d'information, qui a donné lieu à la publication de rapports qui établissent une cartographie de la propagation de la désinformation et analysent les opinions et le comportement des utilisateurs [644]. L'AGCOM a également adopté des lignes directrices visant à garantir l'égalité d'accès aux plateformes en ligne pendant les campagnes électorales[645], qui ont été élaborées au sein de sa table ronde technique et qui ont permis de promouvoir des outils de vérification des faits et la création de groupes de travail sur la surveillance, la classification et l'éducation aux médias.

5.4.3.2. L'application du droit et le rôle de la justice

Les tribunaux jouent un rôle essentiel dans l'application des dispositions relatives aux litiges portant sur des contenus illicites en ligne. Les juridictions italiennes sont régulièrement saisies d'affaires de diffamation et d'incitation à la haine diffusées sur des plateformes, et notamment sur les réseaux sociaux. Ce rôle devrait encore s'accentuer compte tenu des recours prévus par le DSA pour permettre aux utilisateurs d'obtenir réparation[646]. En effet, outre la responsabilité pénale, les victimes peuvent intenter des actions au civil, telles que des demandes de dommages-intérêts, sur la base du principe général de responsabilité civile pour des dommages causés à la suite d'un comportement illicite[647], ou recourir à des mécanismes d'injonction préalable. Les tribunaux peuvent accorder des dommages-intérêts et ordonner des mesures correctrices, comme la suppression du contenu diffamatoire en question.

Les tribunaux continuent d'appliquer le même régime de responsabilité des intermédiaires, fondé sur les exemptions de responsabilité prévues par le DSA, notamment en ce qui concerne la responsabilité des réseaux sociaux et des blogueurs pour les contenus provenant de tiers[648]. Sur ce point, la Cour suprême italienne s'est efforcée de distinguer les fournisseurs passifs des fournisseurs actifs[649] et a réaffirmé la responsabilité des fournisseurs de contenus en ligne pour les contenus diffamatoires lorsqu'ils ne les suppriment pas dans les meilleurs délais après en avoir été informés.

Les juges ont toutefois traité de manière différente des affaires similaires relatives à des discours de haine en ligne, comme en témoignent les décisions divergentes rendues en 2019 au sujet de la suppression par *Facebook* des pages des partis d'extrême droite *CasaPound* et *Forza Nuova*[650]. Alors que *CasaPound* a dans un premier temps obtenu une injonction du tribunal de Rome ordonnant à *Facebook* de rétablir sa page, au motif que le

[644] AGCOM, *Delibera* 309/16/CONS ; *Delibera* 79/20/CONS.
[645] AGCOM, *Linee guida per la parità di accesso alle piattaforme online durante la campagna elettorale per le elezioni politiche 2018* (Lignes directrices pour l'égalité d'accès aux plateformes en ligne pendant les campagnes électorales 2018).
[646] DSA, Article 54.
[647] Code civil italien, Article 2043.
[648] Cour suprême italienne, arrêt 17360/2025.
[649] Cour suprême italienne, arrêt 39763/2023.
[650] Tribunal de Rome, ordonnance 59264/2019 ; Tribunal de Rome, ordonnance 64894/2019.

bannissement d'un parti politique pourtant légal d'une plateforme en ligne constituait une violation des droits constitutionnels à la liberté d'expression et à la participation à la vie politique. L'action de *Forza Nuova* a quant à elle été rejetée d'emblée en 2020, le tribunal ayant estimé que son contenu raciste et fasciste enfreignait clairement les conditions d'utilisation de *Facebook* et que la propagation de la haine n'était pas un droit. Toutefois, après un procès en bonne et due forme en 2022, le contenu de *CasaPound* a été qualifié de discours de haine ne relevant pas de la protection de la liberté d'expression, et la suppression des comptes par *Facebook* a donc été jugée licite. Ensemble, ces affaires mettent en évidence la tension qui existe dans la jurisprudence italienne entre la sauvegarde du pluralisme politique et l'affirmation du droit et du devoir contractuels des plateformes de supprimer les discours de haine.

Parallèlement, les juridictions ont confirmé la responsabilité des utilisateurs en tant que principaux auteurs d'infractions, tout particulièrement en cas de publications diffamatoires sur les réseaux sociaux. Il reste néanmoins difficile de parvenir à un équilibre entre la liberté d'expression et d'autres intérêts constitutionnels divergents. Par exemple, dans une affaire où une femme avait été condamnée pour des publications sur *Facebook* jugées préjudiciables à la réputation d'un conseiller municipal, la Cour suprême italienne a annulé la condamnation, estimant que des commentaires même virulents ou vulgaires pouvaient être licites s'ils constituaient un exercice légitime du droit à la critique[651]. L'essentiel est que ces expressions restent proportionnées, adaptées au contexte et ne constituent pas des attaques personnelles ou des humiliations gratuites. Cependant, dans une autre affaire, portant sur la diffusion de propos diffamatoires par un ancien conseiller municipal, le tribunal a jugé que l'utilisation d'un langage injurieux et d'insultes personnelles dépassait les limites de la critique politique légitime, réaffirmant ainsi l'application de la législation relative à la diffamation dans de tels contextes[652].

Les juges sont confrontés à de nombreuses difficultés lorsqu'ils sont amenés à traiter des affaires de désinformation, dans la mesure où les recours juridiques ont un caractère par essence réactif et nécessitent de longues procédures, alors que les fausses informations diffusées en ligne peuvent se propager à une vitesse fulgurante et de manière incontrôlable. De plus, l'absence de cadre législatif spécifique à ce type de contenus oblige les juges à faire appel à des dispositions déjà en vigueur, notamment celles relatives à la diffamation ou aux discours de haine, qui ne s'appliquent pas toujours aussi facilement à la désinformation. Cette situation entraîne une incertitude dans l'interprétation juridique et une application disparate de la loi. Même après l'adoption du DSA, qui établit des mécanismes procéduraux pour lutter contre les contenus illicites, l'ampleur de la désinformation en ligne, en particulier dans le cas des campagnes électorales, pourrait remettre en cause les recours juridictionnels.

5.4.3.3. Les enjeux de l'application nationale de la réglementation

Le cadre réglementaire italien applicable aux contenus en ligne est en grande partie harmonisé avec le droit européen, notamment grâce au DSA, et s'accompagne

[651] Cour suprême italienne, arrêt 22341/2025.
[652] Cour suprême italienne, arrêt 11571/2025.

d'instruments nationaux tels que le *TUSMA* et la loi *Mancino*. Ensemble, ces mesures constituent un système dans lequel l'AGCOM exerce un contrôle administratif et les tribunaux garantissent des recours judiciaires, qui permettent de traiter certains problèmes tels que les discours de haine et autres formes de contenus illicites au moyen de mécanismes réglementaires, administratifs et judiciaires. Cette approche à plusieurs niveaux trouve principalement son origine dans le droit européen, qui détermine également les modalités d'application à l'échelle nationale.

La question de la désinformation pose toutefois un certain nombre de défis. À l'instar d'autres États membres, l'Italie mise sur des outils réglementaires indirects, des recours judiciaires et des initiatives pilotées par les plateformes. Ces mécanismes s'avèrent cependant insuffisants pour faire face à la rapidité et à l'ampleur de la circulation de la désinformation en ligne. Bien que les autorités administratives soient de plus en plus sollicitées pour lutter contre la circulation de contenus illicites dans les limites de leurs attributions, l'efficacité des réponses au niveau national repose désormais davantage sur la coordination entre les autorités réglementaires nationales et les institutions européennes dans le cadre du comité européen des services numériques, notamment pour lutter contre la désinformation en tant que risque systémique.

6. Les autres catégories de contenus préjudiciables soumises à des restrictions

6.1. L'application des normes au niveau de l'Union européenne

Dr Mark D. Cole, directeur des affaires académiques de l'Institut européen du droit des médias (EMR) et professeur en droit des médias et des télécommunications à l'université du Luxembourg

Alors que les précédents chapitres examinaient principalement les mécanismes d'application des normes visant à supprimer ou à rendre inaccessible les contenus illicites, le présent chapitre se concentre sur les contenus qui ne sont pas nécessairement illicites, mais qui peuvent néanmoins faire l'objet de restrictions d'accès pour certains groupes, en particulier les mineurs, en raison de leur caractère potentiellement préjudiciable[653]. Les contenus pornographiques en sont un excellent exemple : en effet, bien qu'ils ne soient pas interdits en soi dans la plupart des systèmes législatifs nationaux, leur accessibilité par les mineurs fait généralement l'objet de restrictions[654]. Ce contexte a conduit à l'apparition de régimes réglementaires qui ne pénalisent pas le contenu lui-même, mais cherchent davantage à contrôler son accessibilité en fonction du risque et du préjudice potentiel qu'il peut représenter pour les publics vulnérables.

Au sein de l'Union européenne, ces mesures de protection sont clairement formulées par la Directive SMA. Elle établit un cadre harmonisé qui oblige les États membres à veiller à ce que les services de médias audiovisuels ne comportent pas de contenu susceptible de porter atteinte à l'épanouissement physique, psychique ou moral des mineurs, sous réserve que ce contenu soit mis à disposition de manière à ce que les mineurs ne puissent en principe ni l'entendre ni le voir. Comme le souligne le point 2.2.2, la Directive SMA s'applique à la fois à la radiodiffusion traditionnelle et aux services à la demande, ainsi qu'en partie – pour ce qui est notamment de l'obligation de protéger les mineurs – aux fournisseurs de services de plateformes de partage de vidéos, afin de prendre en compte la diversification croissante des modes de consommation des médias. Les mesures prévues par la Directive SMA peuvent inclure des restrictions techniques d'accès,

[653] Pour la définition d'un contenu préjudiciable dans ce contexte, voir A. Lacourt, E. Munch et J. Radel-Cormann, *AVMSDigest, La protection des mineurs sur les plateformes de partage de vidéos*, Observatoire européen de l'audiovisuel, Strasbourg, octobre 2024, pp. 13 et s.

[654] Pour davantage de détails et une comparaison entre les pays, voir J. Ukrow, M.D. Cole et C. Etteldorf, *Stand und Entwicklung des internationalen Kinder- und Jungedmedienschutzes*, EMR Script Bd. 7, dco-Verlag, Püttlingen, 2023 (avec un résumé en anglais, pp. 34 et s.). Voir également V. Verdoodt, E. Lievens et A. Chatzinikolaou, « *The EU Approach to Safeguard Children's Rights on Video-Sharing Platforms: Jigsaw or Maze?* », *Media and Communication* 11(4), 2023, pp. 151-163.

des outils de vérification de l'âge et l'utilisation de systèmes de classification ou de descripteurs pour informer les téléspectateurs. En ce qui concerne les plateformes de partage de vidéos, l'ensemble des mesures que les États membres ont la possibilité de leur imposer sont énumérées en détail dans la directive. Les mesures nationales de protection des mineurs dans les États membres de l'UE ont été présentées dans le récent *AVMSDigest – La protection des mineurs sur les plateformes de partage de vidéos*[655] de l'Observatoire européen de l'audiovisuel. Le présent rapport se concentrera quant à lui sur les restrictions prévues au titre du Règlement sur les services numériques (DSA). De manière générale, on peut observer que la Directive SMA fixe des exigences spécifiques en matière de contenus pour les services de médias audiovisuels, en particulier à l'égard des mineurs et, dans certains cas, du grand public, et que le DSA complète ces dispositions en tenant compte de l'écosystème plus vaste de la diffusion de contenus numériques, notamment par l'intermédiaire des fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne, afin de garantir que des mesures de protection soient globalement intégrées dans l'architecture même des services en ligne.

En sa qualité de règlement européen, le DSA instaure un cadre horizontal pour la réglementation des intermédiaires en ligne, qui a été présenté au point 2.2.2. Sans interdire directement certains contenus, le DSA estime que les fournisseurs de services intermédiaires, comme ceux visés par la Directive SMA, doivent mettre en place des mécanismes qui permettent de restreindre l'accès à certains contenus, en particulier lorsque ceux-ci sont préjudiciables aux utilisateurs vulnérables du service, par exemple les mineurs. La protection des mineurs est un objectif politique majeur de l'Union européenne[656] et a été expressément intégrée dans le DSA. En effet, en vertu de l'article 28(1) du DSA, les plateformes accessibles aux mineurs – c'est-à-dire, en principe, tous les services de plateformes en ligne accessibles au public sans condition d'accès spécifique et dont le champ d'application est par conséquent très étendu – sont tenues de prendre des mesures appropriées et proportionnées pour protéger les mineurs[657]. Ces mesures peuvent inclure la conception des interfaces de la plateforme ou de certaines de leurs parties avec, par défaut, le plus haut niveau de confidentialité, de sûreté et de sécurité pour les mineurs, le cas échéant, ou l'adoption de normes pour la protection des mineurs, ou encore l'adhésion à des codes de conduite destinés à protéger les mineurs[658].

Les contenus préjudiciables et leur impact sur les mineurs constituent par ailleurs l'un des risques systémiques que les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne doivent prendre en compte dans leur évaluation des risques systémiques et dont ils doivent atténuer les effets conformément à

[655] A. Lacourt, E. Munch et J. Radel-Cormann, *op cit*. Voir également en détail J. Weinand, *Implementing the EU Audiovisual Media Sevices Directive*, Nomos, Baden-Baden, 2018, notamment les pages 489 et suivantes et 741 et suivantes.
[656] DSA, Considérant 71.
[657] Sur la proportionnalité de ces mesures, voir M. Liesching, « *Artikel 28 DSA* » *in* M. Liesching (sous la direction de) *op. cit*., paragraphes 38 et suivants. Pour une analyse générale, voir F. Wilman, S.L. Kalėda et P.J. Loewenthal, *The EU Digital Services Act*, Oxford University Press, Oxford, 2024, p. 218.
[658] *Ibid*.

l'article 35(1) du DSA[659]. D'autres risques systémiques peuvent également découler de la conception, du fonctionnement ou de l'utilisation, y compris par manipulation, des fournisseurs de ces plateformes et moteurs de recherche en ligne, avec des conséquences réelles ou prévisibles sur la santé publique, les mineurs et le bien-être physique et mental des individus[660]. Ces mesures d'atténuation doivent être raisonnables, proportionnées et efficaces, et adaptées aux risques systémiques spécifiques ; elles peuvent inclure la sélection de contenus adaptés aux différents âges, des outils de contrôle parental et des paramètres par défaut transparents. Afin de choisir les mesures d'atténuation les plus appropriées, les fournisseurs peuvent, le cas échéant, s'inspirer des meilleures pratiques du secteur, notamment celles établies dans le cadre d'une coopération en matière d'autorégulation, comme les codes de conduite. Ils doivent en outre tenir compte des lignes directrices de la Commission européenne[661].

Ces lignes directrices relatives à l'article 28 du DSA ont été publiées par la Commission européenne en juillet 2025 afin d'aider les plateformes en ligne à se conformer à leur obligation, énoncée à l'article 28 du DSA, de renforcer la confidentialité, la sûreté et la sécurité des mineurs en ligne[662]. Elles dressent une liste non exhaustive de mesures préconisées que les plateformes peuvent mettre en œuvre pour protéger les mineurs. Ces mesures reposent sur le principe de la protection de la vie privée dès la conception et recommandent une approche par défaut qui donne la priorité à la sécurité des enfants. Conformément à la démarche globale du DSA qui repose sur l'évaluation des risques, les lignes directrices reconnaissent tout d'abord que les plateformes présentent des niveaux de risque variables pour les mineurs. Cette approche permet une certaine souplesse de mise en œuvre, en donnant aux fournisseurs la possibilité d'adapter les mesures de protection à leurs services spécifiques tout en évitant de restreindre inutilement les droits des enfants à la participation, à l'accès à l'information et à la liberté d'expression. En conséquence, toute mesure prise par le fournisseur d'une plateforme accessible aux mineurs pour se conformer à l'article 28(1) du DSA doit respecter les principes généraux suivants : le principe de proportionnalité, le respect des droits des enfants, la protection de la vie privée, la sûreté et la sécurité dès la phase de conception et une architecture adaptée à l'âge[663].

---

[659] Pour plus d'informations sur la protection des mineurs au titre du DSA, voir M. Buiten, M. Ledger et C. Busch, « *Future of the DSA : Safeguarding Minors in the Digital Age* », uniquement en anglais, Forum sur la mise en œuvre du DSA, mars 2025.

[660] DSA, Considérant 83.

[661] DSA, Considérant 89.

[662] Commission européenne, « *Commission Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online Pursuant to Article 28(4) of Regulation (EU) 2022/2065* », 2025, en anglais ; le projet de lignes directrices a été soumis à consultation publique du 13 mai au 10 juin 2025 et a été approuvé le 14 juin 2025 ; voir Commission européenne, *Annex to the Communication to the Commission, Approval of the Content on a Draft Communication from the Commission- Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online, pursuant to Article 28(4) of Regulation (EU) 2022/2065*, en anglais. Voir également E. Munch, « Publication par la Commission européenne de lignes directrices sur la protection des mineurs au titre du DSA », *IRIS* 2025-8/9, Observatoire européen de l'audiovisuel, 2025. Pour une évaluation du point de vue de la protection des données, voir S. Stalla-Bourdillon, « *A GDPR Lens on the Draft Article 28 DSA Guidelines and Their Approach to Age Assurance* », *European Data Protection Law Review*, 2025, 11(2), pp. 207-214.

