GCTF
GLOBAL COUNTERTERRORISM FORUM

BOÎTE À OUTILS POLITIQUE

Recommandations de Zurich-Londres du GCTF sur la prévention et la lutte contre l'extrémisme violent et le terrorisme en ligne

BOÎTE À OUTILS POLITIQUE

Recommandations de Zurich-Londres du GCTF sur la prévention et la lutte contre l'extrémisme violent et le terrorisme en ligne

Table des matières

Contexte

Dès son apparition, Internet a ouvert d'innombrables possibilités à la société en facilitant la communication et l'accès à l'information, le développement économique, ainsi que la participation de tous. Un environnement numérique ouvert, sûr, stable, accessible et pacifique est essentiel pour tous et exige une coopération effective entre États afin de réduire les risques pour la paix et la sécurité internationales[1]. Toutefois, des personnes et des groupes extrémistes violents et terroristes utilisent Internet, et en particulier les plateformes des médias sociaux, en vue de diffuser leur propagande, de disséminer du matériel créant les conditions pour leurs activités, de lever des fonds, d'intimider, de former, de radicaliser, de recruter et d'inciter d'autres personnes à commettre des actes extrémistes violents et terroristes.

L'Assemblée générale des Nations Unies a affirmé l'importance de la coopération entre parties prenantes dans la mise en œuvre de la Stratégie antiterroriste mondiale des Nations Unies, y compris entre États et entre organisations internationales, régionales et sous-régionales, ainsi qu'avec le secteur privé et la société civile, pour répondre à l'utilisation croissante par les terroristes et leurs partisans des technologies de l'information et de la communication (TIC), dans le respect des droits de l'homme et des libertés fondamentales et conformément au droit international et aux buts et principes énoncés dans la Charte [2].

L'Assemblée générale a souligné qu'il est essentiel de mettre au point les moyens les plus efficaces possibles de combattre la propagande terroriste, l'incitation au terrorisme et le recrutement de terroristes, notamment en utilisant Internet et ce, dans le respect du droit international, notamment du droit international des droits de l'homme. En outre, l'Assemblée générale des Nations Unies a recommandé que les États mettent en œuvre, là où elles pourront s'appliquer à leur contexte national, les recommandations pertinentes du *Plan d'action du Secrétaire général des Nations Unies pour la prévention de l'extrémisme violent*, lequel avait identifié la communication stratégique, Internet et les réseaux sociaux comme des domaines cruciaux pour la prévention et la lutte contre l'extrémisme violent et le terrorisme[3].

Lors de la septième Réunion ministérielle plénière du GCTF, tenue à New York le 21 septembre 2016, les États membres du Forum mondial de lutte contre le terrorisme (GCTF) ont entériné le lancement d'un examen assorti d'une évaluation des meilleures pratiques gouvernementales existantes et des leçons tirées en matière de prévention et de contre-mesures destinées à lutter contre l'extrémisme violent et le terrorisme en ligne, dans le cadre de l'*Initiative du GCTF visant à interrompre le processus de radicalisation menant à la violence*. L'aboutissement de ces travaux a été l'adoption officielle, en septembre 2017, des *Recommandations de Zurich-Londres du GCTF sur la prévention et la lutte contre l'extrémisme violent et le terrorisme en ligne* (ci-après Recommandations de Zurich-Londres).

1 *Rapport du Groupe d'experts gouvernementaux chargés d'examiner les progrès de l'informatique et de la télématique dans le contexte de la sécurité internationale* (A/70/174), § 2, 22 juillet 2015.
2 *Examen de la Stratégie antiterroriste mondiale des Nations Unies* (A/RES/70/291), § 42, 19 juillet 2016.
3 *Examen de la Stratégie antiterroriste mondiale des Nations Unies*, §. 42f et 40 ; Plan d'action du Secrétaire général des nations Unies pour la prévention de l'extrémisme violent (A/70/674), §. 55, 24 décembre 2015.

Cette Initiative s'appuyait sur la conviction que les pouvoirs publics devraient prendre les devants et soutenir les actions adéquates menées par le secteur des TIC et la société civile en vue de prévenir et de lutter contre l'usage abusif de l'espace numérique, en particulier d'Internet et des plateformes des médias sociaux, à des fins d'extrémisme violent et de terrorisme. Les Recommandations de Zurich-Londres, non contraignantes, constituent une liste non exhaustive de bonnes pratiques à l'intention des gouvernements sur les aspects relatifs à la communication stratégique et aux médias sociaux susceptibles d'être utilisés dans la prévention et la lutte contre l'extrémisme violent en ligne, dans le respect des droits de l'homme, des libertés fondamentales et du principe de l'état de droit.

