Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Le Conseil fédéral

15 novembre 2023

Discours de haine. La loi présente-t-elle des lacunes?

Rapport du Conseil fédéral en réponse au postulat 21.3450 de la Commission de la politique de sécurité du Conseil des Etats du 25 mars 2021

BAKOM-D-BE8C3401/187

Résumé

Le postulat 21.3450 de la Commission de la politique de sécurité du Conseil des Etats (CPS-E) du 25 mars 2021 est formulé comme suit:

> **Texte du postulat:** Le Conseil fédéral est chargé de présenter un rapport faisant état des mesures et moyens de nature pénale, de police préventive et de droit public (droit des télécommunications, p. ex.) qui existent actuellement pour lutter contre les incitations publiques à la haine (discours de haine) ainsi que contre l'importation et la diffusion de matériel de propagande extrémiste. Ce faisant, il indiquera les lacunes éventuelles que présente la législation pertinente.

Le discours de haine menace la cohésion et la sécurité publique des sociétés démocratiques car il dénigre des personnes et des groupes sociaux, leur dénie une participation pleine et active à la vie sociale et les empêche de s'exprimer librement. Il diffuse en outre des idéologies extrémistes violentes et peut contribuer à la radicalisation d'individus. Parfois, les victimes de discours de haine sont contraintes de se retirer du débat public. Le présent rapport examine les possibilités offertes par le droit pénal et le droit public, notamment les mesures préventives et de police, pour lutter contre le discours de haine, et indique où sont les défis particuliers à relever. Dans une moindre mesure, il présente également la situation en matière de droit civil.

Le rapport reprend la définition du discours de haine et de la propagande de haine donnée par le Conseil de l'Europe, à savoir le dénigrement de personnes ou de groupes de personnes en raison de caractéristiques sociales spécifiques, ainsi que la diffusion de contenus diffamatoires. Le discours de haine apparaît en ligne et hors ligne. Il se propage de plus en plus sur les plateformes des intermédiaires numériques, tels que Facebook, YouTube ou TikTok, devenues ces dernières années des canaux centraux de la communication publique. Par conséquent, le rapport met l'accent sur le discours de haine en ligne, soit là où se situent les principaux problèmes au niveau juridique.

Les plateformes de médias sociaux permettent aux utilisateurs d'accéder facilement à un large public, leur confèrent l'anonymat, misent sur l'ouverture des contenus et maximalisent la portée des *contenus générés par les utilisateurs*. Ces éléments renforcent la visibilité et la diffusion des contenus; ils peuvent élargir le discours démocratique, mais aussi conduire à la propagation massive et souvent ciblée du discours de haine.

La haine en ligne peut se transformer en violence hors ligne ou, du moins, être susceptible d'abaisser le seuil de passage à l'acte violent. A l'inverse, des événements survenus hors ligne peuvent alimenter la haine en ligne engendrant un processus d'auto-renforcement. Le contrôle des plateformes effectué par des êtres humains ou des algorithmes est souvent incohérent et inefficace. En outre, les standards d'expression autorisée varient énormément, et des pratiques plus strictes ne font que déplacer le phénomène vers des plateformes qui connaissent peu ou pas de restrictions concernant le contenu.

En Suisse, ces dernières années, les acteurs politiques se sont penchés à plusieurs reprises sur la menace sociale que représente le discours de haine en ligne. Plusieurs interventions parlementaires traitent de l'ampleur que le phénomène prend sur les plateformes numériques et exigent plus de transparence de la part des exploitants. La plupart des interventions portent sur les mesures à prendre pour lutter contre le discours de haine sur les plateformes et responsabiliser davantage les intermédiaires.

L'UE et certains pays européens combattent la diffusion numérique du discours de haine au moyen de leur propre cadre réglementaire, qui responsabilise notamment davantage les intermédiaires et leur impose des devoirs de diligence. En dehors des bases légales de certains Etats, comme la *Netzwerkdurchsetzungsgesetz* en Allemagne ou le *Online Safety Bill* au Royaume-Uni, le *Règlement sur les services numériques* de l'Union européenne entré en vigueur fin 2022 constitue l'approche la plus complète en la matière. Il impose, en particulier aux très grandes plateformes numériques, toute une série d'obligations de diligence.

En Suisse, le droit pénal offre de nombreuses possibilités de lutter contre le discours de haine et contre sa diffusion. Le discours de haine n'est pas une notion utilisée dans le droit suisse en vigueur, mais différentes dispositions peuvent s'appliquer, entre autres la représentation de la violence (art.

135 CP), l'atteinte à l'honneur (art. 173 ss CP), les menaces (art. 180 CP), la contrainte (art. 181 CP) et les crime ou délits contre la paix publique (art. 258 ss. CP), notamment l'incitation publique à la violence (art. 259 CP) et la discrimination et l'incitation à la haine (art. 261bis CP).

Du point de vue du droit pénal, il n'existe aucune différence entre le discours de haine en ligne et hors ligne, si ce n'est que le premier est diffusé au moyen de technologies numériques appropriées. Or, c'est précisément là que réside le plus grand défi. Les données se trouvent généralement sur des serveurs situés à l'étranger, ce qui confère une dimension internationale à la question de l'application du droit et réduit fortement les chances de voir aboutir la poursuite pénale. En fin de compte, la suppression de contenus illégaux n'est souvent possible que si les intermédiaires sont disposés à coopérer.

La situation est semblable en droit civil, où l'application du droit soulève les mêmes problèmes qu'en droit pénal. Dans les deux cas, ce n'est pas le manque de dispositions matérielles, mais les déficits dans l'application du droit en vigueur qui rendent difficile toute action contre le discours de haine.

D'autres dispositions de droit public portent sur les mesures préventives policières relatives à la diffusion de matériel de propagande, à la protection des autorités et des bâtiments et au domaine en ligne. La loi sur la radio et la télévision, la loi sur la protection des mineurs en matière de films et de jeux vidéo, la loi sur la protection des données et la loi sur les télécommunications contiennent ainsi des dispositions relatives au dénigrement de personnes ou de groupes en raison de certaines caractéristiques sociales. Dans la plupart des cas, leur pertinence pratique est faible.

Dans le Règlement sur les services numériques, l'UE suit une approche qui impose aux plateformes une série d'obligations dans leurs relations avec les utilisateurs. En Suisse, l'OFCOM a publié en 2021, en collaboration avec la Chancellerie fédérale, le rapport "Intermédiaires et plateformes de communication. Effets sur la communication publique et approches de gouvernance", qui présente les potentiels sociaux positifs et négatifs des plateformes numériques et examine les approches de réglementation en Europe. Dans la foulée, il a rédigé à l'intention du Conseil fédéral une note de discussion qui indique si et comment les intermédiaires numériques doivent être régulés. Le 5 avril 2023, le Conseil fédéral a chargé le DETEC (OFCOM) d'élaborer un projet sur la réglementation des plateformes de communication destiné à la consultation.

S'appuyant sur le rapport sur la responsabilité civile des fournisseurs de services internet, le Conseil fédéral a privilégié dans le domaine du droit civil la conclusion de traités d'entraide judiciaire et de conventions prévoyant la transmission directe des actes par voie postale.

Dans le cadre des mesures préventives policières, le Parlement a accepté en 2019 la motion "Echange de données de police au niveau national" (Mo 18.3592) qui permet aux autorités de police cantonales d'échanger systématiquement des informations policières entre elles et avec les organes de police de la Confédération. Le Conseil fédéral est chargé de la mise en œuvre.

Des améliorations sont aussi nécessaires dans la gestion des menaces afin de pouvoir mieux identifier et combattre la haine et l'incitation à la haine. Il y a encore aujourd'hui des lacunes notamment en ce qui concerne l'échange de renseignements entre les cantons et la Confédération, les droits d'accès aux informations et l'analyse automatisée des données.

Enfin, le 30 septembre 2022, le Conseil national et le Conseil des Etats ont adopté la loi fédérale sur la protection des mineurs dans les secteurs du film et du jeu vidéo (LPMFJ, FF 2022 2406). La loi contient l'obligation de mettre en place des systèmes de notification qui pourraient aider à contenir la diffusion et la visibilité du discours de haine.

Le Conseil fédéral ne voit pour l'instant aucune autre nécessité de légiférer au-delà des mesures mentionnées.

Table des matières

1 Situation initiale et mandat

Ces dernières années, le discours de haine se propage de plus en plus, en particulier dans les colonnes de commentaires des sites d'information et sur les plateformes des intermédiaires numériques, et est considéré comme un grave problème de société. Sa diffusion dans des réseaux numériques transnationaux pose aux autorités de nouveaux défis en matière d'application du droit.