[663] Voir Commission européenne, *« Commission Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online Pursuant to Article 28(4) of Regulation (EU) 2022/2065 »*, *op. cit.*, pp. 6 et s., en anglais.

L'une des principales recommandations concerne la mise en place de mécanismes de vérification de l'âge afin de limiter le risque que les enfants soient exposés à des contenus inappropriés. Toutefois, préalablement à la mise en place d'un tel mécanisme, il appartient au fournisseur d'examiner si l'objectif d'un niveau élevé de confidentialité, de sûreté et de sécurité pour les mineurs qui utilisent son service peut être pleinement obtenu par d'autres mesures moins contraignantes[664]. La Commission européenne estime l'utilisation d'une méthode de vérification de l'âge comme une mesure appropriée et proportionnée lorsque la législation européenne ou nationale applicable prévoit un âge minimum pour l'accès à certains produits ou services proposés et/ou affichés sur la plateforme en ligne, comme la vente d'alcool, l'accès à des contenus pornographiques ou à des contenus de jeux d'argent et de hasard. Cela vaut également lorsque les conditions générales ou toute autre obligation contractuelle du service exigent que l'utilisateur soit âgé d'au moins 18 ans pour accéder au service, ainsi que dans les cas où le fournisseur a identifié des risques pour les mineurs qui ne peuvent être atténués par d'autres mesures moins intrusives. Il convient de noter que la question de la vérification de l'âge est complexe et qu'elle fait l'objet de longs débats, notamment en raison des difficultés pratiques qu'elle pose, y compris en matière de mise en œuvre[665].

Bien que les dispositions respectives de la Directive SMA et du Règlement sur les services numériques (DSA) reconnaissent clairement la nécessité de protéger les mineurs et les initiatives correspondantes prises par les plateformes, des questions subsistent pour les fournisseurs sur le niveau de vérification de l'âge qui serait jugé suffisant pour décider de la mise en œuvre de mesures de protection des mineurs. Par exemple, la Directive SMA exige que les contenus susceptibles d'être préjudiciables aux mineurs soient diffusés de manière à ce qu'ils ne puissent « normalement » ni être entendus ni être vus par ce groupe d'âge, sans pour autant imposer de technologies spécifiques de vérification de l'âge. De même, l'article 28(1) du DSA impose la mise en œuvre de « mesures appropriées et proportionnées » pour garantir un « niveau élevé de [...] sûreté » sans préciser davantage ce que constitue un niveau élevé.

Les lignes directrices de la Commission européenne, même si elles ne sont pas juridiquement contraignantes en tant que telles, offrent aux fournisseurs une série de recommandations bien plus précises sur les nouvelles normes applicables aux outils de vérification de l'âge. Elles considèrent le futur portefeuille européen d'identité numérique (*EU Digital Identity Wallet*)[666] comme un moyen approprié et fiable d'identification numérique au sens du DSA. Ce portefeuille, que les États membres doivent mettre en place d'ici au 28 novembre 2026, permettra la mise en place d'un cadre harmonisé d'identité numérique et

---

[664] *Ibid.*, p. 9.

[665] Voir OCDE, « *The Legal and Policy Landscape of Age Assurance Online for Child Safety and Well-Being* », document technique de l'OCDE, juin 2025, en anglais. Pour une vue d'ensemble des mécanismes de vérification de l'âge et de contrôle parental mis en œuvre, voir S. Broughton Micova et I. Kostovska, *The Protection of Minors on VSPs: Age Verification and Parental Control*, uniquement en anglais, Observatoire européen de l'audiovisuel, Strasbourg, 2023. S'agissant des difficultés liées à l'application de la réglementation, voir par exemple S. Schmitz-Berndt, « Le tribunal administratif de Berlin rejette le recours en référé des plateformes pornographiques contre la décision de blocage de la LMA compétente », *op. cit.*

[666] Le cadre réglementaire en vertu duquel les États membres sont tenus de fournir aux citoyens des portefeuilles européens d'identité numérique est le Règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique, *JOUE* L 2024/1183, 17 avril 2024.

l'enregistrement centralisé des informations relatives à l'âge. Ces informations seraient alors accessibles uniquement pour vérifier si un utilisateur qui, par exemple, demande l'accès à un site web, appartient ou non à la catégorie des personnes majeures, sans aucune autre précision, par exemple concernant l'âge exact ou les données personnelles de la personne concernée. Toutefois, avant la mise à disposition de ce portefeuille d'identité numérique, la Commission européenne a publié, avec les lignes directrices, une solution de vérification de l'âge de type *open source*, qui comprend une application dédiée, en tant que mesure autonome, et qui, selon elle, pourrait devenir une « norme de référence européenne [pour] une méthode de vérification de l'âge basée sur un appareil »[667]. Tout comme pour le portefeuille européen d'identité numérique, ce système garantirait à l'avenir que, hormis la vérification de l'âge, aucune autre information ne serait divulguée et que les plateformes sollicitant la vérification de l'âge recevraient uniquement l'information attestant que l'utilisateur est âgé de plus de 18 ans.

Il convient d'établir une distinction entre l'estimation de l'âge et la vérification de l'âge. La première mesure permet uniquement d'obtenir une approximation de l'âge de l'utilisateur, c'est-à-dire de confirmer qu'un utilisateur est susceptible d'avoir un certain âge[668]. Les lignes directrices énumèrent les circonstances dans lesquelles les méthodes d'estimation sont suffisantes, par exemple lorsque le fournisseur a identifié, dans son évaluation, des risques tout au plus moyens pour les mineurs sur sa plateforme et que la restriction ne devrait pas s'appliquer à tous les mineurs de moins de 18 ans, mais uniquement aux groupes d'âge les plus jeunes. En revanche, la Commission européenne considère que l'autodéclaration, à savoir le fait que la personne indique elle-même son âge, ne répond pas au critère d'une méthode efficace de vérification de l'âge[669].

Il importe également de souligner que les premières mesures d'application du DSA prises par la Commission européenne concernaient des violations potentielles des obligations en matière de protection des mineurs. Jusqu'à présent, la Commission a pris plusieurs mesures à l'encontre de fournisseurs de très grandes plateformes en ligne pour non-respect des dispositions relatives à la protection des mineurs contre les contenus préjudiciables. Par exemple, en mai 2025, elle a ouvert une procédure officielle à l'encontre de fournisseurs de contenus à caractère pornographique, à savoir les fournisseurs de *Pornhub*, *Stripchat*, *XNXX* et *XVideos*, qui avaient été désignés comme des fournisseurs de très grandes plateformes en ligne[670]. Les enquêtes de la Commission européenne se concentrent sur les risques que présentent ces types de services pour les mineurs, notamment ceux liés à l'absence de mesures efficaces de vérification de l'âge. Par exemple, la procédure engagée contre *Pornhub* reposait sur la conclusion préalable que le fournisseur avait enfreint les articles 28(1) et 34(1), 34(2) et 35(1) du DSA, notamment parce que le fournisseur, *Aylo*, qui proposait ce service, recourait à une méthode d'autodéclaration pour

[667] Communication de la Commission européenne, Lignes directrices concernant des mesures visant à garantir un niveau élevé de protection de la vie privée, de sûreté et de sécurité des mineurs en ligne, conformément à l'article 28, paragraphe 4, du règlement (UE) 2022/2065, *op. cit.*, p. 10.
[668] *Ibid.*, p. 9.
[669] *Ibid.*, p. 15.
[670] Commission européenne, « La Commission ouvre des enquêtes au titre du Règlement sur les services numériques afin de protéger les mineurs des contenus pornographiques », communiqué de presse, 27 mai 2025.

vérifier l'âge des utilisateurs et limiter l'accès du service aux mineurs[671]. L'ouverture d'une procédure officielle autorise la Commission européenne à prendre d'autres mesures coercitives, telles que l'adoption de mesures provisoires et de décisions de non-conformité. Parallèlement et en complément des activités de contrôle de la Commission européenne, les États membres du Comité européen des services numériques ont pris des mesures contre les plateformes de taille plus modeste proposant des contenus pornographiques, qui n'ont pas été désignées comme des très grandes plateformes en ligne et pour lesquelles les autorités nationales restent compétentes. Les États membres ont lancé une action coordonnée afin de garantir une application cohérente et efficace du DSA dans toute l'Union européenne[672], alors que certains États membres avaient déjà pris des mesures à titre individuel[673].

6.2. L'exemple de la Pologne

Dr *Krzysztof Wojciechowski, conseiller juridique, conseiller de la TVP, président de la Commission des droits d'auteur en Pologne, chargé de cours à l'université de Varsovie en études postdoctorales sur la propriété intellectuelle*

6.2.1. Cadre juridique national concernant les plateformes

La Pologne offre l'exemple d'un pays animé par des débats particulièrement vifs autour de la liberté d'internet, notamment en lien avec des initiatives portant sur la régulation des activités en ligne, comme dans les domaines du droit d'auteur et/ou du droit des médias[674].

Le cadre juridique polonais relatif aux plateformes en ligne, en particulier, reste à ce jour incomplet, car la loi de mise en œuvre du Règlement sur les services numériques[675] (DSA), adoptée le 18 décembre 2025 par le Parlement polonais[676], s'est heurtée au véto du

[671] Commission européenne, affaire DSA.100059 – Pornhub – Enquête sur le respect des articles 28(1) et 34(1), 34(2) et 35(1) du règlement (UE) 2022/2065, 27 mai 2025, en anglais.
[672] Commission européenne, « *The European Board for Digital Services Launches a Coordinated Action to Reinforce the Protection of Minors as regards Pornographic Platforms* », communiqué de presse, 27 mai 2025, en anglais.
[673] Voir par exemple S. Schmitz-Berndt, « Le tribunal administratif de Berlin rejette le recours en référé de plateformes pornographiques contre l'ordonnance de blocage de la LMA compétente », *op. cit.*
[674] Citons, à titre d'exemple plus ancien, le recours en annulation engagé par la Pologne à l'encontre de l'article 17, paragraphe 4, sous *b*), et sous *c*), *in fine*, de la Directive (UE) 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE, *JOUE* L 130/92 du 17 mai 2019, au regard de l'article 11 de la Charte des droits fondamentaux de l'Union européenne, qui a abouti au jugement de la CJUE du 26 avril 2022 (C-401/19 *Pologne c. Parlement européen et Conseil de l'UE*, ECLI:EU:C:2022:297).
[675] Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (Règlement sur les services numériques), *JOUE* L 277 du 27 octobre 2022.
[676] *Ustawa z dnia 18 grudnia 2025 r. o zmianie ustawy o świadczeniu usług drogą elektroniczną i niektórych innych ustaw* (loi du 18 décembre 2025 modifiant la loi sur la fourniture de services par des moyens électroniques,

Président le 9 janvier 2026[677]. Avant même le début du processus parlementaire, puis au Parlement, une partie du personnel politique, ainsi que certaines parties prenantes, ONG et autres entités, ont émis des inquiétudes concernant le modèle proposé reposant sur des injonctions préventives, notamment appliqué aux discours de haine, estimant qu'il risquait de conduire à une « censure d'internet[678] ». L'évolution du projet au fil des sessions gouvernementales puis parlementaires témoigne largement de la volonté de répondre à ces inquiétudes. Malgré tout, le Président a invoqué la persistance d'un risque pour la liberté d'expression et refusé de signer la loi adoptée par le Parlement.

La mise en œuvre du DSA devait prendre la forme d'une révision exhaustive de l'*Ustawa o świadczeniu usług drogą elektroniczną*[679] (loi sur la prestation de services par des moyens électroniques – UŚUDE). S'agissant des modalités institutionnelles, la loi de modification désigne comme coordinateur national pour les services numériques (DSC) et autorité de surveillance l'*Urząd Komunikacji Elektronicznej – Prezes* (président du Bureau des communications électroniques – UKE). Des exceptions sont prévues pour le domaine des plateformes de commerce électronique et de la protection des consommateurs qui y ont recours, placé sous la surveillance de l'autorité de la concurrence (le président du Bureau de la protection de la concurrence et des consommateurs ou *Urząd Ochrony Konkurencji i Konsumentów* [UOKiK]), ainsi qu'en ce qui concerne les plateformes de partage de vidéos (VSP), qui relèvent de la compétence du régulateur des médias (le Conseil national de la radiodiffusion ou *Krajowa Rada Radiofonii i Telewizji* [KRRiT]). La loi fixe également les règles et les procédures permettant au président de l'UKE d'accorder le statut de signaleur de confiance et de chercheur agréé, ainsi que celles autorisant la certification des organismes pour le règlement extrajudiciaire des litiges. La loi de révision met également en place des procédures de contrôle du respect du DSA, des sanctions administratives en cas de manquements, ainsi qu'un régime de traitement des plaintes prévues par l'article 53 du DSA. Elle établit en outre des règles de responsabilité civile en cas d'infraction au DSA et définit les procédures judiciaires connexes.

---

ainsi que d'autres lois). L'évolution du projet de loi pendant les consultations et les travaux gouvernementaux est consignée ici. Les travaux parlementaires au *Sejm* (la chambre basse) à partir du projet gouvernemental, ainsi que la résolution du Sénat, sont consultables ici.

[677] Motion présidentielle du 9 janvier 2026 en vue du réexamen de la loi du 18 décembre 2025 modifiant la loi sur la fourniture de services par des moyens électroniques, ainsi que d'autres lois. Le Sejm peut réadopter cette loi (et contrer le veto présidentiel) à la majorité des 3/5 (en vertu de l'article 122, paragraphe 5, de la Constitution). Cette issue est toutefois peu probable, la loi ayant recueilli une proportion de suffrages moindre lors de son vote par le *Sejm*.

[678] Ces divisions trouvent leur illustration dans les résultats du vote au Sejm le 21 novembre 2025 ; le texte a recueilli 237 voix en sa faveur, émanant principalement de la coalition au pouvoir (KO, PSL, Polska 2050, Lewica), tandis que 200 députés se sont prononcés contre (PiS, Konfederacja), et cinq se sont abstenus. Les opinions divergentes se sont exprimées au cours d'une audition publique au Sejm le 4 novembre 2025. Le projet de loi a reçu le soutien des titulaires de droits de propriété intellectuelle, notamment des producteurs de cinéma et de musique, des organismes de gestion collective et des éditeurs de presse. Certaines organisations de la société civile ont relevé l'évolution positive du projet (par exemple la Fondation Helsinki pour les droits de l'homme et la Fondation Panoptykon), tandis que d'autres (notamment Ordo Iuris, la Société des journalistes polonais et la présidente du KRRiT) ont évoqué les risques d'abus et fait valoir que les injonctions de blocage pouvaient aboutir à une censure d'internet.

[679] *Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną* (loi du 18 juillet 2022 relative à la fourniture de services électroniques), texte consolidé : *Dziennik Ustaw* (journal officiel) de 2024, élément 1513.

Les modifications les plus importantes et les plus contestées apportées à la loi concernent les règles et procédures relatives aux injonctions visant à lutter contre les contenus illégaux, ainsi que, bien qu'elles soient moins controversées, les injonctions visant à rétablir les contenus supprimés par erreur[680]. La notion de « contenu illégal » a considérablement évolué au fil des travaux gouvernementaux sur le projet. Au départ, ce dernier évoquait les contenus illégaux sans les définir. À l'issue des consultations, le texte faisait référence de manière générale aux atteintes aux droits de la personnalité et aux droits de la propriété intellectuelle, aux infractions pénales et aux infractions aux règles de protection des consommateurs. Le projet soumis par le Gouvernement au Parlement et adopté par ce dernier a une portée nettement plus limitée et est dans le même temps plus précis, puisqu'il se réfère à une liste exhaustive de 27 infractions pénales.

En vertu de l'exposé des motifs qui accompagne le projet présenté par le Gouvernement, trois critères permettent d'identifier une infraction spécifique : 1) elle doit être commise en ligne, compte étant tenu du mode opératoire de son auteur ; 2) le mode de diffusion du contenu doit être pris en considération ; 3) le blocage de l'accès au contenu ne doit pas avoir de conséquences négatives sur l'expression démocratique ou sur un scrutin électoral. Les infractions répertoriées sont notamment : les menaces passibles de sanctions ; l'incitation au suicide ou à l'automutilation ; la traite des êtres humains ; l'utilisation abusive de l'image d'autrui ; la diffusion non autorisée d'images de nudité ou à caractère sexuel ; la diffusion de pornographie accessible aux mineurs de moins de 15 ans ; la prise de contact en ligne avec des mineurs dans le but de commettre une infraction sexuelle ; la promotion de la pédophilie ; la diffusion de matériel pornographique mettant en scène des mineurs, des animaux ou des actes violents ; les fausses alertes mobilisant des institutions publiques ; la promotion du totalitarisme ; l'incitation à la haine pour des motifs racistes, xénophobes ou religieux ; l'injure publique pour ces mêmes motifs ; la fraude ; les atteintes au droit d'auteur par la diffusion non autorisée d'une œuvre ; ou encore la vente à distance de tabac. La notion de contenus illégaux ne se limite pas aux éléments directement constitutifs des infractions énumérées, mais recouvre également les contenus qui incitent à commettre ces actes[681]. La loi exclut les cas relevant de *leges speciales*, à savoir : les contenus terroristes ; les données informatiques liées au terrorisme ou à l'espionnage ; les atteintes à la législation sur la protection des consommateurs ; les programmes, vidéos ou autres contenus non conformes aux dispositions de l'*Ustawa o radiofonii i telewizji*[682] (loi sur la radiodiffusion) relatives aux plateformes de partage de vidéos (article 47*o*) en ce qui concerne la protection des mineurs, la lutte contre l'incitation à la violence et à la haine et/ou les contenus facilitant le terrorisme, la pornographie mettant en scène des mineurs ou encore les injures à caractère raciste, xénophobe ou religieux.