En 2018, les membres du GCTF ont entériné le lancement d'une Initiative menée par l'Australie, la Suisse et le Royaume-Uni visant à rendre opérationnelles les Recommandations de Zurich-Londres, proposant aux décideurs politiques et aux experts gouvernementaux des orientations sur les bonnes pratiques mises en place par les gouvernements, des études de cas et des références aux initiatives et pratiques existantes à l'échelon international et régional en matière de prévention et de lutte contre l'extrémisme violent et le terrorisme en ligne.

La présente Boîte à outils politique poursuit les objectifs suivants :

- Fournir aux experts gouvernementaux et aux décideurs politiques un accès à l'information sur les politiques et les tendances actuelles en matière de prévention et de lutte contre l'extrémisme violent et le terrorisme en ligne.
- Promouvoir les mesures susceptibles d'être prises par les pouvoirs publics pour respecter les droits de l'homme et les libertés fondamentales telles que la protection de la vie privée et la liberté d'expression, d'association, de réunion pacifique, de religion ou de conviction, ainsi que la nécessité de préserver la libre circulation de l'information et un Internet libre et ouvert.
- Favoriser une collaboration efficace et durable entre gouvernements, entreprises du secteur des TIC et société civile, fondée sur le principe de la responsabilité partagée en matière de prévention et de lutte contre l'extrémisme violent et le terrorisme en ligne.
- Stimuler l'innovation en faisant référence aux bonnes pratiques et enseignements tirés dans des activités qui, bien que relevant d'autres domaines que celui de la prévention et la lutte contre l'extrémisme violent et le terrorisme en ligne, peuvent néanmoins y contribuer avec pertinence.

PUBLIC CIBLE

La présente Boîte à outils est conçue à l'intention des Membres du GCTF ainsi que des partenaires clés du GCTF et de tout autre gouvernement s'intéressant à la prévention et la lutte contre l'extrémisme violent et le terrorisme en ligne.

Reconnaissant que la prévention et la lutte contre l'extrémisme violent et le terrorisme en ligne impliquent une responsabilité partagée entre gouvernements, entreprises du secteur des TIC et société civile, la présente Boîte à outils est également destinée aux experts œuvrant dans ces deux derniers secteurs.

MÉTHODOLOGIE

La présente Boîte à outils politique vise à guider les décideurs politiques et les experts, d'une manière pratique et conviviale, dans leurs actions de prévention et de lutte contre l'extrémisme violent et le terrorisme en ligne. Il est important de noter que la Boîte à outils politique n'est pas exhaustive et prétend plutôt servir de référence comportant des bonnes pratiques et des études de cas.

La Boîte à outils politique est fondée sur les bonnes pratiques identifiées dans les Recommandations de Zurich-Londres. Ni les études de cas ni les exemples de pratiques mises en œuvre par l'une ou l'autre partie prenante évoqués ici ne font la promotion d'une approche particulière de la prévention et de la lutte contre l'extrémisme violent et le terrorisme en ligne ; elles ont été choisies parce qu'elles illustrent avec pertinence ce que l'on doit considérer comme une mise en œuvre réussie, tout en donnant des orientations générales.

Les Recommandations de Zurich-Londres répartissent en deux catégories les réponses à apporter à l'extrémisme violent et au terrorisme en ligne :

1. Les mesures fondées sur les contenus : il s'agit des efforts consentis par les pouvoirs publics pour restreindre la disponibilité et l'accessibilité de la propagande extrémiste violente et terroriste en s'appuyant sur la coopération internationale, ainsi que pour interagir et collaborer avec les sociétés privées dans la lutte contre le terrorisme et l'extrémisme violent en ligne, notamment pour ce qui concerne le signalement, la suppression et le filtrage de contenus au moyen de réglementations et/ou d'une législation appropriées.
2. Les mesures fondées sur la communication : il s'agit du soutien ou de l'aide apportés par les pouvoirs publics aux initiatives visant à saper l'attrait de la propagande extrémiste violente et terroriste en ligne par le biais de la communication stratégique, notamment en soutenant les organisations de la société civile dans leur diffusion de contre-discours et de récits alternatifs, tant en ligne que hors ligne.