1.1 Postulat

Par le postulat 21.3450, la Commission de la politique de sécurité du Conseil des Etats (CPS-E) a donc chargé le Conseil fédéral de présenter les possibilités juridiques existantes et d'examiner les problèmes potentiels.

Concrètement, le postulat demande au Conseil fédéral de "présenter un rapport faisant état des mesures et moyens de nature pénale, de police préventive et de droit public (droit des télécommunications, par ex.) qui existent actuellement pour lutter contre les incitations publiques à la haine (discours de haine) ainsi que contre l'importation et la diffusion de matériel de propagande extrémiste. Ce faisant, il indiquera les lacunes éventuelles que présente la législation pertinente".

Le présent rapport a été rédigé sous la direction de l'Office fédéral de la communication (OFCOM), conjointement avec l'Office fédéral de la justice et avec la collaboration de fedpol.

1.2 Structure du rapport

Le rapport se compose de cinq parties. Le chapitre ci-après (chap. 2) examine le phénomène du discours de haine sous l'angle social et mentionne les interventions politiques sur cette question. Le chapitre 3 situe le discours de haine dans un cadre international, notamment sur la base des projets de loi de l'UE et de plusieurs Etats européens dans le domaine numérique. Le chapitre suivant forme le coeur du rapport et examine successivement les possibilités de lutte contre le discours de haine au niveau du droit pénal (chap. 4.2), de la prévention policière (chap. 4.4.1) et du droit public (chap. 4.4.2) et présente aussi les défis législatifs. Une disgression sur les instruments de droit privé conclut le chapitre. Le chapitre final (chap. 5) résume les conclusions et désigne les champs d'action les plus urgents.

Le rapport omet délibérément deux domaines qui font partie d'une réflexion plus approfondie sur la question du discours de haine. Premièrement, l'analyse du rôle des intermédiaires numériques dans la propagation du discours de haine et de l'application du droit se limite aux plateformes publiques, autrement dit aux réseaux sociaux comme Facebook, YouTube ou TikTok. Les services privés et semi-privés tels que WhatsApp ne sont pas traités. Deuxièmement, le rapport se concentre sur le discours de haine tel que défini par le Conseil de l'Europe et exclut des phénomènes connexes comme l'extrémisme violent et le terrorisme.

1.3 Termes centraux: discours de haine et plateformes numériques

La notion de **discours de haine** n'est pas une catégorie clairement définie, ni au niveau des sciences sociales, ni au niveau juridique. Dans la tradition juridique européenne en particulier, il s'agit plutôt d'un terme générique relativement nouveau désignant différentes formes de discrimination, de dénigrement ou de menace de violence. La définition la plus pertinente, qui est aussi centrale pour le présent rapport, émane d'une recommandation du Comité des ministres du Conseil de l'Europe. Ce comité considère le discours de haine:

> comme tout type d'expression qui incite à, promeut, diffuse ou justifie la violence, la haine ou la discrimination à l'encontre d'une personne ou d'un groupe de personnes, ou qui les dénigre, en raison de leurs caractéristiques personnelles ou de leurs statuts réels ou attribués telles que la "race", la couleur, la langue, la religion, la nationalité, l'origine nationale ou ethnique, l'âge, le handicap, le sexe, l'identité de genre et l'orientation sexuelle[1].

[1] CONSEIL DE L'EUROPE (2022), Recommandation CM/Rec(2022)16 du Comité des Ministres aux Etats membres sur la lutte contre le discours de haine.

En outre, le Conseil de l'Europe propose une gradation des mesures (notamment juridiques) contre le discours de haine en fonction de la gravité de celui-ci, des dommages qu'il cause et de ses conséquences pour les membres de certains groupes sociaux. Il distingue deux catégories. La première comprend les formes de discours de haine (a) qui sont interdites par le droit pénal et (b) qui peuvent être sanctionnées sur la base du droit civil ou administratif. La deuxième catégorie comprend les propos dénigrants qui ne sont pas suffisamment graves pour être combattus par voie juridique, mais qui nécessitent néanmoins des mesures. On peut citer ici notamment les différents programmes dans le domaine de l'éducation ou du dialogue interculturel, ainsi que les mesures de sensibilisation[2].

Le présent rapport se limite à examiner les possibilités légales et les défis posés par le discours de haine et la propagande haineuse, et ne traite pas les autres mesures de nature non juridique.

Les **plateformes numériques**, ou médias sociaux, servent de terme générique pour désigner des plateformes publiques de réseaux sociaux et multimédias ainsi que des services de microblogging comme Facebook, YouTube ou TikTok, qui permettent aussi bien l'échange entre des contacts existants (amis, *followers*, etc.) que la diffusion de contenus destinés à un public potentiellement illimité. Sur la plupart des plateformes, les utilisateurs ont en outre la possibilité de réagir aux contenus publiés (*likes*, *retweets*, etc.). La communication peut aussi se faire à l'aide de programmes informatiques (robots ou *bots*)[3]. Selon le service, les contenus partagés peuvent être conçus, diffusés et utilisés sous forme de textes (p. ex. le service de micro-blogging X [anciennement Twitter]), d'images (p. ex. sur Instagram) ou de vidéos (p. ex. sur YouTube). Généralement, un mélange de ces différentes formes est aussi possible (p. ex. une photo accompagnée d'un texte). Cette définition n'inclut pas les services de messagerie comme WhatsApp, dont la communication revêt plutôt un caractère privé, même si, sur des services numériques comme les plateformes et les messageries, il est courant de passer de la communication privée et à la communication publique.[4]

[2] CONSEIL DE L'EUROPE (2022), Recommandation CM/Rec(2022)16 du Comité des Ministres aux Etats membres sur la lutte contre le discours de haine.

[3] Les robots sont des programmes informatiques qui exécutent automatiquement des tâches répétitives. Dans le domaine de la communication, p. ex., ils sont programmés pour participer à des discussions et réagir automatiquement à certains commentaires.

[4] En effet, la communication privée dans les groupes Messenger peut, par exemple, préparer le terrain pour (une extension) du discours public de haine ou une incitation à la violence.

2 Le discours de haine en tant que problème social et défi politique

Le discours de haine menace l'intégrité des systèmes démocratiques à plusieurs égards. D'une part, il dénigre des personnes et des groupes sociaux entiers, les blesse dans leur dignité et les exclut d'une participation de pleins droits à la vie sociale. Il dénie aux personnes visées leurs droits fondamentaux et humains et les empêche d'exprimer librement leurs opinions, les conduisant parfois à se retirer du débat public. Le discours de haine en ligne peut aussi contribuer à la radicalisation d'individus. D'autre part, la diffusion et la tolérance de ce type de discours entraînent une normalisation de la haine et des idéologies haineuses, et leur confèrent une certaine forme de respectabilité. Le discours de haine peut parfois préparer le terrain à la violence physique et à des atrocités, y compris au génocide.

Le discours de haine n'est pas un phénomène nouveau; il existait déjà bien avant la numérisation. Le développement d'internet, en particulier la "plateformisation" de la sphère publique numérique par des plateformes actives à l'échelle mondiale, comme YouTube, Instagram ou TikTok, accentue le problème et lui confère une nouvelle dimension. En effet, la nature ouverte de ces plateformes de communication favorise aussi bien les potentialités positives que négatives et permet une diffusion presque sans limite du discours de haine. Quatre facteurs jouent un rôle déterminant, comme le démontre aussi le rapport de l'OFCOM "Intermédiaires et plateformes"[5].

Premièrement, les plateformes numériques et les moteurs de recherche facilitent l'accès à l'information et simplifient sa diffusion. Ils réduisent ainsi les obstacles à la visibilité publique et intègrent les utilisateurs dans des réseaux numériques organisés à l'échelle mondiale. Un smartphone suffit pour participer au débat public numérique. Deuxièmement, les plateformes diffusent des informations, mais elles ne produisent pas elles-mêmes de contenus car leur modèle d'affaires se base sur la diffusion de contenus générés par les utilisateurs (*user-generated content*), sans qu'elles exercent de contrôle rédactionnel. Troisièmement, les modèles économiques des plateformes reposent en premier lieu sur la portée et la viralité des contenus. Ils visent à ce que les utilisateurs interagissent le plus souvent possible sur le plus grand nombre de contenus, les commentent, les transmettent ou les approuvent par un *like*. L'agenda public des thèmes abordés est donc déterminé en partie par les utilisateurs eux-mêmes. Quatrièmement, les utilisateurs peuvent souvent rester anonymes et participer aux discussions sans devoir révéler leur identité.