---

[680] UŚUDE, Chapitre 2*a* (Articles 11*a*-11*u*), ajouté par la loi de modification du 18 décembre 2025.

[681] Le projet de loi gouvernemental et le texte initialement adopté par le *Sejm* se référaient également aux contenus « faisant l'apologie » de telles infractions. Les amendements du Sénat ont supprimé cette précision, jugée ambiguë et disproportionnée, car susceptible de porter atteinte à la liberté d'expression ; des doutes ont notamment été émis quant à savoir si le fait d'aimer ou de partager un lien menant vers un contenu illégal pouvait constituer une « apologie » de ce dernier.

[682] *Ustawa z dnia 29 grudnia 1992 r. o radiofonii i telewizji* (loi sur la radiodiffusion), texte consolidé, *Dziennik Ustaw* de 2022, élément 1722, comportant des modifications ; traduction en anglais.

La loi adoptée, mais frappée par le veto présidentiel, prévoyait que les requêtes aux fins d'injonctions visant à empêcher l'accès à des contenus illégaux dans le cadre d'un service fourni par un prestataire de services intermédiaire soient présentées par le parquet, la police[683], un organisme de la *Krajowa Administracja Skarbowa* (Administration fiscale nationale – KAS), un titulaire de droits d'auteur ou de droits voisins, ou un destinataire du service[684]. Ces requêtes auraient été examinées et les injonctions rendues par la présidente du KRRiT, s'agissant des contenus disponibles sur les VSP, et par le président de l'UKE pour tous les autres contenus. Il était question d'une procédure accélérée, les décisions devant être rendues dans un délai de deux jours pour les requêtes émanant du ministère public ou de la police, de sept jours dans les autres cas et de 21 jours pour les affaires particulièrement complexes. L'échéance devait courir à compter de l'expiration du délai de deux jours accordé au destinataire ayant mis en ligne le contenu pour présenter sa position. Pour les requêtes émanant de destinataires et visant à obtenir la suppression des restrictions d'hébergement en vertu de l'article 17, paragraphe 1, du DSA, les décisions devaient être rendues dans un délai de 14 jours selon des règles de procédure similaires. Les parties auraient eu la possibilité de former un recours devant les tribunaux par l'intermédiaire de l'autorité émettrice dans un délai de 14 jours ; la juridiction aurait appliqué des procédures civiles non contentieuses et rendu des décisions susceptibles de recours, y compris en cassation. Les décisions rendues en lien avec les injonctions n'auraient pas été exécutoires immédiatement, mais seulement à l'issue du délai d'opposition, en l'absence d'opposition[685]. Le registre des noms de domaine internet utilisés pour diffuser des contenus illicites aurait été administré par le président de l'UKE et aurait servi à répertorier les noms des domaines n'ayant pas mis en place de mesures efficaces pour faire respecter les injonctions. Les fournisseurs d'accès à internet auraient été tenus de désactiver l'accès aux pages web utilisant les noms de domaine répertoriés et de rediriger les utilisateurs vers le site de l'UKE.

Le mécanisme d'injonctions préventives proposé a suscité des controverses tout au long de l'élaboration de la loi de mise en œuvre du DSA. Ses détracteurs invoquaient notamment l'imprécision des critères dans certains cas et le risque de jugements subjectifs, soulignant que la compétence d'émettre de telles injonctions incomberait à l'autorité réglementaire gouvernementale (le président de l'UKE, nommé par le Sejm sur proposition du Premier ministre). Ces inquiétudes ont été présentées sous l'angle de la censure à laquelle pourrait conduire le dispositif. La définition de la notion de « contenu illégal » ayant été resserrée et précisée, pour remplacer la référence générale antérieure à toute atteinte aux droits de la personnalité ou aux droits de propriété intellectuelle, les critiques

[683] Ainsi que les gardes-frontières, dans les affaires de traite des êtres humains.

[684] Le projet de loi gouvernemental proposait également d'autoriser les signaleurs de confiance à présenter de telles requêtes. Les détracteurs du projet ont critiqué ce point, estimant qu'il risquait d'inciter certaines organisations ayant le statut de signaleur de confiance à présenter des demandes motivées par des considérations politiques ou idéologiques. Le Parlement, suivant les amendements du Sénat, a en définitive décidé de retirer les signaleurs de confiance de la liste des organismes et entités habilités à présenter des requêtes. En revanche, les titulaires de droits d'auteur et de droits voisins ont été ajoutés à la liste.

[685] Le caractère non exécutoire des ordonnances avant la date limite fixée pour l'examen judiciaire de la mesure constituait un autre amendement apporté par le Sénat, en réponse aux préoccupations concernant le risque présumé de censure d'internet par les organismes publics. Le projet de loi gouvernemental et la loi initialement adoptée par le *Sejm* prévoyaient de permettre l'adoption d'ordonnances immédiatement exécutoires, si l'ampleur du préjudice ou l'intérêt public le justifiait.

se sont ensuite concentrées sur certaines des infractions pénales énumérées, souvent désignées collectivement sous le nom de « discours de haine », qui seraient également porteuses de risques. Les partisans du projet soulignent quant à eux que celui-ci dresse une liste précise des types de contenus illégaux en les reliant aux infractions pénales graves correspondantes, et offre la garantie d'un contrôle judiciaire des injonctions préventives[686]. Lors des sessions parlementaires, d'autres mesures visant à atténuer ces craintes ont été adoptées au Sejm et au Sénat ; il s'agit notamment de garanties concernant l'apolitisme, l'impartialité et l'équité des personnes examinant les demandes d'injonctions ; du retrait des signaleurs de confiance de la liste des entités habilitées ; du caractère non exécutoire des injonctions ; et de la suppression de l'« apologie » des infractions pénales citées comme motif possible justifiant la suppression d'un contenu[687]. Jugeant ces mesures insuffisantes, le Président a refusé de signer le texte de loi. Dans sa motivation, la motion présidentielle demandant le réexamen de la loi prend acte du clivage politique constaté au Parlement sur ce texte et de l'absence de consensus. Si la liste strictement délimitée d'infractions pénales est saluée, certains délits, notamment les atteintes aux droits de la propriété intellectuelle, nécessiteraient de l'avis du Président une appréciation judiciaire plus approfondie. Le transfert de la compétence en matière de blocage des contenus à des « organes exécutifs gouvernementaux » tels que le président de l'UKE, sans passage préalable devant la justice, est critiqué au regard de la liberté d'expression, compte tenu du risque d'influence politique. La proportionnalité du blocage administratif des contenus est en outre remise en question ; il ne s'agit en effet pas d'une exigence du DSA et d'autres modes d'action seraient envisageables, par exemple un mécanisme « de notification et d'action » et/ou des procédures judiciaires assorties d'une demande de mesures provisoires (par exemple, une injonction de suppression temporaire des contenus). Le caractère non exécutoire des injonctions avant examen judiciaire et l'absence de procédures d'urgence permettant à la justice d'examiner les objections sont tous deux critiqués au motif qu'ils risqueraient de rendre le mécanisme inefficace[688]. Il reste à voir quelle tournure prendront les événements et, dans le cas – probable – où le veto ne serait pas rejeté par le Sejm, si l'initiative reviendra sous une forme différente ou avec un champ d'application plus restreint.

Outre la mise en œuvre du DSA, le cadre juridique national existant en ce qui concerne les plateformes en ligne est principalement constitué des dispositions de l'UŚUDE, qui transpose la Directive sur le commerce électronique[689] en reprenant pour l'essentiel sa structure et son contenu. L'UŚUDE définit les notions pertinentes, en particulier la fourniture de services par voie électronique. Elle dispose que ces services sont soumis à la législation de l'État membre de l'UE ou de l'AELE/EEE dans lequel le prestataire

[686] *Ministerstwo Cyfryzacji*, « Nowe zasady w Internecie — sprawdź, co zmieni DSA » (Nouvelles règles en matière d'internet – Ce qui change avec le DSA), 3 novembre 2025, portail internet du ministère des Affaires numériques.

[687] Voir par exemple UŚUDE, *op. cit.*, Article 11*c* ; Article 11*a*, paragraphe 1 ; Article 11*n*, ajoutés par la loi modificative du 18 décembre 2025. Concernant la justification des amendements par le Sénat, cf. la motivation de sa résolution du 10 décembre 2025.

[688] La possibilité d'octroyer des subventions provenant du budget de l'État à certains signaleurs de confiance, ce qui entraînerait un « conflit d'intérêts » et UŚUDE réduirait leur indépendance, est également invoquée parmi les raisons du veto.

[689] Union Européenne, Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, *JOUE* L 178 du 17 juillet 2000.

de services a son siège social ou sa résidence (principe du pays d'origine), moyennant certaines exceptions (par exemple, la protection de la propriété intellectuelle) et des restrictions possibles, sous réserve de la procédure précisée à l'article 3, paragraphes 4 et 5, de la Directive sur le commerce électronique[690]. L'UŚUDE définit en outre les obligations des prestataires de services en matière d'informations permettant l'identification, de conditions générales, ainsi que de communications commerciales et de données à caractère personnel. Elle comporte toujours, par ailleurs, des dispositions relatives aux exemptions de responsabilité pour les prestataires de services de simple transport, de *caching* et d'hébergement, ainsi qu'au principe d'absence d'obligation générale de surveillance ; ces dispositions seront abrogées, ces questions étant désormais réglementées directement au chapitre II (articles 4 à 8) du DSA.

Les jeux de hasard en ligne constituent une exception importante au principe du pays d'origine pour les services en ligne. Ils sont soumis à la législation polonaise si le jeu est organisé sur le territoire de la Pologne, si le destinataire du service participe au jeu sur ce territoire et/ou si le service vise des destinataires en Pologne, c'est-à-dire notamment lorsqu'il est disponible en langue polonaise et/ou fait l'objet de publicités dans ce pays[691]. Les obligations incombant aux organisateurs de jeux de hasard sont détaillées dans l'*Ustawa o grach hazardowych*[692] (loi relative aux jeux de hasard), destinée à préserver ceux qui s'y adonnent des conséquences délétères du jeu. Ces mesures recouvrent notamment l'interdiction des jeux aux moins de 18 ans, des procédures de vérification de l'âge, ainsi que la protection des mineurs vis-à-vis de la publicité en ligne pour ces jeux. Le ministre des Finances tient un registre des domaines proposant des jeux d'argent en ligne qui ne respectent pas la loi et sont accessibles en Pologne. Les opérateurs de télécommunications fournissant un accès aux services internet sont tenus d'empêcher l'accès aux pages web utilisant les noms de domaine y figurant. En outre, la fourniture de services de paiement pour ces pages web est interdite. Ce dispositif a inspiré les récents projets de loi sur la protection des mineurs contre les contenus préjudiciables/la pornographie, qui sont présentés un peu plus loin.

Le cadre juridique en vigueur concernant les plateformes en ligne comporte également les dispositions relatives aux VSP de la loi sur la radiodiffusion[693], qui transposent les articles 28 *bis* et 28 *ter* de la directive sur les services de médias audiovisuels[694] (Directive SMA). Elles réglementent entre autres les critères d'établissement

---

[690] UŚUDE, Articles 3*a* et 3*b*. À noter que la loi du 18 décembre 2025 modifiant l'UŚUDE (visant à mettre en œuvre le DSA) et frappée par le veto présidentiel prévoyait l'instauration d'injonctions pour lutter contre les contenus illégaux et le rétablissement de ces contenus dans la liste des exceptions au principe du pays d'origine (l'UŚUDE, Article 3*a*, paragraphe 2).

[691] l'UŚUDE, Article 3*a*[1].

[692] *Sejm*, *Ustawa z dnia 19 listopada 2009 r. o grach hazardowych* (loi sur les jeux de hasard du 18 novembre 2009), texte consolidé : *Dziennik Ustaw* de 2025, élément 595 ; cf. articles 15*d*-15*i*.

[693] La loi sur la radiodiffusion, Chapitre 6*b*, Articles 47*l*-47*w*, *op. cit.*

[694] Directive 2010/13/UE du Parlement européen et du Conseil du 10 mars 2010 visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels (Directive Services de médias audiovisuels), *JOUE* L95/1, modifiée en dernier lieu par la Directive (UE) 2018/1808 du Parlement européen et du Conseil du 14 novembre 2018 modifiant la Directive 2010/13/UE visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels (Directive

de la compétence polonaise en ce qui concerne les VSP, les obligations de transparence, notamment s'agissant de la structure de propriété des fournisseurs, la liste des VSP tenue par l'autorité de régulation des médias (le KRRiT), ainsi que l'obligation pour les fournisseurs de notifier au KRRiT l'existence de leurs VSP. En ce qui concerne les contenus diffusés sur les VSP, les fournisseurs sont tenus de mettre en œuvre des mesures visant à empêcher la diffusion de contenus préjudiciables aux mineurs, incitant à la violence et/ou à la haine, facilitant les crimes terroristes, encourageant les injures racistes ou xénophobes, et comportant du matériel pornographique mettant en scène des mineurs. Ces fournisseurs doivent en outre mettre à disposition des mécanismes de signalement en cas d'infraction aux dispositions relatives aux contenus préjudiciables ou illégaux, et répondre aux utilisateurs dans un délai de 48 heures. Les litiges portant sur le traitement des infractions signalées peuvent être résolus par voie de médiation. Si l'utilisateur qui a mis en ligne le contenu non conforme ne remédie pas à l'infraction dans un délai déterminé, le fournisseur de VSP est tenu d'empêcher l'accès à ce contenu.

Les conditions générales des services en ligne proposés par les fournisseurs de VSP doivent préciser les modalités de classification et de signalisation des contenus, les règles applicables en matière de communications commerciales, les procédures permettant le signalement des contenus préjudiciables aux mineurs et les critères d'évaluation du respect des dispositions relatives aux contenus préjudiciables ; elles doivent de surcroît comporter des informations quant à la façon de contester une décision de blocage de l'accès aux contenus des utilisateurs, ainsi que sur le traitement des données à caractère personnel.

Lorsqu'un utilisateur commet des infractions répétées alors même qu'il lui a été demandé de mettre fin à ce comportement, le fournisseur peut suspendre sa capacité à mettre en ligne des contenus. En règle générale, cette suspension peut durer trois mois ; elle peut toutefois devenir définitive si les infractions commises concernent des contenus susceptibles de faciliter l'exécution d'actes terroristes, des contenus pornographiques mettant en scène des mineurs ou des contenus encourageant les injures racistes. Toute décision de ce type prise par le fournisseur de VSP doit être motivée et peut faire l'objet d'un recours auprès du KRRiT. La présidente de ce dernier est habilitée à prendre des décisions ordonnant la restriction de l'accès à tout contenu du VSP qui enfreint les règles relatives aux contenus préjudiciables ou illégaux, mais aussi à rétablir l'accès au contenu mis en ligne par un utilisateur ou à permettre à nouveau à un utilisateur de téléverser des contenus sur la plateforme. À l'instar des fournisseurs de services de médias, les fournisseurs de VSP sont soumis à une obligation de conservation des preuves et doivent par conséquent conserver des copies des contenus pendant 28 jours à compter de la date de leur retrait de la plateforme et les présenter à la présidente du KRRiT à la demande de celle-ci.

Les dispositions de la loi sur la radiodiffusion relatives aux services de médias audiovisuels[695] (SMA) à la demande peuvent également s'appliquer aux contenus proposés sur les VSP, y compris ceux qui ne relèvent pas de la juridiction polonaise, car les chaînes

« Services de médias audiovisuels »), compte tenu de l'évolution des réalités du marché, *JOUE* L 303 du 28 novembre 2018, ainsi que par le Règlement (UE) 2024/1083 du Parlement européen et du Conseil du 11 avril 2024 établissant un cadre commun pour les services de médias dans le marché intérieur et modifiant la directive 2010/13/UE (Règlement européen sur la liberté des médias), *JOUE* L 2024/1083 du 17 avril 2024.