Lorsqu'elles sont fermement inscrites dans une stratégie à la fois pangouvernementale et sociétale de la prévention et de la lutte contre l'extrémisme violent et le terrorisme sur Internet, ces deux catégories de mesures peuvent contribuer à une approche plus globale de la prévention et de la lutte contre l'extrémisme violent et le terrorisme de manière générale.

Ainsi, toute stratégie menée par les pouvoir publics en vue de prévenir et de lutter contre l'extrémisme violent et le terrorisme en ligne doit se fixer des objectifs clairs et mesurables et être sous-tendue par une « théorie du changement » bien définie, qui explicite en quoi et comment les réponses fondées sur les contenus et celles fondées sur la communication contribuent aux objectifs fixés.

Réponses fondées sur les contenus :

1. Élaboration et adoption de législations et de politiques relatives aux contenus

Ce chapitre vise à apporter un appui aux législateurs et décideurs politiques ainsi qu'aux praticiens dans leur élaboration et adoption de lois et de politiques visant à prévenir et lutter efficacement contre l'extrémisme violent et le terrorisme en ligne. Ce chapitre aborde en particulier la manière dont les pouvoirs publics peuvent adopter des dispositions juridiques de prévention et de lutte contre l'usage abusif d'Internet à des fins extrémistes violentes et terroristes, tout en respectant le droit international des droits de l'homme, notamment la liberté d'expression et le droit à la protection de la vie privée. Ce chapitre comporte deux sections, à savoir : Principes et lignes directrices, et Conception des politiques.

Bonnes pratiques pertinentes des Recommandations de Zurich-Londres

Bonne pratique no 1 : *Adopter et mettre en place à l'échelle nationale des cadres législatifs et politiques destinés à prévenir et à lutter contre le terrorisme et l'extrémisme violent en ligne.*

Bonne pratique no 7 : *Adopter des lois, des règlements et des politiques relatives à la disponibilité et à l'accessibilité des contenus extrémistes violents et terroristes sur l'internet.*

Bonne pratique no 8 : *Prendre en compte les normes et/ou principes internationaux en vigueur pertinents pour agir sur la disponibilité et l'accessibilité des contenus extrémistes violents et terroristes sur l'internet et sur les plateformes des médias sociaux.*

INTRODUCTION

Les États sont responsables au premier chef, dans le cadre d'une réponse sociétale, de la prévention et de la lutte contre l'extrémisme violent et le terrorisme. À l'heure actuelle, seuls quelques États ont adopté des dispositions juridiques érigeant l'incitation à la violence en infraction pénale ; en revanche un nombre sensiblement plus conséquent d'États se sont dotés de dispositions juridiques concernant la commission d'un acte terroriste, la glorification du terrorisme et « l'apologie du terrorisme ». L'adoption ou la mise à jour de la législation, dans le respect du droit international des droits de l'homme, en vue de fournir une base juridique au traitement de contenus à caractère extrémiste violent et terroriste en ligne est essentielle pour garantir que tous les acteurs concernés connaissent les obligations qui leur incombent et disposent de lignes directrices leur permettant de prévenir et de lutter de manière effective contre l'extrémisme violent et le terrorisme en ligne.

Les États ont l'obligation de veiller à ce que les acteurs privés n'enfreignent aucune législation nationale ou internationale dans l'accomplissement de leurs activités. L'élaboration et la mise en œuvre d'un cadre législatif national efficace, qu'il s'agisse d'une nouvelle législation relative aux contenus ou de la mise à jour de textes de loi existants en y incluant des dispositions relatives aux contenus, constituent un point de départ essentiel pour que tous les pays fassent en sorte de traiter les contenus illicites en ligne et que les sociétés du secteur des TIC se voient réellement contraintes d'agir en matière de prévention et de lutte contre l'extrémisme violent et le terrorisme en ligne[4].

A : Principes et lignes directrices

Instruments internationaux : principes et orientations

Un certain nombre d'instruments internationaux énoncent les normes et principes pertinents devant être pris en considération par les États lors de l'élaboration de toute législation concernant la prévention et la lutte contre l'extrémisme violent. La nécessité de respecter les obligations internationales a été mise en exergue à maintes reprises dans les instruments internationaux. Par exemple, la Stratégie antiterroriste mondiale des Nations Unies note qu'il convient que les États, tout comme les autres acteurs concernés, s'attaquent au recours croissant aux TIC par les terroristes et leurs partisans dans le respect des droits de l'homme et des libertés fondamentales et en conformité avec le droit international et les buts et principes de la Charte des Nations Unies[5].