Si ces caractéristiques des plateformes numériques facilitent le débat public et démocratique entre les individus, elles permettent aussi toutes sortes de dérives, dont la propagation du discours de haine compte parmi les plus virulentes. Certes, tout n'est pas permis. Les contenus qui enfreignent les conditions générales de la plateforme ont une visibilité réduite ou sont carrément supprimés. Toutefois, les standards d'expression autorisée varient considérablement d'une plateforme à l'autre. Des services comme Gab ou Telegram renoncent même à modérer les contenus. Facebook ou YouTube par exemple, qui suivent des règles plus strictes, sont confrontés au problème suivant: leurs systèmes automatisés doivent pouvoir détecter et supprimer de manière fiable (a) diverses formes de discours de haine vis-à-vis (b) de différents groupes sociaux, (c) dans plusieurs langues. Or, dans la plupart des cas, ils n'y parviennent pas. L'anonymat ainsi que la portée et l'ouverture des réseaux de communication numériques contribuent donc à ce que les utilisateurs deviennent toujours plus la cible de discours de haine. Par contre, les auteurs n'ont souvent aucune sanction à craindre, encore moins pénale. En fin de compte, le discours de haine, qui est interdit hors ligne, jouit en ligne d'une impunité de fait.

Des recherches menées au niveau international montrent l'ampleur qu'a pris le discours de haine sur les plateformes numériques ainsi que les risques qui en découlent pour la société. Quelques résultats sont aussi disponibles pour la Suisse. Généralement, les plateformes elles-mêmes ne publient que des évaluations (souvent globales) de données agrégées qui ne permettent pas de tirer de conclusions sur la situation en Suisse. Même les analyses par pays dans le cadre du *Code de conduite de l'UE pour la lutte contre les discours de haine illégaux en ligne* (voir chap. 3) ne sont pas significatives par rapport à la prévalence réelle du discours de haine dans les différents pays. En raison des lacunes dans les connaissances, l'OFCOM a lancé un appel d'offres pour la réalisation d'études dans le domaine du

[5] Office fédéral de la communication (OFCOM) Intermédiaires et plateformes de communication (admin.ch)

discours de haine numérique en 2021 et 2022, dont les résultats de la première phase du projet sont désormais disponibles[6].

2.1 Réactions politiques au problème du discours de haine en Suisse

En Suisse, plusieurs interventions parlementaires récentes s'inquiètent de la propagation du discours de haine sur les plateformes numériques. Elles abordent principalement trois domaines. Premièrement, comme l'ampleur réelle du phénomène sur les réseaux sociaux n'est pas claire, les acteurs politiques souhaitent obtenir plus de transparence de la part des intermédiaires quant au nombre de cas qui enfreignent les conditions d'utilisation des plateformes ou les bases légales dans le domaine du discours de haine (voir ch. **Fehler! Verweisquelle konnte nicht gefunden werden.**), et savoir quels groupes sociaux sont particulièrement touchés[7]. Deuxièmement, la majorité des interventions demandent quelles sont les mesures et les possibilités offertes par la réglementation actuelle pour lutter contre la propagation de la haine et poursuivre les exploitants des plateformes numériques; elles s'interrogent aussi sur les mesures à prendre pour endiguer ce phénomène et responsabiliser davantage les intermédiaires[8]. En outre, les autorités devraient avoir la possibilité de sanctionner les propos haineux diffusés en ligne. Troisièmement, plusieurs interventions portent sur le rôle des cantons, notamment en ce qui concerne les possibilités de signalement du discours de haine, ainsi que sur les questions de prévention[9].

2.2 Projet de réglementation du Conseil fédéral

Dans son rapport "Motions et postulats 2022", s'agissant des motions 18.3306 (Renforcer l'application du droit sur internet en obligeant les grandes plateformes commerciales à avoir un domicile de notification) et 18.3379 (Accès des autorités de poursuite pénale aux données conservées à l'étranger), le Conseil fédéral indique qu'il analysera la plus-value et les besoins en matière de mise en œuvre pour la Suisse une fois achevés les travaux du Conseil de l'Europe concernant la révision de la Convention sur la cybercriminalité[10].

Suite à la publication du rapport "Intermédiaires et plateformes de communication. Effets sur la communication publique et approches de gouvernance" de l'OFCOM, rédigé en collaboration avec la Chancellerie fédérale, le Conseil fédéral, sur la base de la note de discussion, a demandé le 5 avril 2023 au DETEC (OFCOM) d'élaborer un projet de consultation sur la réglementation des plateformes de communication.

---

[6] Les études publiées jusqu'à présent sont accessibles sur le site de l'OFCOM: https://www.bakom.admin.ch/bakom/de/home/elektronische-medien/studien/einzelstudien.html

Cinq projets sont soutenus par l'OFCOM dans le cadre d'un appel à projets lancé en 2022. Ils examinent la fréquence du discours de haine sur les plateformes numériques, la sensibilité des utilisateurs, dans quelle mesure les algorithmes sont capables d'identifier le discours de haine, quels groupes sociaux sont particulièrement affectés par ce problème et quelles sont les possibilités offertes, notamment par la réglementation actuelle, pour lutter contre le discours de haine.

[7] Ip. 17.3751, Ip. 19.3255, Ip. 20.5670, Po. 21.4531, Po. 22.3201.

[8] Ip. 14.3888, Ip. 17.3751, Ip. 17.3734, Ip. 19.3255, Ip. 19.3787, Ip 20.3686, Ip. 20.5670, Ip. 21.3123, Ip. 21.3684, Ip. 21.4532, Ip. 22.3156, Ip. 22.3157, Ip. 22.3305, Ip. 21.3683, Mo. 16.4082, Mo. 18.3306, Mo. 18.3379, Mo. 20.4357, Iv.pa 13.407, Iv.pa. 20.445, Iv.pa. 21.524, Iv.pa. 21.525, Po. 11.3912, Po. 22.3201, Po. 21.3969. En font également partie les demandes d'extension des infractions actuelles, visant notamment à inclure la caractéristique du sexe dans le champ de protection de l'art. 261bis CP (voir les six initiatives parlementaires de même teneur 21.513, 21.514, 21.515, 21.516, 21.522, 21.527 "Pénaliser les appels à la haine et à la violence en raison du sexe").

[9] Ip. 20.3686, Ip. 21.3123, Ip. 22.3156, Ip. 22.3305, Po. 22.3201.

[10] *www.bk.admin.ch* > *Documentation* > *Aide à la conduite stratégique* > *Rapport motions et postulats* > *Archives*

3 Approches de la réglementation internationales

La législation sur le discours de haine doit veiller à un équilibre entre deux droits de l'homme fondamentaux, pas toujours compatibles: la liberté d'expression et la protection contre les discrimination. La législation suisse en la matière s'inscrit dans le cadre de normes et d'obligations internationales. Les Nations Unies (ONU) et ses organisations affiliées, le Conseil de l'Europe et ses organes ainsi que les efforts de régulation actuels déployés par l'Union européenne (UE) et par certains pays européens, en particulier dans le domaine numérique, jouent un rôle important à cet égard. Dans différents pays d'Europe ainsi que dans l'UE, il est désormais reconnu que le cadre légal existant ne suffit pas à endiguer le discours et la propagande de haine en ligne, car il date de l'époque analogique et ne tient pas suffisamment compte de l'évolution des conditions numériques.

Le Règlement de l'UE sur les services numériques (*Digital Services Act*; DSA), entré en vigueur le 16 novembre 2022[11], est la principale mesure juridique contre le discours de haine en ligne. Suivant le principe selon lequel ce qui est puni hors ligne doit également être sanctionné en ligne, le DSA formule toute une série d'obligations de diligence à l'égard des plateformes numériques. Il impose aux grands intermédiaires actifs à l'échelle mondiale des obligations supplémentaires en matière de transparence et de présentation de rapports. La mise en place concrète d'une modération des contenus est laissée aux intermédiaires, qui sont chargés d'édicter eux-mêmes les règles déterminantes dont l'impact doit être proche de celles du droit étatique. Les organismes officiels surveillent à leur tour, à des fins de contrôle de qualité, l'efficacité de la modération des contenus par les intermédiaires. S'agissant du discours de haine, le DSA est complété par le *Code de conduite de l'UE pour la lutte contre les discours de haine illégaux en ligne*, une approche volontaire d'autorégulation signée entre autres par Facebook, X [anciennement Twitter], Instagram et YouTube. Son efficacité est régulièrement contrôlée et a été jugée insuffisante par l'UE après une évaluation approfondie. L'intégration de l'accord de la branche dans le cadre de la co-régulation du DSA doit désormais aider à uniformiser les obligations pour les intermédiaires de présenter un rapport. A cela s'ajoutent d'autres recommandations, non contraignantes, de la Commission européenne[12].