[695] La loi sur la radiodiffusion Chapitre 6*a*, articles 47*a*-47*k*, de la loi sur la radiodiffusion, *op. cit*.

diffusées sur les plateformes proposant des catalogues de contenus vidéo, dès lors qu'elles sont exploitées à des fins commerciales, sont considérées comme des services de médias. En conséquence, la liste des fournisseurs de SMA à la demande gérée par le KRRiT recouvre plus de 900 services, pour une grande part disponibles sur YouTube, X, Facebook, Instagram ou TikTok[696]. En revanche, la liste établie par le KRRiT des fournisseurs de VSP soumis à la loi sur la radiodiffusion ne comporte que 14 services[697]. La réglementation des services de médias audiovisuels à la demande en Pologne repose pour l'essentiel sur la Directive SMA[698]. Toutefois, outre l'obligation qui leur incombe de présenter des informations élémentaires permettant leur identification, les fournisseurs de ces services sont soumis à une obligation de transparence en matière de propriété, qui concerne aussi leurs autres services de médias. Les fournisseurs de services de médias audiovisuels à la demande sont ainsi tenus de demander leur inscription sur la liste des fournisseurs de VOD gérée par le KRRiT et doivent remettre à ce dernier des rapports annuels concernant le respect des dispositions relatives à la protection des mineurs, à la promotion des œuvres européennes et à l'accessibilité pour les personnes handicapées. Si des contenus préjudiciables aux mineurs ont été fournis sans mesures de protection, techniques ou autres, au moins deux fois au cours d'une période de 12 mois, la présidente du KRRiT peut (dès lors qu'une demande visant à faire cesser ces pratiques a été adressée sans être suivie d'effets), par une décision formelle, retirer de la liste le fournisseur du service concerné.

6.2.2. Dispositions particulières de la loi sur la radiodiffusion visant à protéger les mineurs contre les préjudices en ligne

La loi sur la radiodiffusion comporte une série de dispositions destinées à protéger les mineurs contre les contenus préjudiciables. Elles concernent les services de programmes linéaires (radio et télévision), y compris lorsqu'ils sont diffusés en ligne[699], ainsi que les services de médias audiovisuels à la demande[700] et les plateformes de partage de vidéos[701], comme on l'a déjà évoqué.

S'agissant des programmes linéaires et des services de médias à la demande, la loi opère une distinction entre les contenus « préjudiciables au développement physique, mental ou moral des mineurs », et notamment ceux qui comportent de la pornographie ou

[696] Liste, établie par la présidente du KRRiT, des fournisseurs de services de médias audiovisuels à la demande (VOD) – 4 août 2025 (*Lista dostawców audiowizualnych usług medialnych na żądanie (VOD) wpisanych do wykazu Przewodniczącej KRRiT stan na 4 sierpnia 2025 r.*)

[697] Liste, établie par la présidente du KRRiT, des fournisseurs de services de partage de vidéos (VSP) – 4 août 2025 (*Lista dostawców Platform Udostępniania Wideo (VSP) wpisanych do wykazu Przewodniczącej KRRiT stan na 4 sierpnia 2025 r.*)

[698] C'est notamment le cas des dispositions relatives à la promotion des œuvres européennes et aux communications commerciales. L'accessibilité pour les personnes handicapées est garantie par l'obligation de proposer au moins 30 % du catalogue assorti de dispositifs adaptés.

[699] La loi sur la radiodiffusion, Article 18, paragraphes 4-6, *op. cit.*, élément 938.

[700] *Ibid.*, article 47*a* de la loi sur la radiodiffusion, élément 913.

[701] *Ibid.*, article 47*o*, paragraphe 1, point 1, et paragraphe 2, ainsi qu'article 47*p*, élément 1019.

de la violence gratuite, et les contenus « susceptibles de nuire au bon développement physique, mental ou moral des mineurs », dont l'incidence délétère n'est qu'une probabilité[702]. Les contenus appartenant à la première catégorie sont complètement interdits dans les programmes linéaires et prohibés à certaines conditions dans les services de VOD, dès lors qu'ils sont mis à disposition en l'absence de mesures techniques efficaces ou d'autres mesures adéquates pour empêcher les mineurs d'y accéder[703]. Les contenus relevant de la seconde catégorie ne peuvent être diffusés dans des services de programmes qu'entre 23 heures et 6 heures du matin, et doivent faire l'objet d'une classification et d'une signalétique adaptées, en fonction du préjudice qu'ils sont susceptibles de causer et du type de contenu préjudiciable[704] (violence, sexe, vulgarité, drogues) ; dans le cas des services de médias audiovisuels à la demande, ces contenus sont soumis aux mêmes règles de classification et à des exigences de signalétique similaires[705]. Une signalétique doit en outre accompagner les programmes radiodiffusés ou proposés à la demande, en fonction de leur degré de nocivité pour les mineurs appartenant à différentes tranches d'âge. Ces dernières sont définies et décrites dans les règles éditées par le KRRiT. Dans le cas des programmes linéaires, cinq catégories sont prévues (sans restriction, réservé aux plus de 7 ans, 12 ans, 16 ans et 18 ans), contre quatre pour les services de VOD (sans restriction, réservé aux plus de 12 ans, 16 ans et 18 ans). Dans les services de radio et de télévision, les programmes estampillés « convient aux mineurs de plus de 16 ans » ne peuvent être diffusés qu'après 20 heures.

En ce qui concerne les services de partage de vidéos, la loi sur la radiodiffusion évoque les contenus « préjudiciables au bon développement physique, mental ou moral des mineurs, en particulier ceux qui contiennent des éléments pornographiques ou mettent en scène de la violence gratuite ». La diffusion de contenus de ce type sans protections techniques efficaces est interdite. Les fournisseurs de VSP sont tenus de mettre en place des mesures techniques efficaces, notamment des systèmes de contrôle parental ou d'autres dispositifs adaptés, afin de protéger les mineurs contre l'accès aux contenus

[702] Cette distinction prend sa source dans des textes antérieurs : la Directive 89/552/CEE du Conseil, du 3 octobre 1989, visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à l'exercice d'activités de radiodiffusion télévisuelle (Directive Télévision sans frontières), ainsi que la Directive SMA avant sa modification par la directive 2018/1808.

[703] Ces protections et mesures ont été précisées par l'autorégulation, notamment le code de bonnes pratiques du 26 juin 2014, dans sa version modifiée en 2022, prévoyant des règles détaillées pour la protection des mineurs dans les services de médias audiovisuels à la demande. Ces protections et mesures recouvrent : a) un système permettant de conditionner l'accès au contenu à la fourniture des coordonnées de carte bancaire de l'utilisateur, à un paiement par carte de crédit, à un virement bancaire électronique ou à une solution équivalente (par exemple PayPal), à un paiement par ajout à la facture, à une connexion à un système bancaire en ligne permettant la vérification de l'âge ou à la confirmation de la majorité par un fournisseur d'identité électronique, et/ou à l'application d'un système technique de contrôle parental efficace ; b) un autre système conditionnant l'accès aux contenus à une vérification rigoureuse de la majorité (déclaré auprès d'IAB Polska). Lorsqu'il opte pour l'un de ces dispositifs, le fournisseur peut proposer un mode sécurisé (contrôle parental) au sein d'un service de VOD, qui soustrait à la vue les contenus inappropriés et ne peut être désactivé qu'au moyen d'un code PIN ou d'une mesure équivalente gérée par un utilisateur adulte.

[704] Les pictogrammes correspondants doivent être visibles pour les téléspectateurs pendant au moins cinq secondes avant le début de la diffusion et cinq secondes après chaque pause publicitaire ; à la radio, l'avertissement verbal prévu doit être donné avant le début de l'émission.

[705] Les règles concernant la durée d'affichage et l'emplacement des pictogrammes sont toutefois plus souples. L'utilisateur d'un service de VOD doit pouvoir identifier facilement le type de programme concerné au moment où il le choisit et pendant toute sa durée.

préjudiciables ; ils doivent de surcroît permettre aux utilisateurs d'appliquer une classification aux contenus qu'ils mettent en ligne et d'enclencher des mesures techniques de protection. Les règles du KRRiT précisent les conditions applicables à la classification et au marquage des contenus préjudiciables aux mineurs, en distinguant quatre tranches d'âge : sans restriction, 12+, 16+ et 18+. Elles caractérisent les différentes catégories et établissent les modèles de pictogrammes à utiliser pour les contenus convenant aux trois tranches d'âge supérieures[706]. Ainsi qu'on l'a déjà évoqué, les fournisseurs de VSP sont tenus de faire figurer dans leurs conditions générales ces exigences en matière de classification et de marquage, ainsi que les procédures de signalement des contenus préjudiciables aux mineurs.

6.2.3. Protection des mineurs au regard de l'accès aux contenus pornographiques – nouvelles initiatives

Le code pénal polonais[707] renferme des dispositions concernant la pornographie, qui sanctionnent notamment la présentation publique de ce type de contenus aux personnes qui ne souhaitent pas y être exposées et la diffusion de pornographie accessible aux mineurs de moins de 15 ans ; différentes dispositions concernent en outre la pornographie mettant en scène des mineurs, des animaux ou des actes de violence[708]. La notion de pornographie n'est cependant pas définie statutairement, mais plutôt interprétée au regard de la doctrine juridique et de la jurisprudence.

Face aux inquiétudes exprimées dernièrement au sujet de la protection des mineurs contre les préjudices en ligne, et en particulier contre la pornographie, des propositions législatives ont vu le jour, visant à restreindre l'accès des mineurs à ce type de contenus. Les statistiques existantes soulignent l'ampleur du problème : plus de 70 % des enfants et des adolescents estiment qu'il est facile d'accéder à de la pornographie ; l'âge moyen de la première exposition s'établit à 11 ans, tandis que 18,5 % des personnes interrogées déclarent avoir été confrontées à des contenus à caractère sexuel avant l'âge de 10 ans. Chez 80 % des enfants, en outre, les appareils mobiles ne sont pas équipés d'un logiciel de contrôle parental ; 54 % environ des adolescents déclarent que leurs parents ne leur imposent aucune règle en matière d'utilisation d'internet, tandis qu'ils sont environ 29 % à considérer que le contrôle parental sur les contenus et le temps passé devant les écrans est inefficace[709].

En mai 2023, déjà, le Gouvernement avait présenté un projet de loi relative à la protection des mineurs contre les contenus en ligne inappropriés[710], permettant aux abonnés aux services d'accès à internet de demander aux fournisseurs de ces derniers de

[706] Règlement du KRRiT du 13 avril 2022, *Dziennik Ustaw* de 2022, élément 1019.
[707] *Ustawa z dnia 6 czerwca 1997 r. Kodeks karny* (loi du 6 juin 1997), texte consolidé : *Dziennik Ustaw* de 2025, élément 383.
[708] Code pénal polonais, Article 202, paragraphe 1, article 200, paragraphes 3-6, et article 202, paragraphes 3-5.
[709] Exposé des motifs de la proposition de loi présentée par le ministère de la Numérisation – 29 août 2025, 3, fichier : *Projekt ustawy i uzasadnienie małoletni 29.08.2025 r.*.docx, pp. 13-14.
[710] *Sejm*, Projet gouvernemental du 19 mai 2023, (IXe législature), nº 3238.

limiter l'accès à la pornographie. Le projet avait été retiré avant les élections législatives de 2023. Début 2025, le ministère de la Numérisation a rendu public un projet de « loi relative à la protection des mineurs contre l'accès aux contenus préjudiciables en ligne » (ci-après le « projet ministériel ») et a engagé des consultations publiques[711]. Une initiative similaire, quoique limitée à la pornographie, avait été présentée auparavant au Sejm sous la forme d'un « projet citoyen[712] ». Le champ d'application du projet ministériel était initialement plus large, car il portait sur la pornographie et sur d'autres types de contenus préjudiciables, sans toutefois définir ces notions. En réponse aux critiques émises lors des consultations, la version modifiée du projet ministériel qui a vu le jour porte sur un périmètre plus restreint, centré sur la pornographie, et a été renommée en conséquence[713] ; toute référence aux autres contenus préjudiciables a été supprimée. Néanmoins, les rédacteurs du projet ont refusé d'accéder aux demandes visant à définir la pornographie, affirmant que cette notion était suffisamment claire dans la doctrine pénale et la jurisprudence, et qu'une définition inscrite dans la loi risquerait d'entraver une approche dynamique. Il est intéressant de noter que le projet citoyen soumis au Parlement comprenait, lui, une définition de la pornographie[714] reprenant les composantes de la notion de contenu « sexuellement explicite » détaillée dans le rapport explicatif de la Convention sur la cybercriminalité du Conseil de l'Europe[715].

Le dispositif de protection des mineurs proposé par le projet ministériel s'articule autour de trois grandes composantes : 1) l'obligation, pour les fournisseurs de services en ligne[716] permettant d'accéder à de la pornographie, de mettre en œuvre des mesures efficaces de vérification de l'âge, afin d'empêcher les mineurs d'accéder à ce type de contenu ; 2) la création d'un registre répertoriant les noms de domaine des services non conformes ; 3) l'obligation, pour les fournisseurs d'accès à internet, d'empêcher l'accès aux sites web utilisant les noms de domaine figurant dans ce registre.

L'obligation de mettre en œuvre des mesures efficaces de vérification de l'âge s'appliquerait à l'ensemble des fournisseurs de services fournis par des moyens

---

[711] *Projekt ustawy o ochronie małoletnich przed dostępem do treści szkodliwych w internecie* (Projet de loi relatif à la protection des mineurs contre l'accès aux contenus préjudiciables sur internet), présentant l'évolution du projet de loi du ministère de la Numérisation, avec l'exposé des motifs et l'analyse d'impact, ainsi que les contributions issues des consultations.

[712] Projet de loi citoyen relatif à la protection des mineurs contre l'accès aux contenus pornographiques en ligne, modifiant la loi sur les télécommunications. Ce projet a été présenté le 20 décembre 2024 par un comité regroupant des organisations conservatrices et opposées à l'avortement. L'article 118.2 de la Constitution octroie un droit d'initiative législative aux groupes composés d'au moins 100 000 citoyens.

[713] Projet de loi relatif à la protection des mineurs contre l'accès aux contenus pornographiques en ligne, 29 août 2025, rendu public le 1er septembre 2025.

[714] Article 2, point 3, du projet citoyen : « Contenu pornographique : contenu présentant sous une forme visuelle, quelle qu'elle soit, les éléments suivants, réels, simulés, créés et/ou retouchés : a) relations sexuelles – y compris génito-génitales, oro-génitales, ano-génitales ou oro-anales – entre personnes de sexes opposés ou du même sexe ; b) masturbation ; c) zoophilie ; d) pratiques sadomasochistes dans un contexte sexuel. »

[715] Conseil de l'Europe, *Rapport explicatif de la Convention sur la cybercriminalité*, point 100. Le ministère de la Numérisation prend acte de la définition du Conseil de l'Europe, mais la juge insuffisante, car elle n'intègre pas d'exigence relative à « l'intention de provoquer une excitation sexuelle », qui, de l'avis général, constitue un aspect essentiel de la notion de pornographie en droit pénal polonais.

[716] Le projet fait référence à la notion de fournisseur de services au sens de l'article 2, paragraphe 6, de l'UŚUDE, qui équivaut à la notion de fournisseur de services de la société de l'information dans la Directive sur le commerce électronique.

électroniques, terme utilisé dans la législation polonaise qui équivaut aux « fournisseurs de services de la société de l'information » dans les textes de l'Union européenne. Au cours des consultations, certaines contributions ont suggéré de restreindre le champ d'application du projet, par exemple en le limitant aux services pornographiques de grande envergure ou aux sites web dont une partie importante du contenu est de nature pornographique, ou ont encore proposé d'exempter certains fournisseurs, tels que les simples intermédiaires ou les microentreprises. Ces suggestions ont été rejetées par les rédacteurs du projet, au motif que l'adoption d'obligations variables en fonction du type de fournisseurs conduirait à une protection inégale des mineurs.

Les règles proposées sont destinées à couvrir un vaste champ territorial, puisqu'elles s'appliqueraient aux prestataires « fournissant des services en ligne à des destinataires sur le territoire polonais, quel que soit le lieu d'établissement ou d'activité professionnelle du prestataire ». Si l'argument du principe du pays d'origine, consacré par l'article 3 de la Directive sur le commerce électronique, a été soulevé lors des consultations, le projet n'évoque aucune exigence s'agissant des mesures dérogeant à ce principe en ce qui concerne les fournisseurs établis dans l'UE ou l'EEE[717]. L'exposé des motifs du projet précise que dans un souci d'efficacité, il est essentiel d'autoriser les actions à l'encontre des pages web basées hors de la Pologne et accessibles aux mineurs polonais, et invoque la « construction similaire » du DSA, applicable aux services intermédiaires proposés à des destinataires dans l'Union, quel que soit le lieu d'établissement du prestataire de services.