Une attention soutenue a été accordée à la nécessité de respecter le droit international des droits de l'homme, et en particulier le droit à la liberté d'expression et le droit à la protection de la vie privée (lesquels seront examinés plus bas). Dans la *Déclaration conjointe de 2016 sur la*

4 Aux fins du présent outil, le terme législation sera utilisé pour faire référence à toute loi, réglementation, règle, texte ou autre instrument ayant force de loi ou doté d'une nature contraignante dans un contexte national.

5 *Examen de la Stratégie antiterroriste mondiale des Nations Unies*, 2016.

liberté d'expression et la lutte contre l'extrémisme violent[6], le Rapporteur spécial des Nations Unies sur la promotion et la protection de la liberté d'expression, et ses homologues au sein de l'Organisation pour la sécurité et la coopération en Europe (OSCE), de l'Organisation des États américains (OAS) et de la Commission africaine des droits de l'homme et des peuples (CADHP), formulaient les recommandations suivantes :

> *2. Recommandations spécifiques (...)*
>
> *(e) Les États ne doivent pas assujettir les intermédiaires d'Internet à des exigences impératives de suppression ou de restriction de contenus sauf lorsque les contenus concernés sont légalement limités dans le respect des normes énoncées ci-dessus. Les États doivent s'abstenir d'exercer des pressions, d'imposer des punitions ou de récompenser des intermédiaires dans le but de restreindre des contenus licites.*
>
> *(...)*
>
> *(j) Les États ne doivent pas adopter, ou doivent réviser, les législations et les politiques impliquant les éléments suivants :*
>
> *(i) Interdictions générales du cryptage ou de l'anonymat, qui ne sont pas intrinsèquement nécessaires et proportionnées, et qui sont par conséquent illégitimes en tant que restrictions à la liberté d'expression, y compris en guise de réponse des États au terrorisme et à d'autres formes de violence.*
>
> *(ii) Toutes les mesures qui affaiblissent les outils numériques de sécurité disponibles, tels que les « trappes » (backdoors) ou les systèmes de séquestre de clés, dans la mesure où elles restreignent la liberté d'expression et le droit à la vie privée de manière disproportionnée et rendent les réseaux de communication plus vulnérables aux attaques.*

En outre, les Principes directeurs des Nations Unies de 2011 relatifs aux entreprises et aux droits de l'homme mettent en œuvre le Cadre de référence onusien « protéger, respecter et réparer » de 2008, fournissent des orientations supplémentaires quant aux obligations des États et responsabilités des entreprises, afin d'améliorer les normes et pratiques relatives aux entreprises et aux droits de l'homme[7]. Le premier pilier de ce cadre est l'obligation de protéger, incombant à l'État, lorsque des tiers, y compris des sociétés, portent atteinte aux droits de l'homme sur leur territoire et/ou sous leur juridiction, par le biais de l'adoption de législations et de mesures appropriées. Il incombe en premier lieu aux États de prévenir et de corriger les atteintes aux droits de l'homme en rapport avec l'activité des entreprises.

Le deuxième pilier est la responsabilité incombant aux entreprises de respecter les droits de l'homme : dans l'accomplissement de leurs activités, les tierces parties ne doivent pas porter atteinte aux droits d'autrui, et doivent remédier aux incidences négatives sur les droits de

6 *Déclaration conjointe sur la liberté d'expression et la lutte contre l'extrémisme violent*, adoptée le 3 mai 2016 par le Rapporteur spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'expression et d'opinion, la Représentante de l'OSCE pour la liberté des médias, le Rapporteur spécial de l'OEA pour la liberté d'expression et la Rapporteure spéciale de la CADHP sur la liberté d'expression et l'accès à l'information. Voir aussi : *Déclaration conjointe sur les défis clés pour la liberté d'expression au cours de la prochaine décennie*, 10 juillet 2019.