En amont de ces initiatives, plusieurs pays d'Europe ont créé leurs propres bases légales afin d'inciter les plateformes numériques, notamment les grandes, à s'engager plus activement dans la lutte contre le discours de haine. La *Netzwerkdurchsetzungsgesetz* allemande, la *Kommunikationsplattformgesetz* autrichienne, la *Online Safety Bill* britannique ou encore la *Loi visant à lutter contre les contenus haineux sur internet* française prennent certes des orientations différentes, mais elles visent toutes un objectif commun: la protection de la population, en particulier des enfants et des jeunes, la sécurité nationale ainsi que la protection des droits fondamentaux[13]. Par le biais de leur législation, certains pays comme l'Allemagne et l'Autriche cherchent en outre explicitement à améliorer l'application du droit pénal à l'égard des intermédiaires numériques.

---

[11] 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)

[12] Commission européenne (01.03.2018), 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, JO L 63 du 6.3.2018, p. 50-61; Commission européenne (2017), Lutter contre le contenu illicite en ligne. Pour une responsabilité accrue des plateformes en ligne. Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions. COM(2017) 555.

[13] Deutscher Bundestag (2017), Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz NetzDG); Österreichischer Nationalrat (2021), Bundesgesetz über Massnahmen zum Schutz der Nutzer auf Kommunikationsplattformen (Kommunikationsplattformen-Gesetz - KoPl-G); Department for Digital, Culture, Media and Sport (2022), A bill to make provision for and in connection with the regulation by OFCOM of certain internet services; for and in connection with communication offences; and for connected purposes (Online Safety Bill); Assemblée nationale française (25.06.2020), Loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet.

4 Analyse juridique

Le présent chapitre présente, du point de vue des différents domaines juridiques, les possibilités actuelles pour lutter contre le discours de haine, mais soulignent également les problèmes existants. Les sous-chapitres suivants mettent en lumière les possibilités et les difficultés juridiques spécifiques du point de vue du droit pénal (chap. 4.2), les mesures policières préventives (chap. 4.4.1) ainsi que d'autres dispositions de droit public (chap. 4.4.2). Un excursus sur le droit civil (chap. 4.3) complète l'analyse. Les explications relatives aux différents domaines juridiques sont précédées de quelques remarques introductives sur la spécificité du discours de haine numérique.

4.1 Particularités du discours de haine en ligne

Le principe de territorialité signifie que toutes les personnes se situant sur le territoire helvétique sont soumises aux lois suisses. Ce principe s'applique également à l'espace numérique: selon la jurisprudence du Tribunal fédéral, quiconque recourt, via un accès internet en Suisse, à un service proposé par une entreprise étrangère n'agit pas à l'étranger, d'autant plus qu'il est souvent difficile de savoir dans quel pays les données sont stockées (principe d'accès)[14]. Selon le Tribunal fédéral, les lois suisses s'appliquent aux utilisateurs de plateformes numériques, même si le siège principal de ces plateformes se trouve à l'étranger.

Si les données se trouvent en Suisse, les autorités de poursuite pénale demandent d'abord leur dépôt au détenteur (art. 265 CPP, voir aussi art. 264 CPP), soumettent les systèmes informatiques de tiers à perquisition (art. 246 CPP) et mettent sous séquestre des supports informatiques ou des données, tels des smartphones ou ordinateurs (art. 263 ss CPP)[15]. Il faut donc évidemment que le détenteur puisse être identifié sans aucun doute, ce qui peut poser problème pour les profils et les comptes sur les plateformes numériques, car ceux-ci sont souvent anonymes.

L'obligation de conserver les données relatives au trafic internet n'est pas réglée de manière uniforme et dépend en grande partie du fait que l'exploitant du serveur tombe ou non dans le champ d'application de la loi fédérale du 18 mars 2016 sur la surveillance de la correspondance par poste et télécommunication (LSCPT; RS 780.1).

Selon la jurisprudence du Tribunal fédéral, les succursales suisses d'Alphabet (Google) et Meta (Facebook/Instagram) ne sont pas propriétaires des données des utilisateurs, car elles commercialisent uniquement les prestations, mais ne les exploitent pas[16]. Leur personnel n'est par conséquent *pas soumis à l'obligation de coopérer*. Les autorités suisses de poursuite pénale doivent alors acquérir, par voie d'entraide judiciaire, les données non sauvegardées en Suisse (voir chap. 4.2.3.2). La problématique de la difficulté à mener des poursuites pénales est exposée au chapitre 4.2.3 ci-dessous et présentée en détail dans le rapport du Conseil fédéral "Compléments concernant la cyberintimidation dans le code pénal"[17].

4.2 Analyse du droit pénal

Le droit pénal suisse ne prévoit pas d'infraction de discours de haine. Plusieurs dispositions du Code pénal suisse du 21 décembre 1937 (CP; RS 311.0) peuvent toutefois s'appliquer dans des situations concrètes, comme le montre l'analyse suivante.

4.2.1 Possibilités de droit pénal

Selon les cas de figure, les infractions peuvent notamment tomber sous le coup de:

- l'art. 135 CP (Représentation de la violence);

[14] ATF 143 IV 270, 287 s.

[15] Le détenteur peut certes demander la mise sous scellés des données (art. 248 CPP), mais le Tribunal fédéral fixe des exigences relativement élevées en matière de demande de maintien du secret.

[16] ATF 143 IV 21, 25 f. et décision du Tribunal fédéral 1B_142/2016 du 16.11.2016, consid. 3.

[17] Disponible sous https://www.newsd.admin.ch/newsd/message/attachments/73647.pdf.

- les art. 173 ss CP (Délits contre l'honneur);
- l'art. 180 CP (Menaces);
- l'art. 181 CP (Contrainte);
- les art. 258 ss CP (Crimes ou délits contre la paix publique).

A noter en particulier, parmi ce dernier groupe, l'art. 259 CP (Provocation publique au crime ou à la violence), de même que l'art. 261bis CP (Discrimination et incitation à la haine). Ce dernier s'applique lorsque le discours de haine est prononcé par quelqu'un qui incite publiquement à la haine ou à la discrimination contre une personne ou un groupe de personnes en raison de leur appartenance raciale, ethnique, religieuse ou de leur orientation sexuelle (al. 1), propage de telles idéologies (al. 2), organise ou encourage des actions de propagande, ou y prend part (al. 3), abaisse ou discrimine publiquement et d'une façon qui porte atteinte à la dignité humaine, par la parole, l'écriture, l'image, le geste, par des voies de fait ou de toute autre manière, une personne ou un groupe de personnes en raison de leur appartenance raciale, ethnique ou religieuse ou de leur orientation sexuelle ou qui, pour la même raison, nie, minimise grossièrement ou cherche à justifier un génocide ou d'autres crimes contre l'humanité (al. 4) [18]. Cet article de loi protège la dignité humaine et accessoirement la paix publique en pénalisant l'incitation à la haine ou à la discrimination publique contre des caractéristiques personnelles.

Du point de vue pénal, le discours de haine en ligne ne se différencie de celui "hors ligne" que par le fait qu'il est commis au moyen de technologies de l'information et de la communication (TIC). Par conséquent, toutes les dispositions pénales mentionnées sont applicables aux cyber-infractions.

4.2.2 Responsabilités pénales dans le domaine en ligne

Les personnes qui dissimulent des données malgré la demande des autorités qui en ont besoin comme moyen de preuve dans une procédure pénale se rendent punissables (art. 265, al. 3, CPP)[19]. Quiconque viole une obligation de collaborer dans une procédure pénale peut être puni pour insoumission à une décision de l'autorité (art. 292 CP). Une disposition spéciale similaire s'applique aux personnes soumises à une obligation de collaborer selon la LSCPT[20] (art. 39, al. 1, let. a, LSCPT).

Quiconque met à disposition l'infrastructure technique avec laquelle l'utilisateur commet une infraction peut être puni pour complicité à l'acte principal de l'utilisateur (art. 25 CP). Sur la base de la pratique judiciaire existante, une procédure pénale pourrait donc être ouverte à l'encontre du CEO d'une plateforme de médias sociaux non coopérative à l'étranger pour complicité d'un délit d'expression commis par un utilisateur de la plateforme.

Par ailleurs, en application de la responsabilité en cascade, la responsabilité pénale de l'exploitant de la plateforme peut être envisagée sur la base du droit pénal des médias si un délit d'expression est commis via une plateforme de médias sociaux, pour autant que l'exploitant de la plateforme ait un devoir de surveillance et un pouvoir de blocage[21]. Si l'auteur d'une publication sur une plateforme ne peut pas être identifié, le responsable de la plateforme peut être sanctionné sur la base du droit pénal des médias pour ne pas avoir empêché, intentionnellement ou par négligence, une publication constituant une infraction (art. 28 CP).