Le mécanisme de vérification de l'âge vise à établir avec certitude que le destinataire du service a atteint la majorité ; l'autodéclaration, les méthodes d'estimation de l'âge et les méthodes biométriques sont expressément exclues. Si le projet n'indique pas dans le détail les méthodes à utiliser, il définit les exigences auxquelles doit répondre le dispositif. En particulier, celui-ci doit garantir le plus haut degré de protection des données à caractère personnel et de la vie privée du destinataire ; au moins deux méthodes universellement accessibles et faciles à utiliser pour les destinataires doivent être proposées (dont une au moins adaptée aux personnes handicapées et/ou ne parlant pas polonais) ; la méthode retenue doit être disponible en permanence ; les données sur lesquelles elle repose doivent être fiables ; il ne doit pas être facile pour les utilisateurs de contourner la méthode de vérification ; enfin, dans la mesure du possible, l'une au moins des méthodes proposées doit être interopérable avec d'autres services en ligne. Les modalités de vérification de l'âge doivent en outre répondre aux critères correspondant à un niveau de garantie élevé pour un schéma d'identification électronique[718] ; de surcroît, si le traitement de données à caractère personnel est nécessaire, celui-ci doit être conforme au RGPD[719], en particulier au principe de minimisation des données ; les données collectées ne peuvent être utilisées qu'à des fins de vérification de l'âge et ne doivent pas servir à établir le profil des destinataires. Certaines de ces garanties en matière de protection des

[717] La Directive sur le commerce électronique, Article 3, paragraphes 4 et 5 ; l'UŚUDE, *op. cit.* Article 3b.
[718] Comme le prévoit l'article 8, paragraphe 2, point *c*), du Règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, *JOUE* L 257/73 du 28 août 2014.
[719] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données), *JOUE* L 119/1 du 4 mai 2016.

données ont été instaurées en réponse aux préoccupations exprimées lors des consultations sur le premier projet ministériel. L'exposé des motifs du projet se réfère aux travaux sur le portefeuille numérique européen, soulignant que ce dernier offrira une possibilité de vérification de l'âge sans qu'il soit nécessaire de fournir des informations supplémentaires[720].

Le registre des noms de domaine donnant accès à des contenus pornographiques sans vérification préalable de l'âge sera géré par le Réseau informatique scientifique et universitaire de l'Institut national de recherche (*Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy*), ou NASK[721]. Ce choix tient compte de l'expérience du NASK ainsi que de son expertise technologique, et plus particulièrement de son rôle actuel dans la gestion de la liste d'alerte des sites web dangereux[722]. Avant d'émettre une notification, le président de l'UKE doit en informer le titulaire du domaine (fournisseur de services), en lui accordant un délai de deux jours pour présenter ses commentaires. La notification doit également être communiquée au fournisseur de services, qui peut à tout moment s'opposer à son inscription sur cette liste[723]. Les objections doivent être examinées par le président de l'UKE dans un délai de 14 jours ; en cas de rejet, il reste possible de former un recours devant les tribunaux. Si l'objection est admise, le président doit demander au NASK de supprimer le domaine du registre sous trois jours. Les fournisseurs d'accès à internet sont tenus d'empêcher l'accès aux sites web utilisant les noms de domaine inscrits au registre, sans frais et dans les 48 heures suivant cette inscription. La mise en œuvre du blocage doit passer par la suppression des noms concernés du système de noms de domaine (DNS) et par une redirection des utilisateurs vers un site web de l'UKE affichant un message donné. Lorsqu'un nom de domaine est supprimé du registre, l'accès à celui-ci doit être rétabli sous 48 heures. Le registre, tenu informatiquement de façon à permettre le transfert automatique des données aux fournisseurs, ne sera pas public.

Le projet ministériel confère également au président de l'UKE des compétences lui permettant de vérifier le bon respect des obligations décrites ci-dessus par les fournisseurs de services en ligne et les fournisseurs d'accès à internet, mais aussi d'infliger des sanctions financières, d'émettre des recommandations a posteriori et d'adopter des décisions ordonnant de mettre fin aux irrégularités et précisant les mesures correctives à appliquer. Contrairement au projet citoyen et à la loi sur les jeux de hasard, qui prévoient des restrictions concernant les domaines répertoriés ne respectant pas les dispositions en vigueur relatives à la protection des mineurs, le projet ministériel ne propose pas d'interdire la fourniture de services de paiement sur les pages web répertoriées dans le registre des noms de domaine permettant l'accès à des contenus pornographiques sans vérification préalable de l'âge.

---

[720] Pour de plus amples informations sur le portefeuille numérique européen, voir le site web que lui consacre la Commission européenne.

[721] Organisme de recherche et de développement, opérateur de réseaux de données et opérateur de registre des noms de domaine de premier niveau national (.pl), partie intégrante du système national de cybersécurité.

[722] En vertu de la loi du 28 juillet 2023 relative à la lutte contre les abus dans les communications électroniques (*Ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej*), texte consolidé : *Dziennik Ustaw* de 2024, élément 1803.

[723] L'absence de date limite pour le dépôt de cette objection marque une différence avec la solution retenue concernant le registre des jeux de hasard, pour lesquels un délai de deux mois est prévu.

À la fin de l'année 2025, le projet de loi ministériel relatif à la protection des mineurs contre les contenus pornographiques en ligne n'en est qu'aux premières étapes de son élaboration. On ignore à ce stade si ce projet sera adopté, a fortiori à quelle échéance et sous quelle forme. Il ne fait aucun doute, en revanche, que l'adoption de la loi mettant en œuvre le DSA faciliterait l'examen d'autres initiatives portant sur la protection des mineurs. Les liens entre ces initiatives et les textes législatifs de l'Union européenne (DSA, Directive sur le commerce électronique et Directive SMA), ainsi que les dispositions du droit polonais qui les mettent en œuvre et développent ainsi la politique publique nationale dans les différents domaines concernés, demeurent une question complexe qui mériterait un examen plus approfondi.

6.3. L'exemple du Royaume-Uni

Dr Mariette Jones, Maître de conférences en droit, Université de Middlesex, London

6.3.1. Le cadre législatif national applicable aux plateformes prévu par la loi relative à la sécurité en ligne

Après près d'une décennie des travaux préparatoires, la loi britannique relative à la sécurité en ligne (*Online Safety Act* – OSA) est entrée en vigueur en septembre 2023[724]. À ce jour, la plupart de ses dispositions sont applicables et elle devrait être pleinement opérationnelle d'ici à 2026. L'OSA est une loi d'une ampleur considérable, tant par sa taille et le nombre de ses dispositions que par son champ d'application et ses objectifs affichés. Elle cherche à traiter la quasi-totalité des atteintes pouvant être commises en ligne ou via un support en ligne, et s'agissant des mineurs, elle ne se limite pas aux contenus illicites, mais réglemente également les contenus en ligne « licites mais préjudiciables ».

La principale caractéristique opérationnelle de l'OSA consiste à imposer aux entreprises privées de surveiller, d'évaluer et de supprimer activement les contenus créés par des tiers, et à rendre obligatoires les mesures visant à protéger les mineurs, notamment le renforcement de la vérification de l'âge. Par exemple, depuis le 25 juillet 2025, les services qui publient des contenus pornographiques doivent utiliser un « système de vérification de l'âge extrêmement efficace » afin d'empêcher les mineurs d'y accéder[725].

L'OSA s'applique à un large éventail de services entre utilisateurs, de moteurs de recherche et de fournisseurs de contenus accessibles aux utilisateurs britanniques, quel que soit le lieu où le service est établi. Elle couvre à la fois les « services d'utilisateur à

[724] Gouvernement britannique, loi relative à la sécurité en ligne de 2023.

[725] L'article 81 de l'OSA prévoit :

(2) L'obligation de s'assurer, par le biais d'une vérification ou d'une estimation de l'âge (ou les deux), que les enfants ne sont généralement pas en mesure d'accéder à des contenus pornographiques réglementés par le fournisseur dans le cadre du service. (3) La vérification ou l'estimation de l'âge doit être d'une nature et d'une utilisation qui permettent de déterminer de manière très efficace si un utilisateur donné est un enfant ou non.

utilisateur », y compris les plateformes sur lesquelles les utilisateurs peuvent télécharger et partager des contenus, comme *YouTube* ou *Facebook*, et les « services de recherche », qui incluent les moteurs de recherche tels que *Google*. Un service d'utilisateur à utilisateur est un service réglementé dès lors qu'il compte un nombre significatif d'utilisateurs au Royaume-Uni. À quelques exceptions près, comme les courriers électroniques et les services de messagerie, tous les contenus générés par les utilisateurs sur un service d'utilisateur à utilisateur réglementé sont eux-mêmes réglementés.

L'OSA impose des obligations supplémentaires à différentes catégories de services. Les obligations et les mesures de surveillance les plus rigoureuses s'appliquent aux services de « catégorie 1 ». Lorsque l'OSA a été instaurée, elle comportait des dispositions distinctes visant à protéger les adultes contre les contenus « licites mais préjudiciables ». Bien que ces dispositions aient été supprimées, elles ont été remplacées par les obligations qui s'appliquent aux fournisseurs de catégorie 1. Les fournisseurs de catégorie 1 sont ceux qui comptent en moyenne plus de 34 millions d'utilisateurs mensuels au Royaume-Uni et qui utilisent un système de recommandation de contenus, ou ceux qui comptent plus de 7 millions d'utilisateurs mensuels au Royaume-Uni, utilisent un système de recommandation de contenus et offrent aux utilisateurs la possibilité de transférer ou de partager avec d'autres utilisateurs du service des contenus réglementés générés par les internautes[726]. Les services susceptibles d'être consultés par des mineurs sont soumis à des obligations supplémentaires plus contraignantes.

L'OSA distingue les principales catégories suivantes de contenus préjudiciables : tout d'abord, les contenus illicites tels que le terrorisme, l'exploitation et les abus sexuels envers des mineurs, les discours de haine et l'escroquerie. Ensuite, viennent les contenus préjudiciables aux mineurs, qui sont subdivisés en contenus à priorité absolue, comme la pornographie ou les contenus incitant au suicide, à l'automutilation ou aux troubles du comportement alimentaire, et en contenus prioritaires, comme le harcèlement, l'incitation à la haine ou à participer à des activités dangereuses, ainsi qu'en contenus non spécifiés qui présentent néanmoins des risques sérieux de graves préjudices.

Le régime en vigueur n'est pas le traditionnel système de « notification et de retrait » (*notice-and-takedown*) que l'on retrouve dans d'autres législations et juridictions, mais plutôt une obligation préventive d'identifier et de supprimer certains contenus. L'OSA impose une série d'obligations à l'ensemble des services réglementés de type « utilisateur à utilisateur ». Il s'agit notamment de l'obligation d'évaluer, d'atténuer et de gérer les risques posés par certains types de contenus illicites, de permettre aux utilisateurs de signaler les contenus illicites, de mettre en place une procédure de plainte et de tenir compte de la liberté d'expression et du respect de la vie privée lors de la mise en œuvre des mesures et politiques de sécurité.

Comme nous l'avons mentionné, les fournisseurs de catégorie 1 ont des obligations plus contraignantes, à savoir (1) permettre aux utilisateurs de choisir de vérifier leur identité et le type de contenus qu'ils consultent, y compris s'ils souhaitent voir les contenus d'utilisateurs qui n'ont pas confirmé leur identité ; (2) protéger la liberté d'expression ; (3) protéger les utilisateurs contre les publicités mensongères ; (4) garantir le respect des conditions d'utilisation du service (y compris le fait que le fournisseur de services supprime

[726] Règlement 3 de l'OSA (critères de seuil des catégories 1, 2A et 2B) de 2025.

les contenus générés par les utilisateurs si, et seulement si, ces contenus ne respectent pas les conditions d'utilisation ; (5) publier un « rapport de transparence » annuel à l'Ofcom[727] (voir ci-dessous, point 6.1.3.4) dans lequel figurent les informations requises par l'Ofcom ; et (6) diverses obligations supplémentaires, notamment établir une synthèse de la dernière évaluation des risques liés aux contenus illégaux et des risques pour les enfants, ainsi que prévoir une procédure de traitement des plaintes.

En résumé, l'OSA impose une obligation de vigilance similaire à celle prévue par la législation en matière de responsabilité civile ou de santé et de sécurité. Les plateformes doivent désormais prendre les mesures nécessaires pour empêcher la publication de contenus illicites et, lorsqu'ils ont été publiés, les supprimer ou en désactiver l'accès. Cette obligation s'applique notamment aux contenus déjà reconnus comme illicites par la législation britannique, par exemple les contenus liés au terrorisme, les contenus pédopornographiques, les incitations à la haine et les escroqueries, notamment. En ce qui concerne les mineurs, cette obligation s'étend aux contenus licites qui sont susceptibles de leur être préjudiciables (voir ci-dessous le point 6.3.2). Outre cette obligation de modération des contenus, les fournisseurs de services et les plateformes sont également tenus de procéder à des évaluations des risques et de mettre en place des mesures d'atténuation appropriées, ainsi que de respecter leurs obligations en matière de signalement et de conception des plateformes.

Afin de faire respecter ces nouvelles exigences, l'OSA confère de nouveaux pouvoirs étendus à l'Ofcom, l'organisme réglementaire indépendant qui supervise le secteur des communications au Royaume-Uni. Elle désigne également l'Ofcom comme l'autorité indépendante chargée de la sécurité en ligne, dont le rôle consiste notamment à superviser et à contrôler l'application de ce nouveau régime réglementaire[728].

Ces codes comprennent, notamment, des éléments d'orientation sur les options de configuration des plateformes, les algorithmes de recommandation, la modération des contenus, la surveillance et la gouvernance, les outils de signalement et de traitement des plaintes, le contrôle parental, l'évaluation de la conformité et des enquêtes en cas de manquements, l'application des obligations et l'imposition de sanctions[729]. Les sanctions encourues peuvent être extrêmement sévères, avec des amendes pouvant atteindre 18 millions GBP ou 10 % du chiffre d'affaires mondial, ainsi que le blocage des services concernés[730].

[727] L'Ofcom (*Office of Communications*) est l'autorité britannique de régulation des services de communication.
[728] Gouvernement britannique, loi relative à la sécurité en ligne de 2023, partie 7.
[729] Gouvernement britannique, ministère des Sciences, de l'Innovation et des Technologies, *Online Safety Act: Protection of Children Codes of Practice – explanatory memorandum – GOV.UK*, (loi relative à la sécurité en ligne : codes de bonnes pratiques pour la protection des mineurs – exposé des motifs), en anglais, 24 avril 2025.
[730] Annexe 13 de l'OSA ; règlement d'application de l'OSA (recettes mondiales admissibles) 2025/1032.

6.3.2. Les dispositions spécifiques en matière de protection des mineurs

Les mineurs sont réputés être des utilisateurs particulièrement vulnérables en ligne, davantage susceptibles d'être victimes d'exploitation, de manipulation et de préjudice psychologique. L'OSA vise donc à renforcer la protection des mineurs en ligne[731], en adoptant une philosophie de « sécurité dès la conception » (*safety-by-design*)[732] qui impose aux plateformes de protéger de manière proactive les utilisateurs âgés de moins de 18 ans[733]. Elle oblige les plateformes susceptibles d'être consultées par des mineurs à mettre en œuvre des évaluations des risques pour la sécurité des mineurs et à prendre des mesures préventives pour éviter tout préjudice[734]. L'article 37 de l'OSA étend considérablement le champ d'application de la loi en définissant explicitement l'expression « susceptible d'être consultée par des mineurs » comme toute situation dans laquelle « il est possible que des mineurs puissent accéder au service ou à une partie de celui-ci ».

L'obligation d'empêcher tout préjudice s'étend non seulement à la protection contre les contenus illicites tels que les contenus à caractère pédopornographique, mais aussi à la protection contre les contenus licites susceptibles d'être préjudiciables, comme les contenus incitant à l'automutilation, au suicide ou aux troubles du comportement alimentaire, ou encore la pornographie[735]. Ces mesures consistent notamment à mettre en place des contrôles stricts de l'âge des utilisateurs grâce à des technologies de vérification adaptées, à configurer des algorithmes de manière à empêcher que des contenus préjudiciables puissent être recommandés à des mineurs, à prendre en compte les mineurs lors de la configuration des fonctionnalités d'autorisation pour les discussions de groupe ou l'ajout automatique, et à empêcher les contacts non sollicités, tels que les messages directs envoyés à des mineurs par des inconnus[736].

Concernant la vérification de l'âge, l'OSA exige plus qu'une simple déclaration sur l'honneur : des méthodes telles que la reconnaissance faciale ou la vérification d'identité doivent être utilisées[737]. Il sera probablement difficile de concilier cette obligation avec les différentes lois sur la protection de la vie privée et des données, qui sont elles aussi conçues pour protéger davantage les mineurs que les adultes. Les exigences en matière de gouvernance prévoient notamment la nomination de cadres supérieurs responsables des questions de conformité. Il convient de mettre en place des procédures de signalement clairement définies, ainsi que des politiques en matière de contenus et des technologies permettant de repérer les contenus préjudiciables. Les mineurs et leurs tuteurs doivent avoir accès à des systèmes transparents de signalement et de traitement des plaintes. L'OSA

---

[731] *Ibid*., article 1(3)(*b*)(i).
[732] *Ibid*., article 1(3)(*a*).
[733] Ces obligations sont présentées dans les parties 11 « Obligations en matière d'évaluation des risques pour les mineurs », 12 « Obligations en matière de sécurité pour la protection des mineurs » et 13 « Obligations en matière de sécurité pour la protection des mineurs : interprétation » de l'OSA, *op. cit.*
[734] *Ibid*., parties 35, 36 et 37.
[735] *Ibid*., article 61.
[736] *Ibid*., parties 11, 12 et 13, ainsi que les obligations correspondantes imposées aux moteurs de recherche dans les parties 28, 29 et 30.
[737] Ofcom, *Age Assurance and Children's Access Statement* (Déclaration relative à la vérification de l'âge et à l'accès des mineurs, 16 janvier 2025, en anglais.

demande également aux plateformes de procéder régulièrement à des évaluations des risques pour les mineurs et de communiquer publiquement les conclusions de ces évaluations[738].