7 *Principes directeurs de l'ONU relatifs aux entreprises et aux droits de l'homme*, 2011.

l'homme dans lesquelles elles ont une part. S'il est vrai que le respect des droits n'est pas une obligation imposée directement aux tierces parties par le droit international des droits de l'homme, il est désormais devenu un élément fondamental commun à presque tous les instruments volontaires et non contraignants relatifs à la responsabilité des entreprises et entérinés par le Conseil des droits de l'homme. En outre, il se peut que la responsabilité de respecter les droits incombant aux entreprises soit déjà couverte en droit national. Le rapport annuel du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression du 6 avril 2018, qui aborde la réglementation portant sur les contenus en ligne générés par les usagers, évoque la responsabilité à la fois des pouvoirs publics et des entreprises[8].

Enfin, l'accès à des voies de recours effectives, troisième pilier du Cadre, joue un rôle important à la fois concernant l'obligation de l'État de protéger et la responsabilité des entreprises de respecter. Au titre de leur obligation de protéger contre les atteintes aux droits de l'homme commises par des entreprises, les États doivent prendre des mesures appropriées pour garantir par le biais de moyens judiciaires, administratifs, législatifs ou autres, que lorsque de telles atteintes se produisent sur leur territoire et/ou sous leur juridiction, les parties affectées ont accès à un recours effectif.

Liberté d'expression

Il incombe aux États de veiller à ce que toute législation concernant la disponibilité et l'accessibilité des contenus à caractère extrémiste violent et terroriste en ligne soit en conformité avec les normes et principes internationaux, en particulier eu égard à la liberté d'expression. Le droit à la liberté d'expression est l'un des piliers du droit international des droits de l'homme et il est indispensable pour la pleine jouissance d'autres droits de l'homme, tels que le droit à la liberté de réunion pacifique et d'association. Ce droit universel est consacré dans l'article 19 de la Déclaration universelle des droits de l'homme, qui stipule que « Tout individu a droit à la liberté d'opinion et d'expression, ce qui implique le droit de ne pas être inquiété pour ses opinions et celui de chercher, de recevoir et de répandre, sans considérations de frontières, les informations et les idées par quelque moyen d'expression que ce soit. »

Les garanties à la liberté d'expression ont été détaillées à l'article 19 du Pacte international relatif aux droits civils et politiques (PIDCP)[9]. La liberté d'expression a également été intégrée dans un certain nombre d'instruments juridiques régionaux en matière de droits de l'homme, telles la Convention européenne sur les droits de l'homme (CEDH), la Convention américaine relative aux droits de l'homme (CADR) et la Charte africaine des droits de l'homme et des peuples (CADHP).

8 *Rapport annuel du Rapporteur spécial du Conseil des droits de l'homme sur la réglementation des contenus en ligne* (A/HRC/38/35), 6 avril 2018.

9 L'article 19(2) du PIDCP prévoit les garanties les plus complètes pour la liberté d'expression, la liberté de chercher, de recevoir et de répandre des informations et des idées de toute espèce. La liberté d'expression protège toutes les formes d'expression, y compris orales, écrites, imprimées, en langue des signes ou les expressions non verbales telles que des images, ainsi que les moyens de leur diffusion, y compris les livres, les journaux, les tracts, les affiches, les bannières et les modes de diffusion audiovisuels, électroniques et fondés sur Internet. À noter que les États membres du GCTF n'ont pas tous signé ou ratifié le PIDCP, et que certains l'ont fait en y apposant des réserves.

Les restrictions à la liberté d'expression

L'article 19(3) du PIDCP prévoit deux situations spécifiques dans lesquelles il est possible de restreindre la liberté d'expression : le respect des droits ou de la réputation d'autrui, et la sauvegarde de la sécurité nationale, de l'ordre public, de la santé ou de la moralité publiques. Il est important de souligner que la clause de restriction prévue à l'article 19(3) doit être interprétée de manière restrictive. *Les Principes de Syracuse relatifs aux dispositions limitatives et dérogatoires au PIDCP* apportent un éclairage utile concernant les conditions figurant à l'article 19(3) pour limiter la liberté d'expression : dans le contexte de la prévention et de la lutte contre l'extrémisme violent et le terrorisme en ligne, les raisons les plus appropriées pour restreindre la liberté d'expression seraient la sauvegarde de la sécurité nationale et/ou de l'ordre public. En vertu des Principes de Syracuse, la sécurité nationale « ne peut être invoquée pour justifier des mesures restreignant certains droits que lorsqu'il s'agit de mesures prises pour protéger l'existence de la nation, son intégrité territoriale ou son indépendance politique contre l'emploi ou la menace de la force »[10]. La justification de la sécurité nationale « ne peut servir de prétexte pour imposer des restrictions vagues ou arbitraires et elle ne peut être invoquée que lorsqu'il existe des garanties adéquates et des recours utiles contre les abus »[11]. Les dérogations et restrictions aux droits de l'homme justifiées en vertu de l'ordre public ne peuvent être adoptées que dans l'objectif de préserver « la somme des règles qui assurent le fonctionnement de la société ou l'ensemble des principes fondamentaux sur lesquels repose la société »[12]. À cet égard, les principes de Syracuse soulignent que « le respect des droits de l'homme fait partie de l'ordre public »[13].