---

[18] Le sexe ou l'identité sexuelle d'une personne ne tombent pas actuellement pas dans le champ de protection de l'art. 261bis CP (voir note de bas de page 7).

[19] La personne incriminée n'a aucune obligation de collaborer (principe *nemo tenetur*, art. 113 CPP); le droit de refuser de témoigner peut constituer une exception, voir art. 264 s., CPP.

[20] En particulier les fournisseurs de services de télécommunication (FST), mais également les fournisseurs de courriel, les exploitants de plateformes, etc.

[21] TRECHSEL/JEAN-RICHARD, PK StGB, art. 28 N 14. Une obligation de surveillance générale est toutefois exclue selon la doctrine dominante. En Suisse, le Tribunal fédéral n'a jusqu'à présent pas dû décider de la responsabilité des exploitants de plateformes en tant que médias au sens de l'art. 28 CP.

Si une décision entre en force, les contenus illégaux diffusés sur internet doivent être supprimés[22]. Ce retrait est néanmoins compliqué, voire impossible, si le fournisseur de services est établi à l'étranger et que tant lui que l'auteur de l'infraction refusent de coopérer. Des décisions de blocage aux fournisseurs d'accès en Suisse sont donc envisagées afin de bloquer des contenus internet au public suisse. En pratique, ces mesures n'ont qu'une efficacité limitée car elles sont relativement faciles à contourner.

4.2.3 Problèmes posés par le droit pénal

Les explications ci-dessus relatives aux dispositions pénales montrent qu'en principe, le droit matériel offre des instruments différenciés pour aborder pénalement le discours de haine. Or, les auteurs de ce type de discours agissent souvent de manière anonyme. Leur identification ainsi que la recherche et la conservation des preuves sur les plateformes numériques sont de ce fait particulièrement problématiques. Les difficultés ne se situent donc pas au niveau du droit matériel, mais plutôt de son application.

4.2.3.1 Limites du CP: violation de la souveraineté territoriale étrangère

Une intervention directe des autorités suisses de poursuite pénale n'est en principe pas autorisée en droit suisse: en cas de non-respect des dispositions de l'entraide judiciaire internationale en matière pénale, il y a violation de la souveraineté territoriale étrangère et les éventuels moyens de preuve recueillis ne sont pas exploitables. Il faut en outre tenir compte du fait que l'exécution d'un acte officiel peut également être punissable en vertu du droit étranger. Certes, les Etats-Unis autorisent les autorités suisses de poursuite pénale à demander directement aux fournisseurs d'accès Internet la sauvegarde et la restitution de données, mais ces derniers ne donnent souvent pas suite à ces demandes directes, notamment en ce qui concerne les données de contenu. Dès lors, l'entraide judiciaire revêt une importance capitale pour l'obtention de données à l'étranger.

4.2.3.2 Entraide judiciaire

L'entraide judiciaire en matière pénale permet de mener, dans un Etat sur demande d'un autre Etat, des mesures d'investigation pénales identiques à celles qui auraient été prises dans une procédure pénale nationale, la seule différence étant que les moyens de preuves récoltés peuvent être utilisés dans une procédure étrangère (dans l'Etat requérant). Les bases juridiques sont en général de nature internationale[23] ou administrative. La procédure est alors régie par la loi fédérale du 20 mars 1981 sur l'entraide internationale en matière pénale (EIMP; RS 351.1). Les procédures d'entraide judiciaire sont complexes et, selon les cas, peuvent durer plusieurs mois avant que les autorités de poursuite pénale ne reçoivent les données. De plus, selon le système juridique étranger, il n'y a pas de sauvegarde provisoire immédiate ou de blocage des données, ce qui complique encore le travail des autorités de poursuite pénale. La voie de l'entraide judiciaire peut être longue et fastidieuse[24].

Cette situation découle de plusieurs facteurs. La plupart des exploitants de plateformes - notamment les plus grands - ont leur siège aux Etats-Unis. La maîtrise des données est souvent revendiquée par les groupes à leur siège principal, raison pour laquelle la collecte de preuves par voie d'entraide judiciaire se fait souvent sur la base du traité du 25 mai 1973 entre la Confédération suisse et les Etats-Unis d'Amérique sur l'entraide judiciaire en matière pénale (TEJUS; RS 0.351.933.6). Une condition essentielle pour ordonner de force l'obtention de preuves est la double punissabilité (art. 4, ch. 2, TEJUS). Celle-ci existe si l'acte punissable selon le droit suisse l'est également selon le droit américain. L'infraction doit en outre figurer dans la liste des infractions pour lesquelles des mesures de contrainte peuvent être appliquées en vertu de l'accord bilatéral. Indépendamment d'une éventuelle punissabilité en vertu du droit américain pour des délits contre l'honneur (art. 173 ss CP) et des infractions contre l'interdiction de la discrimination raciale (art. 261bis CP), les demandes d'entraide judiciaire adressées aux Etats-Unis pour de tels délits ne sont pas satisfaites en raison de la liberté d'expression garantie par le premier amendement de la Constitution américaine. Pour ces délits, il

[22] P. ex. pornographie, atteinte à l'honneur ou discrimination raciale.

[23] Traités multilatéraux ou bilatéraux.

[24] A ce sujet: SIEBER/NEUBERT, p. 246.

n'est par conséquent pas possible d'ordonner des mesures de contrainte dans le cadre de l'entraide judiciaire avec les Etats-Unis.

Les exploitants de plateformes n'envisagent de fournir des données que sur la base d'une mesure juridictionnelle, qui ne peut toutefois pas être prise selon le droit américain.

Des considérations similaires s'appliquent aux demandes d'entraide judiciaire adressées aux pays européens. Certes, bon nombre d'entre eux imposent des limites plus strictes que les Etats-Unis à la liberté d'expression. Reste que les propos doivent être examinées au cas par cas à la lumière des notions de droits à la liberté ou du droit pénal en vigueur. De plus, comme les délits de haine sont souvent assimilés à des infractions mineures et que les poursuites pénales entraînent de lourdes dépenses, les autorités suisses ne réussissent à accéder aux données situées en Europe que de manière limitée. La Suisse ne participe pas à des solutions plus poussées de l'UE qui rendent superflu l'examen de la punissabilité réciproque - contrairement aux Etats de l'AELE que sont la Norvège et l'Islande.

4.3 Excursus: instruments de droit privé

Une victime de discours de haine ou d'autres formes d'attaques numériques subit généralement une atteinte illicite à sa personnalité. Pour sa protection, elle peut donc saisir le tribunal civil contre toute personne participant à l'atteinte (art. 28, al. 1, CC). De cette façon, elle peut notamment exiger que l'atteinte cesse, si elle dure encore, ou soit interdite, si elle est imminente (art. 28a, al. 1, ch. 1 et 2, CC). Cette réglementation est technologiquement neutre. Par conséquent, il est envisageable d'ordonner la suppression et le blocage de contenus illégaux sur internet sur la base de ces dispositions.

Dans ce contexte, il est important de souligner qu'en droit civil, il est impossible de déposer plainte contre inconnu. Le plaignant doit produire la preuve devant le tribunal qu'une certaine personne porte une atteinte illicite à sa personnalité. Si l'utilisateur qui enfreint la loi n'est pas connu, la possibilité de porter plainte contre des participants gagne en importance. Dans son rapport "Responsabilité civile des fournisseurs Internet" du 11 décembre 2015, le Conseil fédéral a donc examiné la possibilité d'actions en cessation contre différents acteurs d'internet[25].

Afin de garantir la protection juridique des personnes concernées, il est possible en vertu des bases juridiques générales - et du point de vue du Conseil fédéral souhaitable - que les fournisseurs proches du contenu, tels que les exploitants de plateformes de médias sociaux, puissent être tenus de supprimer, en application du principe de proportionnalité, les contenus illégaux et contraires au droit.

4.3.1 Difficultés dans l'application du droit privé

L'application du droit privé à l'étranger présente souvent des difficultés, tant pour les notifications que pour l'exécution des décisions. Le tribunal peut ordonner aux parties dont le domicile ou le siège se trouve à l'étranger d'élire en Suisse un domicile de notification (art. 140 CPC). Cette demande doit toutefois être notifiée par la voie de l'entraide judiciaire, à moins que le pays concerné n'ait déclaré autoriser la notification directe. La possibilité de notification directe par voie postale existe déjà dans certains Etats où des exploitants de plateformes connus possèdent leur siège juridique[26].