6.3.3. Les jeux d'argent et de hasard en ligne, les mineurs et la loi relative à la sécurité en ligne

L'OSA a défini de nouvelles infractions, comme le « *cyberflashing* »[739], et regroupe sous une même bannière les dispositions pénales en vigueur dès lors qu'elles concernent des actes commis ou facilités en ligne. En outre, l'un des aspects les plus importants de l'OSA est l'imposition d'obligations légales relatives aux contenus qui sont licites, mais qui peuvent s'avérer préjudiciables aux mineurs, comme nous l'avons vu plus haut. La combinaison des dispositions légales et des infractions pénales existantes, ainsi que la manière dont la loi s'étend et s'applique aux mineurs, sont illustrées par son effet sur le régime juridique britannique en matière de jeux d'argent et de hasard.

La loi britannique de 2005 relative aux jeux d'argent et de hasard (*Gambling Act 2005*)[740] est la principale loi en la matière au Royaume-Uni. L'un de ses trois objectifs concernant l'octroi de licences est de protéger les mineurs et autres personnes vulnérables de tout préjudice ou exploitation liés aux jeux d'argent et de hasard. Cette loi érige en infraction le fait d'inviter, d'inciter ou d'autoriser toute personne âgée de moins de 18 ans à participer à des jeux d'argent, et elle prévoit un système de vérification de l'âge et d'octroi de licences qui garantit que seules les personnes âgées de plus de 18 ans peuvent miser en ligne ; il revient aux opérateurs titulaires d'une licence de vérifier l'identité et l'âge des joueurs. La publicité en faveur des jeux d'argent et de hasard est réglementée par des normes établies par un organisme indépendant : la Commission des pratiques publicitaires (*Committee of Advertising Practice* - CAP) de l'Autorité des normes publicitaires (*Advertising Standard Authority* - ASA). Les normes établies par la CAP, ainsi que la réglementation prévue par la loi relative aux jeux d'argent et de hasard et la loi relative aux jeux d'argent et de hasard (licences et publicité) de 2014[741], interdisent toute publicité destinée aux mineurs ou qui les attire fortement, et précisent que les personnes qui semblent avoir moins de 25 ans ne doivent pas figurer dans la plupart des publicités en faveur des jeux d'argent et de hasard.

La manière dont l'OSA complète la législation britannique existante illustre parfaitement cette approche. Elle renforce la protection existante des mineurs en étendant les responsabilités et les mandats aux plateformes qui hébergent ou font la promotion de contenus relatifs aux jeux d'argent et de hasard. Par exemple, les dispositions de la loi

[738] *Ibid*., partie 36.
[739] Service des poursuites pénales de la Couronne, « *Prison sentence in first cyberflashing case* » (Condamnation à une peine de prison dans la première affaire de *cyberflashing*), 19 mars 2024.
[740] Gouvernement britannique, loi britannique relative aux jeux d'argent et de hasard de 2005 (*Gambling Act 2005*).
[741] Gouvernement britannique, loi relative aux jeux d'argent et de hasard (licences et publicité) de 2014 (*Gambling (Licensing and Advertising) Act 2014*).

relative aux jeux d'argent et de hasard qui interdisent aux mineurs de jouer et obligent les opérateurs agréés à vérifier l'âge des joueurs s'étendent désormais aux plateformes de réseaux sociaux, aux moteurs de recherche et aux plateformes de diffusion en continu (*streaming*). Chargée d'appliquer les codes publicitaires[742] prévus par la loi britannique relative aux jeux d'argent et de hasard, l'ASA a interdit en 2023 plusieurs publicités en faveur de ces jeux qui utilisaient des dessins animés et des bandes dessinées susceptibles d'attirer les enfants[743]. Ces publicités ont été jugées contraires à l'article 16 du Code de la publicité non audiovisuelle et du marketing direct et promotionnel (Code CAP)[744], qui précise que les annonceurs ne doivent pas exploiter les jeunes ou les personnes vulnérables. L'ASA a également interdit les publicités dans lesquelles des footballeurs de haut niveau faisaient la promotion de plateformes de jeux d'argent, ces publicités étant jugées particulièrement séduisantes pour les mineurs[745]. Ainsi, alors que la législation en vigueur appliquait une approche réactive, qui consistait notamment à évaluer les publicités comme indiqué ci-dessus, l'entrée en vigueur de l'OSA signifie désormais que ces entités doivent prendre des mesures préventives pour empêcher que des mineurs soient exposés à des publicités et à des contenus faisant la promotion de jeux d'argent et de hasard.

En outre, alors que jusqu'à présent, la responsabilité potentielle de la promotion des sites web de jeux d'argent et de hasard incombait principalement aux sites web eux-mêmes ou à leurs promoteurs, comme les influenceurs sur des plateformes telles que YouTube, l'OSA étend effectivement la potentielle responsabilité aux plateformes elles-mêmes, qui hébergent les sites web, les influenceurs et les promoteurs.

Il convient également de mentionner les éléments des jeux en ligne qui imitent les mécanismes des jeux d'argent en encourageant les enfants à dépenser de l'argent pour obtenir des récompenses aléatoires, comme l'inclusion de « *loot boxes* » (boîtes à butin) dans les jeux en ligne. Ces boîtes renferment des objets aléatoires dont le joueur ne connaît pas le contenu avant de les avoir ouvertes. Les joueurs peuvent généralement acheter ces boîtes avec de l'argent (y compris avec des monnaies virtuelles) ou y accéder en jouant. Le fait que ces dispositifs puissent être préjudiciables aux enfants a suscité de nombreuses inquiétudes, dans la mesure où ils pourraient, par exemple, favoriser la dépendance au jeu[746]. La loi britannique de 2005 relative aux jeux d'argent et de hasard ne considère pas ces *loot boxes* comme des jeux d'argent et, après de longues consultations, le Gouvernement britannique a refusé de légiférer à leur sujet, préconisant plutôt une

---

[742] *Code of Non-broadcast Advertising and Direct and Promotional Marketing (CAP Code)* (Code de la publicité non audiovisuelle et du marketing direct et promotionnel (Code CAP)), en anglais ; *Code of Broadcast Advertising (BCAP Code)* (Code de la publicité audiovisuelle (Code BCAP)), en anglais.

[743] Voir par exemple ASA, *« ASA Ruling on Buzz Group Ltd. »*, réclamation n° A23-1217474 *Buzz Group Ltd*, communiqué de presse, 3 janvier 2024.

[744] *Code of Non-broadcast Advertising and Direct and Promotional Marketing (CAP Code)* (Code de la publicité non audiovisuelle et du marketing direct et promotionnel (Code CAP)), en anglais

[745] Pour des cas particuliers, voir ASA, « *Gambling, betting and gaming: Appeal to children – ASA | CAP* », 9 mai 2023. Ainsi que ASA, *« ASA Ruling on LC International Ltd t/a Ladbrokes »*, réclamation n° A22-1171467 *Ladbrokes Betting Gaming Ltd*, communiqué de presse, 21 décembre 2022.

[746] D. Zendle et autres (2020), « *Paying for loot boxes is linked to problem gambling, regardless of specific features like cash-out and pay-to-win* », *Computers in Human Behavior,* 102, pp. 181-191, cité avec l'accord du gouvernement britannique, ministère de la Culture, des Médias et des Sports : *Government response to the call for evidence on loot boxes in video games – GOV.UK*, 18 juillet 2022.

autorégulation du secteur afin de minimiser les risques en 2023[747]. Il est toutefois intéressant de noter qu'il a pris en compte les préoccupations formulées, notamment celles de la Commission britannique des jeux d'argent et de hasard, quant aux risques potentiels pour les mineurs et les joueurs vulnérables. En imposant une obligation concrète de prévention des contenus licites mais potentiellement préjudiciables aux mineurs, l'OSA a désormais transformé l'autorégulation du secteur en réglementation juridiquement contraignante.

Au vu de l'ensemble des éléments évoqués ci-dessus, l'OSA se révèle particulièrement ambitieuse en termes de champ d'application, d'objectifs et de fonctionnement, ce qui pose un certain nombre de défis à bien des égards. Pour ne citer qu'un exemple, l'obligation « extrêmement efficace » de vérification de l'âge, qui pourrait impliquer une vérification biométrique ou par documents d'identité, risque de contrevenir aux dispositions relatives à la protection de la vie privée et des données à caractère personnel et soulève des interrogations quant à l'inclusivité pour les mineurs ne disposant pas d'une pièce d'identité officielle, sans parler des difficultés techniques liées à la mise en œuvre de systèmes de vérification fiables mais non intrusifs, en particulier pour les fournisseurs de services de petite taille.

L'Ofcom, en sa qualité d'autorité de régulation compétente, ainsi que les entités réglementées par l'OSA, sont confrontés à des obligations contraignantes et exigeantes qui, à bien des égards, ne sont pas encore clairement définies. Ces obligations ne seront précisées qu'après avoir été examinées par les tribunaux et devront probablement faire l'objet de nouveaux règlements ou codes de bonnes pratiques supplémentaires. L'encyclopédie en ligne Wikipédia a récemment lancé le premier test juridique du nouveau régime en contestant la manière dont l'Ofcom a défini les services de catégorie 1 dans le règlement 3 de l'OSA[748]. Elle a contesté le fait qu'en tant qu'organisation caritative à but non lucratif, elle soit placée dans la même catégorie que de grandes multinationales telles que *Google* ou *Facebook*. Dans son arrêt rendu en août 2025, la Haute Cour d'Angleterre et du Pays de Galles a autorisé le réexamen judiciaire de deux aspects du processus décisionnel de l'Ofcom, mais a rejeté de manière catégorique les deux recours de Wikipédia basés sur les droits de l'homme[749]. L'affaire peut encore faire l'objet d'un appel, et il est fort probable que la législation et les règlements connexes seront à nouveau examinés par les tribunaux, puisqu'ils pourraient avoir un impact significatif sur des aspects du droit tels que la liberté d'expression et le respect de la vie privée, ainsi que sur l'économie numérique et l'économie au sens large du Royaume-Uni.

[747] Ministère britannique de la Culture, des Médias et des Sports, *Loot boxes in video games: update on improvements to industry-led protections – GOV.UK*, 18 juillet 2023.
[748] *Wikimedia Foundation (a charitable foundation registered in the United States of America), BLN c. Secretary of State for Science, Innovation and Technology* [2025] EWHC 2086 (Admin).
[749] *Ibid.*, paragraphes 133 à 137.

7. Analyse comparative

Dr Mark Cole, directeur des affaires académiques de l'Institut européen du droit des médias (EMR) et professeur en droit des médias et des télécommunications à l'université du Luxembourg, et Sandra Schmitz-Berndt, chercheuse associée à l'Institut européen du droit des médias (EMR)

Même si un cadre international commun en matière de droits fondamentaux et, dans la plupart des pays mentionnés dans cette publication, un cadre législatif européen commun ont été mis en place, les rapports nationaux révèlent qu'il existe en Europe d'importantes disparités dans la manière dont la législation s'applique aux intermédiaires d'internet.

Une compréhension globale des défis liés à l'application des réglementations en vigueur contre les contenus illicites et la désinformation en Europe suppose d'établir une analyse comparative des obligations légales nationales, des mécanismes de sanction et des solutions mises en place par chaque pays. Bien que la législation de l'UE – principalement à travers les récents ajouts au « corpus réglementaire numérique » (« *digital rulebook* ») – ait conduit à une harmonisation substantielle directement contraignante pour ses seuls États membres, des pays tiers comme la Türkiye s'efforcent également de conformer leurs réglementations aux normes de l'Union européenne.

En mettant l'accent sur l'application de la législation, la présente analyse traitera uniquement des différences nationales en matière de définition des contenus illicites, en particulier dans le droit pénal national. Aucune véritable « européanisation » du droit pénal ne s'est encore concrétisée en dehors de la juridiction de l'UE et, au sein de l'Union européenne, l'harmonisation se limite jusqu'à présent aux délits particulièrement graves qui revêtent une dimension transfrontalière au sens du Traité de Lisbonne et à la coopération policière et judiciaire dans le cadre du TFUE. Cette harmonisation concerne par ailleurs certains comportements qui menacent les valeurs fondamentales de l'Union européenne, notamment ceux mentionnés dans la directive relative à la lutte contre la violence à l'égard des femmes et la violence domestique[750]. Il est en revanche particulièrement intéressant d'observer les différentes approches nationales lorsqu'il s'agit de contenus qui ne sont pas illicites en soi, mais qui sont réputés avoir des effets préjudiciables, à l'instar de la très controversée question de la réponse à apporter aux campagnes de désinformation. Cet aspect constitue donc le point de départ de l'analyse proposée ci-dessous, qui se concentrera ensuite sur les différentes stratégies nationales de lutte contre les contenus illicites, avant d'aborder, dans la dernière partie, d'autres dispositions en matière de contenus préjudiciables.

[750] Directive (UE) 2024/1385 du Parlement européen et du Conseil du 14 mai 2024 sur la lutte contre la violence à l'égard des femmes et la violence domestique [2024] *JOUE* L 2024/1385.

7.1. L'application des dispositions visant à lutter contre la désinformation

Le phénomène de la désinformation en Europe a été perçu comme un défi majeur et a été associé à des problématiques plus générales telles que la diffusion d'informations sur des questions de santé, les « théories du complot » ou les influences politiques étrangères. La désinformation constitue désormais un risque systémique dans l'environnement en ligne, et fait l'objet de mesures à la fois volontaires et réglementaires, qui visent en particulier les campagnes de manipulation de l'information et d'influence étrangères – FIMI (*Foreign Interference in Member States' Internal Affairs*) et les ingérences électorales. L'Union européenne a donc progressivement abandonné les mesures non contraignantes, telles que le code de bonnes pratiques sur la désinformation de 2018, au profit d'obligations contraignantes prévues par le DSA, ce qui lui a permis de renforcer son action contre la désinformation par une combinaison d'autorégulation, de coordination renforcée et d'amélioration de la détection des risques. Cette stratégie est également renforcée par le règlement sur la transparence et le ciblage de la publicité à caractère politique (TTPAR) et l'EMFA, qui abordent des questions telles que le financement étranger des publicités à caractère politique et les services de médias malhonnêtes. Compte tenu du rôle essentiel des très grandes plateformes en ligne et des très grands moteurs de recherche en ligne (VLOPSE) dans l'accès à l'information, les engagements en matière d'autorégulation s'accompagnent de nouvelles obligations de diligence raisonnable pour les fournisseurs de VLOPSE. Afin de lutter contre la désinformation au moyen de mesures coercitives, le DSA prévoit un dispositif hybride dans lequel la Commission européenne et les États membres de l'UE agissent en tant que corégulateurs, qui s'ajoute au rôle des intermédiaires eux-mêmes. Les autorités nationales compétentes sont chargées de la surveillance et de l'application du DSA dans les domaines qui ne sont pas expressément délégués à d'autres autorités désignées, ce qui signifie que les autorités nationales appliquent la réglementation relative aux fournisseurs de services intermédiaires établis sur leur territoire. La Commission européenne est essentiellement responsable de la surveillance et de l'application de la réglementation relative aux VLOPSE. Cette double approche en matière d'application de la réglementation s'illustre dans le rapport. national roumain, qui analyse notamment l'affaire TikTok.

La Roumanie, dont la population utilise très massivement des plateformes telles que Facebook, WhatsApp, YouTube et TikTok comme sources d'information – un phénomène comparable à celui observé dans d'autres États membres – et dont le niveau de culture numérique reste faible, constitue un environnement particulièrement vulnérable à la désinformation. Il est ainsi apparu que la population roumaine était particulièrement exposée aux campagnes de désinformation ayant une incidence sur l'opinion publique et les processus démocratiques. Ce risque s'est matérialisé avant les élections présidentielles de 2024, alors que le DSA était déjà pleinement en vigueur. L'exemple roumain met en évidence les limites du DSA, qui se concentre davantage sur la mise en place de mécanismes que sur un ensemble de mesures définitives permettant de lutter contre le risque systémique de désinformation et d'ingérence électorale et d'en limiter les effets. Cette faille a été en partie comblée par le Code de bonnes pratiques renforcé sur la désinformation, qui était initialement volontaire mais qui a désormais été intégré dans le dispositif du DSA comme Code de conduite sur la désinformation. Cette intégration au DSA

en février 2025 permettra au code de fournir des éléments d'orientation aux VLOPSE pour les accompagner dans le respect de leurs obligations en matière de risques systémiques.