L'observation générale no 34 du Comité des droits de l'homme des Nations Unies stipule que des infractions telles que l'« encouragement du terrorisme », l'« activité extrémiste », ainsi que le fait de « louer », « glorifier » ou « justifier » le terrorisme devraient être définies avec précision, de façon à garantir qu'il n'en résulte pas une « interférence injustifiée ou disproportionnée » avec la liberté d'expression[14].

Le Rapporteur spécial des Nations Unies sur la liberté d'expression recommande que des restrictions soient adoptées uniquement au cas par cas et conformément aux critères de légalité, de nécessité, de proportionnalité et de légitimité[15] :

- **Légalité :** Toute restriction doit être prévue par la loi. De telles lois doivent être adoptées par les voies législatives ordinaires et formulées de façon suffisamment précise. En outre, de telles lois doivent être accessibles au public et fournir une orientation suffisante aux personnes chargées de leur exécution. Toute restriction spécifique d'un droit doit se conformer à des dispositions garantissant une procédure régulière, stipulées en droit

10 Commission des droits de l'homme des Nations Unies, *Principes de Syracuse concernant les dispositions du pacte international relatif aux droits civils et politiques qui autorisent des restrictions ou des dérogations* (E/CN.4/1985/4), § 29, 28 septembre 1984.
11 *Ibidem*, § 31.
12 *Ibidem*, § 22.
13 *Ibidem*.
14 Comité des droits de l'homme des Nations Unies, *Observation générale no 34, article 19, Libertés d'opinion et d'expression* (CCPR/C/GC/34), § 46, 12 septembre 2011.
15 Conseil des droits de l'homme des Nations Unies, *Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression* (A/HRC/29/32), § 57, 22 mai 2015.

national, et faire l'objet d'une supervision par des organes juridictionnels indépendants, notamment des tribunaux.

- **Nécessité et proportionnalité :** Toute restriction doit être nécessaire, et constituer le moyen le moins perturbateur parmi ceux permettant d'obtenir le résultat légitime recherché. D'après le Rapporteur spécial sur la liberté d'expression, les plateformes de médias sociaux devraient « divulguer des données et des exemples apportant un éclairage sur les facteurs qu'elles évaluent lorsqu'elles déterminent qu'une violation a été commise, sa gravité et l'action prise pour y remédier »[16]. En outre, dans le contexte des discours haineux, « expliquer de quelle manière certaines situations spécifiques ont été résolues peut aider les usagers à mieux comprendre les difficiles distinctions opérées par les entreprises entre des contenus offensants et une incitation à la haine, ou les considérations sur l'évaluation, en ligne, de l'intention de l'orateur ou de la probabilité que des violences soient commises »[17].
- **Légitimité :** Toute restriction doit satisfaire à l'une des deux limitations spécifiques de l'article 19(3) du PIDCP : le respect des droits ou de la réputation d'autrui, et la sauvegarde de la sécurité nationale, de l'ordre public, de la santé ou de la moralité publiques. Il convient d'interpréter les limitations de l'article 19(3) de manière restrictive. Par exemple, des dérogations ou limites ne peuvent être imposées à la liberté d'expression au motif de la sécurité nationale que si elles visent à protéger l'existence d'un État, son intégrité territoriale ou son indépendance politique contre l'emploi ou la menace de la force[18]. Le motif de sécurité nationale ne peut servir « de prétexte pour imposer des restrictions vagues ou arbitraires »[19]. Le motif d'ordre public ne peut être invoqué que lorsqu'il y a lieu de préserver le fonctionnement de la société ou les principes fondamentaux sur lesquels elle repose[20].