Si une décision a été rendue en Suisse, mais que le défendeur ne s'y conforme pas volontairement, elle doit être exécutée, ce qui, dans les cas transfrontaliers, implique à nouveau un surcroit de travail. Dans les Etats-membres de la Convention de Lugano (CL; RS 0.275.12), la personne lésée peut, avec un jugement suisse, s'adresser directement à l'autorité d'exécution de l'Etat concerné. Si une décision suisse doit être exécutée en dehors de l'espace UE/AELE, parce que le fournisseur y détient son siège, la reconnaissance dépend en général du droit interne de l'Etat en question[27]. Si des

[25] Rapport du Conseil fédéral "Responsabilité civile des fournisseurs de services Internet" du 11 décembre 2015, consultable sous https://www.ejpd.admin.ch/bj/de/home/aktuell/mm.msg-id

[26] USA, Irlande, voir Rapport du CF sur la responsabilité civile du fournisseur de services Internet, chap. 6.2.4.

[27] Rapport du Conseil fédéral "Responsabilité civile des fournisseurs de services Internet" (n. 1), ch. 6.2.5.

difficultés sont à prévoir, la personne lésée est obligée d'intenter une nouvelle action dans l'Etat concerné, voire d'y déposer une plainte dès le début. Le droit auquel la responsabilité civile du fournisseur est soumise dans des cas concrets est déterminé par la législation de cet Etat. La nécessité de faire respecter le droit à l'étranger peut parfois entraîner des difficultés pratiques et des retards importants dans le retrait de contenus illicites[28].

Jusqu'à présent, le Tribunal fédéral n'a rendu que peu de décisions concernant les atteintes à la personnalité sur internet en Suisse, et celles-ci concernent des portails de médias suisses[29]. Il n'existe par contre aucun jugement connu concernant des plateformes étrangères. L'une des hypothèses les plus probables est que l'exécution transfrontalière de demandes de droit civil est considérée comme trop coûteuse et trop longue.

4.4 Droit public

Dans les domaines du droit public, contrairement au droit privé, l'Etat veille en principe à ce que la loi soit respectée. Des mesures policières préventives y sont par exemple prises (voir ci-dessous le chapitre 4.4.1); pour la radio et la télévision, l'OFCOM vérifie le respect de la loi fédérale sur la radio et la télévision (LRTV, RS 784.40), de l'ordonnance sur la radio et la télévision (ORTV, RS 784.401) et des conventions internationales pertinentes (voir ci-dessous le chapitre 4.4.2.1).

4.4.1 Aspects préventifs et policiers

Les mesures policières préventives de la Confédération contre le discours de haine comprennent notamment la saisie, le séquestre et la confiscation de matériel de propagande au contenu incitant à la violence, ainsi que la protection des autorités et des bâtiments de la Confédération. En outre, dans le domaine en ligne, certains intermédiaires disposent de programmes de *trusted flagger*, qui traitent en priorité les annonces faites par des institutions enregistrées, comme fedpol[30].

4.4.1.1 Matériel de propagande

Une grande partie des mesures de lutte contre la propagande haineuse découlent de la loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI, RS 120). Celle-ci prévoit des possibilités d'agir de manière préventive non seulement contre la violence, les appels à la violence et les activités terroristes, mais aussi contre le discours de haine et la propagande haineuse.

Les autorités policières et douanières peuvent, sur la base de l'art. 13e LMSI, saisir le matériel utilisé à des fins de propagande. Si des collaborateurs compétents du Service de renseignement de la Confédération (SRC) ou de fedpol trouvent du matériel de ce type, ils peuvent également le saisir.

S'agissant de diffusion de propagande haineuse terroriste, les autorités compétentes peuvent prendre préventivement des mesures spécifiques à l'encontre des personnes qui représentent un danger terroriste. En cas de tentative de radicalisation de tiers par de la propagande haineuse terroriste, une interdiction de contact peut notamment être prononcée (art. 23*l* LMSI). L'assignation d'un lieu de résidence ou d'un périmètre d'exclusion, qui permet d'empêcher les personnes dangereuses de séjourner dans certains lieux, est également possible (art. 23*m* LMSI). Si une personne propage des idéologies haineuses terroristes, il faut en outre envisager une obligation de se présenter et de participer à des entretiens (art. 23*k* LMSI). Ces mesures peuvent être ordonnées par fedpol au cas

[28] Voir à ce sujet la contribution de *Schneider-Marfels*, Jusletter 20 février 2012 sur une ordonnance superprovisionnelle contre Facebook.

[29] ATF 147 III 185 (Blick.ch), arrêt du Tribunal fédéral 5A_792/2011 du 14 janvier 2013 (Tribune de Genève).

[30] De novembre 2016 à novembre 2020, fedpol a signalé 365 vidéos sur YouTube, dont la majeure partie (311) a été restreinte ou supprimée. Selon les estimations de fedpol, au moins 90 % des vidéos signalées concernaient des contenus terroristes et des représentations de la violence qui en découlent. Les autres signalements concernaient par exemple des vidéos de suicide, des vidéos de cruauté envers les animaux, des vidéos de sextorsion et des vidéos à contenu raciste. Ces dernières années, fedpol n'a pas fait de signalement parce qu'il n'a pas trouvé de contenu pour lequel il aurait fallu demander la suppression. fedpol agit de sa propre initiative, souvent sur la base de signalements de contenus illégaux par la population.

par cas, à la demande des cantons, éventuellement des communes, ou du SRC. Elles interviennent toujours de manière subsidiaire et complémentaire aux mesures sociales, intégratives ou thérapeutiques, ainsi que de manière subsidiaire aux mesures cantonales de prévention générale des dangers et aux mesures de procédure pénale (art. 23*f* LMSI).

Si un étranger met en danger la sécurité intérieure ou extérieure de la Suisse en diffusant de la propagande haineuse, faisant l'apologie de l'extrémisme ou du terrorisme, fedpol peut prendre des mesures relevant du droit des étrangers (interdiction d'entrée, expulsion) en vertu des art. 67, al. 4, et 68 de la loi du 16 décembre 2005 sur les étrangers et l'intégration (LEI, RS 142.20).

Des possibilités d'intervention policière existent sur la base du droit cantonal de la police, comme une expulsion pour la propagation de discours de haine punissable par la loi et diffusé dans l'espace public. Dans les cas de diffusion de propos haineux, la gestion cantonale des menaces peut intervenir pour identifier, évaluer et désamorcer à temps le danger que représentent certaines personnes.

4.4.1.2 Protection des autorités et des bâtiments de la Confédération

En collaboration avec les autorités cantonales, fedpol veille à la protection des autorités et des bâtiments de la Confédération, ainsi que des personnes et des bâtiments dont la Confédération doit garantir la sécurité en vertu du droit international public (art. 22 LMSI). Dans l'exécution de ce mandat, fedpol intervient en tant que conseiller ou ordonne les mesures policières nécessaires lorsque des personnes à protéger sont mises en danger par des discours de haine ou des menaces. S'il existe des raisons concrètes de penser qu'une personne va commettre une infraction, fedpol peut, de même que les autorités de police cantonales qu'il a mandatées, procéder par exemple à un entretien avec la personne constituant une menace (art. 23, al. 3bis, LMSI, en relation avec l'art. 14 OPF; RS 120.72).

4.4.1.3 Domaine online

Des entreprises comme Alphabet (Google), Meta (Facebook, Instagram) et X (anciennement Twitter) proposent des procédures dites de notification et de retrait (*notice and take down*), qui permettent aux utilisateurs de signaler aux plateformes des violations de la loi dans tous les pays. Ces intermédiaires bloquent[31] ou suppriment les contenus après les avoir examinés. Diverses plateformes traitent de manière privilégiée les signalements de certaines institutions. On connaît par exemple le programme de *priority flagger* de YouTube. Un *flagger* est un utilisateur particulièrement digne de confiance; l'entreprise réagit plus rapidement à ses remarques et alertes qu'à celles adressées par des utilisateurs ordinaires. Fedpol possède le statut de *flagger* pour YouTube et entretient des contacts avec X (anciennement Twitter) et Facebook.

Si du matériel de propagande incitant à faire usage de la violence est diffusé sur internet, fedpol peut, en vertu de l'art. 13*e* LMSI (après consultation du SRC), ordonner la suppression du site internet concerné si ce matériel se trouve sur un serveur suisse. Si le matériel de propagande ne se trouve pas sur un serveur suisse, fedpol peut tout de même recommander au fournisseur d'accès suisse de bloquer le site internet. Il est en outre possible de révoquer un nom de domaine suisse si du matériel de propagande violente est diffusé par le biais de ce nom de domaine[32].