Au-delà du processus électoral national roumain, la Commission européenne avait déjà engagé une procédure d'application des dispositions du DSA. À l'occasion des élections roumaines, la Commission a ensuite émis une ordonnance conservatoire à l'encontre de TikTok afin de bloquer et de conserver les données relatives aux risques systémiques réels et prévisibles que ce service était susceptible de faire peser sur les processus électoraux et sur le débat public dans l'Union européenne. Les conclusions préliminaires de l'enquête de la Commission européenne ont confirmé que TikTok avait enfreint plusieurs dispositions du DSA en matière de diligence raisonnable, notamment sur la méthode de ciblage du public et le recours au parrainage de publicités à caractère politique[751]. Ces questions peuvent désormais être examinées dans le cadre du règlement sur la transparence et le ciblage de la publicité à caractère politique, ce qui implique qu'une réponse nationale pour protéger l'intégrité du processus électoral, comme celle apportée par la Roumanie sous la forme de l'ordonnance nationale d'urgence n° 1/2025, ne serait plus nécessaire. La possibilité de se fonder sur un cadre juridique général garantirait également une plus grande transparence par rapport à une mesure d'urgence prise par l'exécutif.

Parallèlement à ces démarches au niveau européen et national, des mesures politiques ont été adoptées en vue des élections qui ont été organisées à nouveau après avoir été annulées en raison d'influences extérieures. Ces mesures politiques ont pu bénéficier des mécanismes de coopération renforcés mis en place par les différentes parties du nouveau cadre législatif européen en matière de numérique. Une table ronde a ainsi été organisée avec les VLOPSE, le coordinateur roumain des services numériques (ANCOM), les autorités publiques compétentes et les organisations de la société civile afin de recueillir des informations et de garantir la bonne préparation des élections roumaines en cours[752]. Compte tenu de la durée de la procédure officielle engagée par la Commission européenne, il était tout à fait compréhensible que le législateur national cherche à remédier aux lacunes constatées par des mesures nationales. Toutefois, au vu de la décision rendue par la Cour de justice de l'Union européenne au sujet de la loi autrichienne relative aux plateformes de communications, qui a été invalidée pour non-respect du principe du pays d'origine prévu par la Directive sur le commerce électronique, il n'est pas certain qu'une législation telle que celle qui a été proposée, mais pas encore définitivement approuvée, en Roumanie soit considérée comme compatible avec la législation européenne secondaire pertinente. La proposition roumaine obligerait *notamment* les plateformes à limiter la diffusion de contenus potentiellement préjudiciables à un maximum de 150 utilisateurs et à supprimer les contenus illicites dans un délai de 15 minutes après leur publication, sur la base d'une classification automatisée.

---

[751] Commission européenne, « La Commission estime à titre préliminaire que le registre des annonces publicitaires de TikTok ne respecte pas le Règlement sur les services numériques », communiqué de presse, 15 mai 2025. Il convient par ailleurs de mentionner la décision de la Commission européenne d'accepter les engagements pris par TikTok au sujet des problématiques publicitaires identifiées et de clore cette partie de l'enquête, « La Commission accepte les engagements pris par TikTok sur la transparence en matière de publicité au titre du Règlement sur les services numériques », communiqué de presse, 5 décembre 2025.

[752] Commission européenne, « La Commission, les plateformes en ligne et la société civile renforcent leur contrôle durant les élections roumaines », communiqué de presse, 5 décembre 2024.

L'exemple de la France dans ce contexte illustre la manière dont les mesures réglementaires et les politiques nationales permettent de renforcer la lutte contre la désinformation. Contrairement au projet de loi roumain, la démarche française n'interfère pas avec la réglementation harmonisée de l'Union européenne relative aux plateformes, mais met plutôt l'accent, au niveau national, sur la lutte contre la désinformation à travers un cadre législatif sur l'identification algorithmique de ce type de contenus, contribuant ainsi indirectement à l'application des dispositions du DSA. La mission de l'organisme spécialisé VIGINUM, qui surveille, détecte et analyse les FIMI, et surtout identifie et répertorie les techniques utilisées et les acteurs à l'origine des menaces afin d'améliorer la vigilance et la sensibilisation du public, constitue un outil essentiel pour parvenir à cet objectif. En l'absence de mandat officiel lui permettant de faire respecter la réglementation visant à lutter contre les fausses informations, le rôle de VIGINUM reste purement consultatif. La priorité que la France accorde aux actions de sensibilisation transparaît également dans d'autres mesures, telles que l'amélioration des compétences en matière d'information dans les établissements scolaires. La France met un point d'honneur à répondre aux risques posés par les FIMI, comme en témoignent non seulement les missions de VIGINUM, mais également la loi Léotard qui habilite *notamment* l'Arcom à prendre des mesures à l'encontre des services de communications audiovisuelles qui sont contrôlés ou influencés par un État étranger et qui diffusent intentionnellement de fausses informations, en particulier dans les trois mois précédant une élection.

Bien que le cadre général applicable à la France et à la Roumanie, ainsi qu'à tous les autres États membres de l'Union européenne, ait été largement harmonisé grâce à la réglementation européenne en vigueur, il est intéressant de le comparer à celui d'un pays non-membre de l'UE/EEE, mais signataire de la Convention européenne des droits de l'homme. L'Ukraine constitue à cet égard un exemple particulièrement éloquent, puisqu'elle est exposée depuis plus de dix ans à des campagnes massives de FIMI menées par un acteur hostile. La législation ukrainienne ne réglemente pas les plateformes en ligne, mais uniquement les plateformes de partage de vidéos qui relèvent de sa compétence en vertu de la loi ukrainienne relative aux médias. Pour ce qui est des plateformes en général, seules des solutions non contraignantes telles que des mémorandums ou des accords de coopération sont actuellement prévues. Cette lacune réglementaire est jugée préoccupante compte tenu des campagnes de propagande à grande échelle menées par la Russie et de la dépendance croissante de la population à l'égard des réseaux sociaux pour s'informer, lesquels sont également utilisés pour diffuser de la désinformation. Toutefois, depuis l'instauration de la loi martiale en 2022, laquelle permet notamment de restreindre la liberté d'expression, il est désormais possible de bloquer temporairement l'accès aux services de médias audiovisuels à la demande et aux services des fournisseurs de services audiovisuels de l'État agresseur sur le territoire ukrainien. Les plateformes de partage de vidéos sont par ailleurs contraintes d'interdire temporairement la diffusion de toute désinformation en lien avec l'agression armée contre l'Ukraine.

L'absence de mécanismes efficaces permettant à l'État de faire pression sur les plateformes en ligne étrangères afin de protéger ses intérêts nationaux a conduit au blocage de sites web et de plateformes en ligne en vertu de la loi ukrainienne relative aux sanctions et, à la suite de l'invasion massive de l'Ukraine par la Russie, également sur ordre spécifique du Centre national de gestion opérationnelle et technique des réseaux de télécommunications. Ces mesures de blocage restent controversées, faute d'un cadre

spécifique sur les conditions dans lesquelles elles doivent être appliquées. Le blocage de ces services est également possible au titre de la loi martiale. Cependant, ces mesures sont étroitement liées à la protection des intérêts nationaux et doivent à ce titre être considérées comme une *solution de dernier recours* (*ultima ratio*), en l'absence d'un cadre réglementaire plus général applicable aux plateformes en ligne. À l'instar de la France, l'Ukraine recourt également à des mesures de contrôle préventif en cherchant à renforcer l'éducation aux médias et les campagnes de sensibilisation, notamment sur la manière d'identifier la désinformation et en particulier la FIMI.

7.2. L'application des dispositions relatives à la lutte contre les contenus à caractère terroriste

Face aux contenus à caractère terroriste en ligne, l'Union européenne combine une réglementation contraignante et une coopération volontaire des intermédiaires, qui instaurent toutes deux des obligations spécifiques aux plateformes en matière de lutte contre ces contenus.

La Directive SMA impose aux États membres de l'Union européenne l'obligation de veiller, par des moyens appropriés, à ce que les services proposés par les fournisseurs de services de médias audiovisuels et les fournisseurs de plateformes de partage de vidéos qui relèvent de leur compétence ne comportent aucun contenu incitant publiquement à commettre des infractions terroristes[753]. En juin 2022, le règlement relatif à la diffusion de contenus terroristes en ligne (*Terrorist Content Online Regulation* – TCOR) a instauré un ensemble de dispositions harmonisées plus largement applicables, qui couvrent tous les fournisseurs de services d'hébergement proposant des services au sein de l'UE. Outre une définition uniforme des contenus terroristes, il a également instauré des ordonnances de retrait imposant aux fournisseurs de supprimer les contenus terroristes dans un délai d'une heure, ainsi que des demandes de retrait volontaires ; il comprend notamment des dispositions procédurales à cet égard. L'accent est mis sur la coopération et la coordination transfrontalières entre les États membres et, par exemple, Europol. Par ailleurs, en application du DSA, les contenus terroristes constituent un risque systémique, ce qui signifie que les VLOPSE sont tenus de procéder à une évaluation préventive des risques associés à ces contenus. Cette réglementation normative est complétée par des mécanismes de coopération volontaire et de réponse coordonnée.

Le fonctionnement concret du mécanisme du TCOR est illustré par l'exemple de l'Allemagne, un État membre dans lequel les autorités ont été particulièrement actives dans la prise de mesures visant à supprimer des contenus au titre du TCOR à la suite de l'attaque terroriste du Hamas contre Israël. L'Allemagne s'est en effet révélée être l'État membre de l'Union européenne le plus dynamique dans l'application du TCOR et, dans ce contexte, celui qui a renvoyé le plus grand nombre d'affaires au titre du DSA à la Commission européenne pour un complément d'enquête. L'approche allemande en matière d'application du TCOR a bénéficié d'une infrastructure institutionnelle déjà existante et de

[753] Directive SMA, *op. cit.* Article 6.

l'expérience acquise dans le cadre d'un centre de signalement centralisé mis en place par la législation nationale antérieure, qui visait à supprimer les contenus illicites et qui a depuis été largement remplacée par des dispositions harmonisées. L'application du TCOR en Allemagne a révélé un taux de conformité aux ordonnances de retrait supérieur à 95 %. Plutôt que de se concentrer sur les ordonnances de retrait officielles, l'Allemagne fait largement appel à des demandes de retrait volontaire avant de délivrer des ordonnances de retrait. Le BKA agit en tant qu'autorité centrale au titre du TCOR et est également habilité, en vertu de l'article 18 du DSA, à signaler les contenus pénalement répréhensibles. L'application stricte du TCOR témoigne également de la sensibilité historique à l'égard du terrorisme et de l'antisémitisme et, en définitive, de la maturité juridique et institutionnelle avérée de cet État membre, grâce à sa législation antérieure et aux structures institutionnelles instaurées sur cette base.

La Türkiye, qui n'est pas membre de l'UE, adopte une position tout aussi ferme à l'égard des contenus terroristes en ligne. Toutefois, hormis la législation turque relative à internet qui impose au fournisseur d'hébergement de supprimer les contenus illicites, les autorités administratives turques avaient depuis longtemps recours au blocage de l'accès à des sites web entiers lorsque les contenus n'étaient pas supprimés volontairement, ce qui suscitait de vives inquiétudes quant à la liberté d'expression et des médias, comme l'illustrent notamment les arrêts rendus par la Cour européenne des droits de l'homme dans des affaires concernant la Türkiye. La pertinence de cette approche est également discutable, dans la mesure où les contenus restent accessibles en dehors du territoire visé par les restrictions. La nouvelle stratégie réglementaire de la Türkiye vise donc à supprimer les contenus illicites à la source, plutôt que de se contenter d'en restreindre l'accès. Un délai très court de quatre heures est imposé pour la suppression des contenus à caractère terroriste. Les plateformes de réseaux sociaux devront désigner des représentants locaux, répondre aux demandes des utilisateurs, publier des rapports de transparence, localiser les données et protéger les mineurs, selon des principes similaires à ceux du dispositif réglementaire du DSA. Afin de garantir le respect de ces obligations, la Türkiye a mis en place diverses sanctions, parmi lesquelles des amendes, des interdictions de publicité, une limitation de la bande passante et une responsabilité partagée en cas de contenus illicites. Il semble toutefois que le blocage de l'accès, en particulier lors de manifestations citoyennes, soit encore largement utilisé pour diverses raisons[754].

7.3. L'application des dispositions visant à lutter contre les propos diffamatoires, les discours de haine et l'incitation à la violence

L'approche réglementaire européenne en matière de propos diffamatoires, de discours de haine et d'incitation à la violence en ligne a évolué en réaction à la multiplication de ce type de propos, en particulier dans les environnements numériques. Bien que la décision-

[754] Voir, par exemple, F. Schräer, « *Access to Various Internet Platforms in Turkey Restricted* », *heise.de*, 20 mai 2025.

cadre du Conseil de l'Union européenne de 2008 sur la lutte contre le racisme et la xénophobie propose une définition de base des discours de haine illicites, les États membres ont souvent étendu les protections contre les discours de haine à d'autres motifs que ceux mentionnés dans la définition de la décision-cadre, tels que le genre ou le handicap.

Comme nous l'avons vu précédemment, le DSA a instauré une série de responsabilités pour les plateformes en ligne, avec un certain nombre d'obligations spécifiquement destinées aux VLOPSE. Le Code de conduite sur la lutte contre les discours de haine illicites en ligne, révisé en 2025 sous le nom de « Code de conduite+ », a été intégré dans le dispositif de corégulation du DSA. Il permet une suppression plus rapide des discours de haine illicites et harmonise la modération sur les plateformes. L'Union européenne a commencé à appliquer ces dispositions aux VLOPSE qui relèvent de la compétence de la Commission. Celle-ci a notamment pris des mesures à l'encontre de X (anciennement Twitter), au motif que ses pratiques en matière d'atténuation des risques et de modération étaient insuffisantes. La Commission européenne a exercé ses pouvoirs d'enquête au titre du DSA et continue à veiller au respect de la réglementation[755].

Certaines difficultés persistent, notamment pour les contenus à caractère diffamatoire, dont la légalité est largement tributaire du contexte et des normes nationales. Comme le soulignent les exemples nationaux, il existe un certain nombre de différences entre le droit pénal et le droit civil des différents pays en matière de propos diffamatoires, de discours de haine ou d'incitation à la violence, bien que ces dispositions soient soumises aux mêmes normes européennes et internationales des droits de l'homme. Contrairement à l'Irlande, par exemple, l'Italie prévoit une responsabilité pénale plus précise pour les contenus diffamatoires ou d'incitation à la haine qui sont diffusés par des moyens de communication publics. L'exemple de l'Irlande prouve quant à lui que les législations qui se sont avérées efficaces dans l'univers hors ligne ne sont pas nécessairement appliquées avec la même efficience aux discours en ligne.

En termes de responsabilité, le DSA reprend le principe de la Directive sur le commerce électronique selon lequel les intermédiaires ne sont pas soumis à une obligation générale de surveillance, mais autorise les injonctions permettant d'exiger des plateformes qu'elles empêchent toute réapparition de contenus illicites similaires à ceux qui ont déjà été déclarés illicites, c'est-à-dire des obligations de surveillance (« *staydown* »), pour autant que le recours à une telle injonction ne nécessite pas une évaluation juridique indépendante de la part des fournisseurs concernés.

Une harmonisation accrue au niveau de l'Union européenne sous la forme d'un règlement directement applicable (DSA) plutôt que d'une directive (Directive sur le commerce électronique), qui n'est contraignante que sur le plan des objectifs mais qui nécessite une transposition nationale, implique l'existence d'un cadre réglementaire uniformisé et commun à toutes les plateformes dans les pays de l'Union européenne mentionnés dans cette publication. Toutefois, comme le démontrent les exemples,

[755] Voir également la première décision de sanction prise au titre du DSA qui concerne une partie de l'enquête menée à l'encontre de X sans rapport avec les éléments évoqués ici, Commission européenne, « La Commission inflige à X une amende de 120 millions d'euros au titre du Règlement sur les services numériques », communiqué de presse, 5 décembre 2025.

l'application effective repose sur des mécanismes nationaux. Contrairement à l'Irlande, l'Italie dispose d'un système d'application plus perfectionné dans la pratique, avec des pouvoirs administratifs étendus conférés à l'autorité nationale de régulation des communications, l'AGCOM, qui est également le coordinateur des services numériques dans le cadre du DSA. Le système italien, qui combine des dispositions harmonisées au niveau européen (DSA et Directive SMA), des instruments nationaux (TUSMA et loi Mancino), le rôle administratif de l'AGCOM et des recours judiciaires, constitue une structure d'application hiérarchisée de la réglementation. En revanche, la responsabilité des plateformes en Irlande était auparavant essentiellement basée sur la responsabilité civile et la notification, avec une réglementation limitée (avant le DSA) qui visait spécifiquement les obligations des plateformes en matière de discours de haine et de diffamation. Il semble que la transposition tardive de certaines parties de la Directive SMA révisée et la récente création de la nouvelle autorité de surveillance irlandaise CnAM, qui n'a vu le jour qu'en mars 2023, ont eu pour conséquence, jusqu'à présent, de limiter les mesures d'application, malgré le fait que la CnAM soit également chargée de veiller au respect du DSA au niveau national et qu'elle soit l'autorité de régulation de la sécurité en ligne. Toutefois, compte tenu des prérogatives exclusives de la Commission européenne en matière de surveillance des risques systémiques posés par les VLOPSE et des mesures récemment prises par la Commission à cet égard, la CnAM devrait intensifier ses activités, notamment en contribuant à l'action de la Commission européenne par la collecte et le partage d'informations sur la multitude de VLOPSE établis en Irlande.