4.4.1.4 Lacunes dans les mesures policières préventives

La diffusion de discours de haine, en particulier sur internet, constitue un problème croissant. Le discours de haine peut déclencher ou renforcer des processus de radicalisation. Il peut aussi conduire à la violence physique, même si l'auteur lui-même ne passe pas à l'acte. La haine et les menaces visent parfois des acteurs politiques. Par peur, certains d'entre eux préfèrent alors se retirer du débat public. Le discours de haine peut aussi dissuader certaines personnes d'exercer des fonctions politiques, par crainte de s'exposer à des menaces ou des propos haineux. C'est pourquoi ce type de

[31] Dans le sens d'un géoblocage (blocage de contenus pour certaines régions).

[32] La loi sur les télécommunications régit la procédure selon laquelle fedpol peut décider de révoquer un nom de domaine (voir chap. 4.4.2.4).

discours représente une menace non seulement pour les personnes, mais aussi pour les institutions et le débat démocratique.

4.4.1.4.1 Diffusion de discours de haine sur les plateformes internet

La Suisse ne dispose pas de mécanismes de notification et d'action (*notice and action*) comparables à ceux du DSA. La question de savoir si un intermédiaire est tenu de vérifier et, le cas échéant, de supprimer des contenus suite à une notification des autorités suisses s'apprécie au regard des règles générales du droit civil et pénal. De même, les autorités policières n'ont pas la possibilité d'exiger de services numériques qu'ils suppriment les discours de haine illégaux (voir tout de même ci-dessus, chap. 4.4.1.3).

Actuellement, les exploitants de plateformes ne sont pas tenus par la loi de signaler ou de supprimer les contenus illégaux aux autorités de police et de poursuite pénale, même s'ils disposent d'indices concernant une infraction (éventuellement grave)[33].

4.4.1.4.2 Matériel de propagande

En vertu de l'art. 13*e* LMSI, Fedpol ne peut agir que contre le matériel de propagande dont le contenu le contenu incite, *d'une manière concrète et sérieuse*, à faire usage de la violence contre des personnes ou des objets. La disposition ne tient pas compte du contexte d'utilisation de certains symboles. Du point de vue de la prévention des menaces, l'importation et la diffusion, par exemple, de symboles nazis ou de l'EI est difficilement tolérable si, au vu des circonstances concrètes, il faut sérieusement s'attendre à ce qu'ils soient utilisés à des fins punissables, telles que le soutien à des organisations terroristes (art. 260ter CP), la discrimination ou l'incitation à la haine (art. 261bis CP) ou la provocation publique au crime ou à la violence (art. 259 CP).

4.4.1.4.3 Echange d'informations

Les autorités policières cantonales n'ont pas la possibilité d'échanger systématiquement entre elles des informations policières. L'accès aux informations ne peut être obtenu que sur demande concrète, au cas par cas, car il n'existe pas de plateforme nationale de consultation des données de la police qui permette aux autorités habilitées d'interroger en une seule fois les systèmes d'information de police de la Confédération, des cantons et de l'étranger[34].

4.4.1.4.4 Gestion des menaces

La gestion des menaces, dans le cadre de laquelle les informations publiques et non publiques provenant des systèmes de la Confédération et des cantons sont analysées, présente plusieurs lacunes. Il n'existe pas de base légale permettant une analyse automatisée des données et l'établissement de profil de risque pour les personnes concernées, afin de pouvoir procéder à une évaluation précoce de la situation ou de la menace. La base légale actuelle ne prévoit pas de droits d'accès des autorités cantonales aux données de gestion des menaces de fedpol, et inversement. De même, les droits d'accès aux données des services de fedpol compétents en matière de procédures de police judiciaire doivent être réglementés afin de garantir que les informations résultant des activités d'analyse puissent également être utilisées dans le cadre d'une procédure pénale engagée en cas de menace par exemple.

4.4.2 Autres réglementations de droit public en vigueur

L'Etat a l'obligation de prendre des mesures pour garantir l'exercice effectif des droits fondamentaux, notamment lorsque cet exercice est menacé par d'autres acteurs[35]. Une protection efficace des biens

[33] Dans la loi sur les télécommunications, il existe une exception pour les contenus pornographiques, basée sur l'art. 197, al. 4 et 5, CP.

[34] Cette lacune est abordée par la motion 18.3592 "Echange national de données de police", adoptée par le Conseil national et le Conseil des Etats en 2019 ; le Conseil fédéral est désormais chargé de la mise en œuvre.

[35] Voir aussi: Waldmann, BSK Cst., art. 35 Cst., n. 6 et 40;

juridiques doit être assurée tant hors ligne qu'en ligne. Ces principes valent aussi bien pour le droit à l'intégrité physique et psychique face aux discours de haine que pour les droits fondamentaux en matière de communication (liberté d'expression et d'information).

4.4.2.1 Loi fédérale sur la radio et la télévision

La loi fédérale sur la radio et la télévision (LRTV) régit l'aménagement, la préparation, la transmission et la réception de programmes de radio et de télévision en Suisse. Elle est conçue de manière technologiquement neutre, à savoir que son champ d'application ne dépend pas du type de diffusion (internet, lignes, fréquences). Les radios et télévisions diffusées sur internet entrent donc aussi dans son champ d'application.

Dans le contexte du droit des médias, seule une disposition légale, l'art. 4, al. 1, LRTV, couvre explicitement le phénomène du discours de haine. Elle ne s'applique toutefois qu'aux radios et télévisions suisses ainsi qu'aux autres services journalistiques de la SSR. Pour le reste des médias journalistiques en Suisse (p. ex. la presse et les plateformes en ligne des entreprises de médias), il n'existe pas de dispositions légales spéciales concernant le contenu des publications. Comme l'indiquent les chapitres 4.2 et 4.3, la législation suisse en vigueur contient de nombreuses dispositions visant à protéger les personnes contre les discours de haine. Ces dispositions peuvent être considérées comme suffisantes pour lutter contre le discours de haine. En effet, contrairement au discours de haine numérique dans un contexte international, les médias basés en Suisse ne rencontrent pas de problèmes d'application de la loi.

La branche suisse des médias a toutefois défini elle-même ses règles déontologiques. Les médias de masse journalistiques s'engagent par exemple eux-mêmes à rechercher la vérité, à respecter la dignité humaine et à s'abstenir de toute allusion discriminatoire[36]. Le Conseil suisse de la presse veille au respect de ces règles déontologiques. En qualité d'organe d'autorégulation, il a rappelé dans un avis que les obligations inscrites dans le code des journalistes devaient également être observées pour le traitement rédactionnel des lettres de lecteurs ou des commentaires en ligne[37].

D'autres défis se posent quant aux radios et télévisions étrangères car la LRTV ne s'applique qu'aux diffuseurs suisses. La Suisse est toutefois liée par la Convention européenne sur la télévision transfrontière (CETT; RS 0.784.405) du 5 mai 1989. Cette réglementation, tout comme l'art. 4, al. 1, LRTV, couvre également le phénomène du discours de haine.

La CETT obéit au principe dit de la Partie de transmissionhttps://www.fedlex.admin.ch/eli/fga/2003/223/fr, c'est-à-dire que l'Etat dans lequel le diffuseur a son siège doit veiller à que ce diffuseur applique les règles en vigueur. Par conséquent, si un programme étranger diffusé par un Etat partie prenante de la CETT, qui est capté en Suisse, enfreignait la CETT, la Suisse ne pourrait pas en empêcher la retransmission de sa propre initiative, mais devrait s'adresser à la Partie de transmission (art. 24, al. 1, CETT). Ce n'est qu'en cas de violation manifeste, sérieuse et grave de la convention que l'Etat de réception peut, deux semaines après en avoir informé l'Etat de transmission, suspendre provisoirement la retransmission du programme mis en cause (art. 24, al. 2, CETT)[38]. En revanche, pour les programmes diffusés depuis des Etats non membres de la CETT, la Suisse n'est pas tenue de respecter l'art. 24 de la CETT. L'art. 52, al. 1, let. b, LRTV donne à l'OFCOM la possibilité de restreindre ou d'interdire la transmission d'un programme diffusé par des moyens de télécommunication si celui-ci contrevient gravement et durablement aux dispositions du droit international public relatives à la conception du programme, à la publicité ou au parrainage qui sont contraignantes pour la Suisse.

[36] Conseil suisse de la presse, Code des journalistes.

[37] Conseil suisse de la presse, avis 8/2016 du 2.5.2016 (X. c. «Tribune de Genève»).

[38] Art. 24, al. 2, CETT, en relation avec art. 52 LRTV.

4.4.2.2 Loi fédérale sur la protection des mineurs dans les secteurs du film et du jeu vidéo (LPMFJ)

Le 30 septembre 2022, le Conseil national et le Conseil des Etats ont adopté la loi fédérale sur la protection des mineurs dans les secteurs du film et du jeu vidéo (LPMFJ, FF 2022 2406), qui n'est actuellement pas encore en vigueur[39].

Cette nouvelle loi vise à protéger les mineurs contre les contenus médiatiques de films et de jeux vidéo qui pourraient porter préjudice à leur développement physique, mental, psychique, moral ou social, notamment des représentations de la violence - dont font partie les contenus haineux -, de sexe et de scènes effrayantes. En Suisse, tous les cinémas, détaillants, vendeurs en ligne et services à la demande sont tenus d'indiquer les limitations d'âge et de procéder à des contrôles. Cette obligation s'applique également aux fournisseurs de services de plateforme de vidéos ou jeux vidéo (p. ex. YouTube, Twitch).

La LPMFJ poursuit en premier lieu un objectif de protection des enfants et des adolescents contre les contenus qui leur sont préjudiciables[40]. Même si la loi ne contient pas de mesures visant à empêcher explicitement le discours de haine et la propagande haineuse, l'obligation incombant au fournisseur de mettre en place des systèmes de signalement offre au moins la possibilité d'endiguer la diffusion et la visibilité de ce type de discours.

4.4.2.3 Loi totalement révisée sur la protection des données

La nouvelle loi sur la protection des données (LPD; RS 235.1), la nouvelle ordonnance sur la protection des données (OPD; RS 235.11) ainsi que la nouvelle ordonnance sur les certifications en matière de protection des données (OCPD; RS 235.13) sont entrées en vigueur le 1er septembre 2023. La révision totale de la LPD a permis d'adapter cette loi à l'évolution des conditions technologiques et sociales.

Les grandes plateformes internet et les réseaux sociaux ayant leur siège à l'étranger sont tenus de désigner un représentant en Suisse s'ils traitent des données de personnes en Suisse. Celui-ci doit servir d'interlocuteur pour le Préposé fédéral à la protection des données et à la transparence (PFPDT) ainsi que pour les personnes concernées en Suisse (art. 14, al. 2, LPD). L'art. 14 LPD doit permettre de prendre facilement contact avec les exploitants de plateformes internet afin que les personnes concernées puissent mieux faire valoir leurs droits, comme par exemple le retrait de contenus portant atteinte à l'honneur. L'efficacité de ce point de contact se révélera à l'usage, après l'entrée en vigueur de la nouvelle loi sur la protection des données.

4.4.2.4 Loi sur les télécommunications (LTC)

La loi sur les télécommunications (LTC) régit la transmission d'informations au moyen de techniques de télécommunication, y compris la transmission de programmes de radio et de télévision. Selon l'art. 3, let. b, LTC, quiconque transmet des informations entre deux parties au moins au moyen de techniques de télécommunication offre un service de télécommunication[41].

La LTC définit les obligations des fournisseurs de services de télécommunication (FST). Il s'agit notamment des obligations de sécurité, de confidentialité, d'information, de conciliation, de blocage et d'information. Le droit des télécommunications ne prévoit pas de mesures contre les discours de haine.

---

[39] L'ordonnance a été mise en consultation le 16 juin 2023. La loi et l'ordonnance devraient entrer en vigueur en même temps. Voir Protection des mineurs dans les secteurs du film et du jeu vidéo (admin.ch).

[40] Message reconcernant la loi fédérale sur la protection des mineurs dans les secteurs du film et du jeu vidéo du 11 septembre 2020, FF 2020 7907, 8221, 8232 s.

[41] Les exploitants de plateformes de médias sociaux ne sont en principe pas soumis à la LTC, car ils ne représentent généralement qu'une des parties entre lesquelles des informations sont transmises.

L'ordonnance sur les domaines Internet (ODI, RS 784.104.2) règle toutefois la *procédure* selon laquelle fedpol peut ordonner la révocation d'un nom de domaine si celui-ci sert à la diffusion de propagande incitant à la violence (art. 13*e*, al. 5, let. a^{bis}, LMSI, voir chap. 4.4.1.3)[42]. La procédure de révocation en application de l'art. 13*e*, al. 5, let. a^{bis}, LMSI est réglée aux art. 30 et 31 ODI, à savoir que l'exploitant du registre (actuellement SWITCH pour le .ch) révoque l'attribution d'un nom de domaine lorsqu'une autorité administrative ou de poursuite pénale suisse (dans ce cas fedpol) l'ordonne dans le cadre de sa compétence.

[42] La révocation d'un nom de domaine n'intervient qu'en dernier recours, lorsque toutes les autres mesures envisageables sont restées sans effet.

5 Conclusion

Le discours de haine constitue un grave problème pour les sociétés démocratiques: il empêche certaines personnes de participer au débat public, dénie leurs droits humains, favorise la radicalisation et prépare le terrain à la violence. Il représente une atteinte à la sphère publique des sociétés démocratiques, leurs membres et leurs institutions.

Bien que la Suisse ne connaisse pas de catégorie juridique autonome pour le discours de haine, les dispositions du code pénal recouvrent en grande partie la définition du Conseil de l'Europe. Au-delà des différents domaines juridiques, c'est dans l'application du droit que se dressent les plus grands écueils. L'augmentation massive du discours de haine en ligne, notamment sur les plateformes numériques, pose de sérieux défis à la société et à la politique.

Certes, le droit pénal met à disposition différents moyens pour la conservation des preuves. Toutefois, les demandes d'entraide judiciaire correspondantes ne sont souvent pas exécutées, par les Etats-Unis notamment, où se trouve le siège social des intermédiaires les plus influents. En effet, des pratiques considérées comme des délits par le droit suisse sont admises dans de nombreux cas par le droit américain au nom de la liberté d'expression. Ces lacunes s'avèrent d'autant plus problématiques que le discours de haine en ligne se multiplie et qu'il se propage plus rapidement et plus largement que hors ligne.

Actuellement, l'application de normes contre le discours de haine repose principalement sur les plateformes elles-mêmes. La démarche s'avère peu fiable. De plus, les conditions générales des plateformes divergent considérablement du droit suisse, et les normes applicables varient fortement d'une plateforme à l'autre. En outre, le discours de haine se déplace vers les plateformes moins restrictives. Au final, il en résulte que le discours de haine qui est interdit et peut être poursuivi hors ligne, n'est généralement pas poursuivi pénalement en ligne.

Avec le Règlement sur les services numériques, l'Union européenne a présenté un instrument destiné précisément à combler ces lacunes en imposant aux intermédiaires des obligations de diligence plus importantes et en les soumettant à un contrôle. L'élaboration de ce cadre de corégulation est fondée sur le principe selon lequel ce qui est illégal et poursuivi hors ligne doit également pouvoir être sanctionné en ligne. Certains pays comme le Royaume-Uni, la France ou l'Allemagne disposent de lois nationales, également destinées à renforcer l'application du droit.

En Suisse, le 5 avril 2023, le Conseil fédéral a chargé le DETEC (OFCOM) d'élaborer un projet de consultation sur la réglementation des plateformes de communication. Ce projet doit se pencher en particulier sur les défis résultant de la non-exécution des décisions dans les domaines du droit pénal et civil (voir chap. 4.2.3 et 4.3.1).

Dans domaine du droit civil, le Conseil fédéral a en outre donné la priorité à la conclusion d'accords d'entraide judiciaire et de conventions prévoyant la notification directe par voie postale de documents administratifs.

Dans le domaine des mesures policières préventives, le Conseil national et le Conseil des Etats ont adopté en 2019 la motion "Echange de données de police au niveau national" (Mo. 18.3592), qui doit permettre aux autorités policières cantonales l'échange systématique d'informations entre elles et avec les organes de police de la Confédération. Le Conseil fédéral est désormais chargé de la mise en œuvre. Dans le cadre du projet POLAP (plateforme de recherche de la police), la Confédération et les cantons travaillent à l'amélioration de l'échange national et international de données policières.

Enfin, le 30 septembre 2022, le Conseil national et le Conseil des Etats ont adopté la loi fédérale sur la protection des mineurs dans les secteurs du film et du jeu vidéo (LPMFJ, FF 2022 2406). Cette loi contient des obligations relatives à la mise en place de systèmes de signalement qui doivent aider à endiguer la diffusion et la visibilité des discours de haine.

En sus des mesures mentionnées, le Conseil fédéral ne voit pour l'instant aucune autre nécessité de légiférer.