Alors que le renforcement des mesures coercitives permet de garantir l'application et la mise en œuvre effectives de la réglementation et des obligations, l'exemple de l'Autriche met en évidence un autre aspect de la lutte contre le discours de haine en ligne. Cet exemple démontre que, compte tenu de l'harmonisation complète des principes de responsabilité applicables aux services intermédiaires au niveau de l'UE, le champ d'application de la réglementation des contenus illicites en ligne se limite essentiellement au droit matériel. La nouvelle législation autrichienne sur les discours de haine en ligne a été adoptée en réponse aux nouvelles formes de discours de haine en ligne, afin de mieux tenir compte des caractéristiques spécifiques aux communications dans le cyberespace. Les modifications apportées au cadre national existant pour lutter contre les propos diffamatoires, les discours de haine et l'incitation à la violence concernent également le droit procédural et permettent ainsi de faciliter et de promouvoir l'application de la réglementation par les particuliers.

7.4. L'application des dispositions relatives aux autres types de contenus préjudiciables

Après avoir examiné la question de la suppression des contenus illicites, ce rapport *IRIS* s'intéresse ensuite aux autres contenus préjudiciables, bien que licites. Il s'agit notamment des contenus inappropriés pour les enfants et susceptibles de nuire à leur épanouissement, comme la pornographie. Dans l'UE, la Directive SMA, qui s'applique à la fois à la radiodiffusion traditionnelle et aux services à la demande, ainsi qu'en partie – y compris l'obligation de protection des mineurs – aux fournisseurs de services vidéo à la demande,

exige des États membres qu'ils veillent à ce que ces contenus soient inaccessibles aux mineurs grâce à des outils tels que les systèmes de vérification de l'âge et de classification appliqués par les fournisseurs. Le DSA complète cette mesure et impose des obligations horizontales aux plateformes en ligne, lesquelles doivent prendre des mesures appropriées et proportionnées pour protéger les mineurs, notamment en matière de confidentialité et de normes de sécurité dès la conception. En juillet 2025, la Commission européenne a publié des lignes directrices au titre de l'article 28 du DSA qui préconisent des mesures telles que des outils de vérification de l'âge, tout en mettant l'accent sur la proportionnalité, les droits des enfants et une divulgation minimale des données, qui pourraient être mises en œuvre dans le cadre du futur portefeuille d'identité numérique de l'UE. Dans ce contexte, l'application de la réglementation a déjà débuté, puisque la Commission a engagé en 2025 des procédures à l'encontre de grandes plateformes pornographiques en raison d'une vérification insuffisante de l'âge des utilisateurs, tandis que les autorités nationales ont coordonné des actions similaires au moyen du Comité européen des services numériques (EBDS). afin d'harmoniser les mesures coercitives à l'encontre de ce type de contenus.

L'exemple de la Pologne montre que certains États membres rencontrent des difficultés avec la mise en œuvre nationale du DSA[756] et ne parviennent donc pas à établir des procédures nationales pour l'application de la réglementation. En septembre 2025, le Gouvernement polonais a finalement adopté la loi nationale, qui remaniera en profondeur l'actuel cadre juridique. Comme tous les autres États membres de Union européenne, la Pologne applique le modèle décentralisé d'application du DSA et de la Directive SMA décrit précédemment, en conférant à la Commission européenne des compétences spécifiques en matière de VLOPSE. Bien que le projet de loi national détaille les procédures de suppression des contenus illicites, il n'aborde pas spécifiquement la question des contenus licites mais préjudiciables qui ne relèvent pas des dispositions directement applicables du DSA. Certaines dispositions spécifiques relatives aux contenus préjudiciables figurent néanmoins dans des *leges speciales*, qui abordent par exemple la question des jeux d'argent et de hasard en ligne ou des plateformes de partage de vidéos. Dans la pratique, limiter l'accès à des contenus pornographiques sur les plateformes de partage de vidéos n'empêche pas pour autant les mineurs d'y accéder facilement ailleurs en ligne. Le législateur polonais entend combler cette lacune réglementaire en adoptant une nouvelle loi relative à la protection des mineurs contre l'accès à des contenus préjudiciables en ligne. Le projet de loi met principalement l'accent sur la prévention de l'accès des mineurs à des contenus pornographiques en exigeant des services en ligne qu'ils mettent en œuvre des mesures efficaces de vérification de l'âge comparables à celles imposées aux plateformes de partage de vidéos dans le cadre de la transposition nationale de la Directive SMA.

Tout comme la réglementation en vigueur sur les jeux d'argent et de hasard en ligne, les dispositions relatives aux restrictions d'accès s'accompagnent d'un mécanisme d'application précis. Dans les deux cas, la Pologne adopte un mécanisme basé sur un registre qui combine une désignation administrative (liste des sites non conformes) et des

[756] En mai 2025, la Commission européenne a décidé de saisir la Cour de justice de l'Union européenne contre plusieurs États membres, parmi lesquels la Pologne, pour ne pas avoir désigné et/ou habilité un coordinateur national des services numériques dans le cadre du DSA, voir Commission européenne, « La Commission décide de saisir la Cour de justice de l'Union européenne d'un recours contre la Tchéquie, l'Espagne, Chypre, la Pologne et le Portugal en raison de l'absence de mise en œuvre effective du Règlement sur les services numériques », communiqué de presse, 7 mai 2025 (en anglais).

obligations techniques pour les intermédiaires. L'application de la réglementation ne vise donc pas directement les services en infraction, qui sont généralement établis hors du territoire polonais. Le cadre réglementaire des jeux d'argent et de hasard intègre une dimension financière, avec le blocage des paiements versés aux services non conformes, tandis que le projet de loi sur la protection des mineurs contre l'accès à des contenus préjudiciables en ligne se concentre uniquement sur le contrôle de l'accès aux contenus. Cette distinction s'explique par les différences entre les structures économiques et les objectifs réglementaires des deux régimes. Les services de jeux d'argent et de hasard en ligne tirent leurs recettes des paiements directs des utilisateurs. L'interdiction des services de paiement constitue par conséquent un outil coercitif efficace qui prive les opérateurs de leurs sources de revenus et protège les consommateurs contre les pertes financières. En outre, cette mesure empêche les échanges monétaires entre les utilisateurs mineurs et les opérateurs. En revanche, la plupart des sites pornographiques fonctionnent selon un modèle publicitaire ou de monétisation du trafic, qui offre un accès gratuit aux utilisateurs et tire ses recettes d'annonceurs tiers ou de réseaux partenaires. Le projet de loi reconnaît le faible impact du blocage des paiements dans ce contexte et se concentre davantage sur la prévention de l'accès, qui constitue une mesure plus ciblée et proportionnée, conforme à son objectif de protection.

Contrairement à la réglementation européenne sur les contenus préjudiciables, qui fait l'objet de différents textes législatifs spécifiques, le Royaume-Uni s'efforce de mettre en place une législation couvrant tous les aspects. À la suite du Brexit, le Royaume-Uni a adopté l'OSA, une législation nationale qui établit un cadre réglementaire national complet applicable aussi bien aux contenus illicites qu'aux contenus préjudiciables en ligne. L'OSA va bien au-delà du DSA en termes de champ d'application et de niveau de réglementation, et impose aux plateformes de nouvelles obligations juridiquement contraignantes. L'application de l'OSA relève d'une autorité nationale unique, l'Ofcom, le régulateur britannique des communications, qui dispose de pouvoirs étendus en matière d'enquête, de surveillance et de sanction, y compris d'amendes pouvant atteindre 10 % du chiffre d'affaires mondial de la plateforme ou le blocage du service.

En vertu de l'OSA, les plateformes ont l'obligation de prendre des mesures proactives pour identifier, supprimer et empêcher la diffusion de contenus illicites et préjudiciables aux mineurs. Concrètement, la responsabilité est transférée aux plateformes dans des proportions bien plus importantes que dans le cadre du DSA. En résumé, le DSA impose, *notamment*, une évaluation systématique des risques, des rapports de transparence et des mécanismes de notification et d'action, mais l'article 28 du DSA, par exemple, impose uniquement aux plateformes accessibles aux mineurs de prendre des mesures appropriées et proportionnées pour la protection de ces derniers, tout en conservant une certaine flexibilité et la prise en compte des risques. En revanche, les dispositions de l'OSA relatives à la protection des mineurs prévoient des mesures strictes de vérification de l'âge, des systèmes de « sécurité dès la conception » et des évaluations régulières des risques, qui s'étendent à des secteurs tels que les jeux d'argent et de hasard en ligne et les boîtes à butin (*loot boxes*). L'application de ces dispositions a déjà donné lieu à des mesures réglementaires et à des contestations judiciaires, telles que le recours judiciaire de Wikipédia contre l'Ofcom, mettant en évidence les tensions entre sécurité en ligne, vie privée et liberté d'expression alors que le dispositif sera pleinement mis en œuvre en 2026.

8. Conclusions et perspectives d'avenir

Dr Mark Cole, directeur des affaires académiques de l'Institut européen du droit des médias (EMR) et professeur en droit des médias et des télécommunications à l'université du Luxembourg

L'environnement numérique a redéfini à la fois les possibilités d'expression et l'étendue des responsabilités en matière d'informations exprimées et disséminées. Comme le montre le présent rapport IRIS, la même infrastructure en ligne qui permet une participation et un pluralisme sans précédent dans le débat public accentue également les risques que représentent les contenus illicites et la désinformation pour les droits individuels, la cohésion sociale et la résilience démocratique. L'environnement en ligne est par ailleurs dominé par un petit nombre de plateformes particulièrement influentes. Les cadres législatifs internationaux, mais surtout européens et nationaux, ont progressivement évolué pour faire face à ces risques, mais leur application reste partiellement fragmentée et inégale, à l'image de la diversité des traditions nationales, des compétences réglementaires et des priorités politiques. Le DSA, ainsi que l'OSA au Royaume-Uni et d'autres instruments émergents, traduisent une transition vers une réglementation plus systématique, fondée sur les risques et davantage réactive à l'égard des intermédiaires en ligne, mais soulignent également le dilemme persistant entre la protection de la liberté d'expression et la garantie de la sécurité en ligne et de l'obligation de rendre des comptes.

Une mise en application efficace ne peut être assurée par des initiatives strictement nationales ou des mesures unilatérales. La nature sans frontières des communications en ligne impose une coopération transfrontalière et des mécanismes qui garantissent la cohérence tout en respectant les systèmes juridiques nationaux et le respect des droits fondamentaux. Elle exige également une plus grande transparence et des procédures plus strictes de la part des plateformes qui jouent un rôle toujours plus important de contrôleurs d'accès dans le monde numérique. En conséquence, le point commun des récentes législations sur le numérique réside dans l'importance qu'elles accordent à la transparence et à une approche basée sur les risques pour répondre aux menaces et les atténuer[757]. L'application de la législation évolue ainsi de mesures ponctuelles de suppression de contenus vers un modèle de gouvernance cohérent.

Parmi toutes les thématiques examinées dans le présent rapport, trois grandes tendances peuvent être observées :

Premièrement, les modèles de mise en application se diversifient en fonction des rôles et des compétences spécifiques des intermédiaires. Les principes originaux de limitation de responsabilité et d'« absence de contrôle généralisé » hérités des débuts du web restent théoriquement en vigueur, mais ils coexistent avec des obligations de plus en plus précises pour les plateformes qui jouent un rôle systémique dans la formation de la communication publique, ce qui amène à se demander si le principe de sécurité juridique pour les intermédiaires perdurera sur le long terme. La démarche réglementaire fondée sur

[757] Voir à ce sujet M. Cappello (sous la direction de), *Transparence et responsabilité en matière d'algorithmes des services numériques*, IRIS *Spécial*, Observatoire européen de l'audiovisuel, Strasbourg, 2023.

les risques adoptée par l'UE, tout particulièrement dans le cadre du DSA, mais également à travers d'autres dispositifs juridiques tels que le TCOR, illustre le passage d'une logique de réaction, de notification et de retrait, à une surveillance préventive. Les exemples nationaux montrent comment les États membres mettent en œuvre des normes communes à travers des dispositifs institutionnels et procéduraux parfois distincts. Des pays non-membres de l'UE, comme la Türkiye et l'Ukraine, confirment également que les modèles nationaux d'application de la réglementation sont fortement influencés par le contexte politique, les réalités géopolitiques et les contraintes constitutionnelles.

Deuxièmement, les limites des cadres réglementaires actuels s'avèrent particulièrement visibles en matière de désinformation et d'autres formes de contenus préjudiciables mais licites. Bien que la notion d'illégalité puisse, en principe, être clairement définie, les contenus préjudiciables se situent souvent dans une zone grise où se mêlent intérêt général, sécurité démocratique et droits fondamentaux. Dans ce domaine, les interventions réglementaires sont intrinsèquement plus controversées et seule l'application des mesures existantes permettra de déterminer si ce domaine fera également l'objet d'une réglementation plus stricte à l'avenir.

Troisièmement, les études de cas nationales mettent en évidence l'importance croissante des compétences institutionnelles, de la coopération transfrontalière et de l'expertise technique. Les seules dispositions légales ne suffisent pas à garantir une application efficace. Les résultats dépendent davantage de la maturité des autorités réglementaires, de la qualité de la coopération entre les agences, de l'accès aux outils techniques et de l'engagement des plateformes elles-mêmes, ainsi que de la coopération avec celles-ci. Les exemples de la Roumanie et de l'Ukraine soulignent les vulnérabilités structurelles des États dont le niveau de culture numérique est faible, qui sont davantage exposés aux FIMI ou qui exercent une influence limitée sur les plateformes d'envergure mondiale. À l'inverse, les expériences de l'Allemagne et de la France montrent comment des infrastructures réglementaires bien établies peuvent fournir des réponses rapides et coordonnées, même si ces systèmes doivent en permanence s'adapter aux nouveaux risques et aux nouvelles technologies.

La sélection d'exemples de désinformation et de contenus illicites et préjudiciables démontre qu'il n'existe pas d'approche unique, mais que la réglementation peut nécessiter des mesures adaptées aux risques que présentent les contenus. À l'instar de l'approche granulaire du DSA, qui prévoit des dispositions plus strictes pour les VLOPSE, et de ses principes généraux fondés sur les risques, qui se retrouvent également dans d'autres réglementations du secteur technologique, comme le Règlement sur l'IA. De la même manière, certains contenus indésirables peuvent exiger une réglementation plus stricte que d'autres contenus illicites, avec des délais et des procédures harmonisées, comme c'est le cas au sein de l'UE pour les contenus à caractère terroriste. Les exemples nationaux mentionnés en matière de désinformation ont démontré que la lutte contre la désinformation doit aller au-delà de simples mesures punitives ou de suppression de contenus. Elle nécessite une réponse sociétale plus globale, qui passe notamment par le renforcement de l'éducation aux médias et la fiabilité des médias, ainsi que par la garantie que les choix de configuration algorithmique n'amplifient pas involontairement les récits préjudiciables. L'application de la législation devrait donc non seulement dissuader les

comportements préjudiciables, mais également renforcer les structures indispensables au maintien d'écosystèmes informationnels fiables, pluralistes et démocratiques.

À l'avenir, la protection des droits fondamentaux en ligne – et notamment la liberté d'expression, l'accès à l'information et le droit de participer au débat public – doit rester le fil conducteur des décideurs politiques, des régulateurs et, à terme, des plateformes. Parallèlement, les obligations qui incombent aux États de garantir un environnement dans lequel le processus de formation de l'opinion puisse se dérouler de manière indépendante, libre et sécurisée, ainsi que l'engagement de l'UE envers ses valeurs fondamentales, pourraient nécessiter la mise en place de mesures réglementaires supplémentaires. Il convient toutefois d'examiner attentivement ces mesures afin de s'assurer que leur application en ligne n'entraîne pas une limitation prématurée de la liberté d'expression, mais reste efficace pour lutter contre les contenus qui s'avèrent illicites et, dans certaines conditions, potentiellement préjudiciables. Cette exigence ne fera que s'accentuer du fait de l'impact croissant de la création de « contenus » alimentés par l'IA dans le secteur des communications, et notamment de la réorientation de l'attention du public et des moyens financiers vers d'autres sources que celles qui ont initialement créé les contenus d'information en question. De même, l'influence de la diffusion de contenus alimentés par des algorithmes dans l'espace de formation de l'opinion publique exigera à l'avenir un examen minutieux de l'efficacité des moyens de contrôle présentés dans le présent rapport et de la nécessité éventuelle de procéder à de nouvelles adaptations.

Une publication
de l'Observatoire européen de l'audiovisuel