Le droit à la vie privée

Il convient, lors de la surveillance des contenus en ligne pour détecter des sympathisants ou des recruteurs extrémistes violents ou terroristes, ou pour déceler un complot terroriste, de protéger le droit à la vie privée. Par exemple, le suivi des contenus en ligne par le biais de la surveillance, de l'interception, de la collecte et de la rétention de données, est un moyen supplémentaire de contrer l'extrémisme violent et le terrorisme en ligne.

L'article 17 du PIDCP stipule que le droit à la vie privée, tout en n'étant pas un droit absolu, doit être protégé contre toute immixtion arbitraire ou illégale. Plus spécifiquement, une immixtion illégale survient lorsqu'elle se trouve en dehors du champ d'application prévu par la loi. Les immixtions arbitraires doivent elles aussi être évitées, et par conséquent même lorsque la loi prévoit des motifs d'immixtion, ceux-ci doivent être raisonnables, nécessaires et proportionnés eu égard aux circonstances particulières. Tout stockage des données concernant une personne, par les autorités publiques comme par des acteurs privés, doit être réglementé par la loi.

16 *Ibidem*, § 47.
17 *Ibidem*.
18 Commission des droits de l'homme des Nations Unies, Principes de Syracuse, § 29.
19 *Ibidem*, § 31.
20 *Ibidem*.

L'observation générale no 16 du Comité des droits de l'homme des Nations Unies recommande que les États veillent à ce que « les renseignements concernant la vie privée d'individus ne tombent pas entre les mains de personnes non autorisées par la loi à les recevoir, les traiter et les exploiter, et ne soient jamais utilisés à des fins incompatibles avec le Pacte »[21].

S'agissant de la collecte et du traitement de données à caractère personnel dans le cadre de la lutte contre le terrorisme, les lignes directrices du Conseil de l'Europe sur les droits de l'homme et la lutte contre le terrorisme stipulent que la collecte et le traitement de données à caractère personnel par toute autorité compétente en matière de sécurité de l'État ne peuvent porter atteinte au respect de la vie privée que si les mécanismes de collecte et de traitement sont :

(i) régis par des dispositions appropriées en droit interne ;
(ii) proportionnés à l'objectif pour lequel cette collecte et ce traitement ont été prévus ;
(iii) susceptibles d'un contrôle par une autorité externe indépendante[22].

Instruments internationaux non contraignants

Outre les obligations prévues en droit international par les traités sur les droits de l'homme et le droit international coutumier, il existe également des instruments non contraignants pouvant guider les décideurs politiques et d'autres parties prenantes dans leur procédures législatives sur la prévention et la lutte contre l'extrémisme violent et le terrorisme en ligne. La complexité de cette problématique a incité à lancer de nombreuses initiatives multipartites visant à concevoir des normes régissant la modération des contenus en ligne. De ce fait, il convient que toute action législative d'endiguement des contenus à caractère extrémiste violent et terroriste en ligne tienne compte de ces nouveaux travaux.

Le *Plan d'action de Rabat sur l'interdiction de tout appel à la haine nationale, raciale ou religieuse qui constitue une incitation à la discrimination, à l'hostilité ou à la violence*[23] annexé au Rapport du Haut-Commissaire des Nations Unies aux droits de l'homme sur les ateliers d'experts portant respectivement sur l'interdiction de l'incitation à la haine nationale, raciale ou religieuse, propose un examen de seuil comportant six étapes avant de qualifier une expression d'infraction pénale. Les six facteurs à prendre en considération sont les suivants :

1. le contexte dans lequel l'acte verbal a été émis ;
2. le statut ou le rôle de l'orateur au sein de la société ;
3. l'intention de l'orateur ;
4. le contenu et la forme du discours ;
5. la portée du discours, la mesure dans laquelle il est public et diffusé ;
6. la probabilité et l'imminence de l'action criminelle à laquelle le discours incite.

21 Comité des droits de l'homme des Nations Unies, *Observation générale no 16 : Article 17 (Droit à la vie privée). Le droit au respect de sa vie privée, sa famille, son domicile et sa correspondance, et à la protection de son honneur et sa réputation*, § 10, 8 avril 1988.
22 Conseil de l'Europe, *Lignes directrices sur les droits de l'homme et la lutte contre le terrorisme*. 11 juillet 2002.
23 Conseil des droits de l'homme des Nations Unies, *Rapport annuel du Haut-Commissaire des Nations Unies aux droits de l'homme – Rapport sur les ateliers d'experts sur l'interdiction de l'incitation à la haine nationale, raciale ou religieuse* (A/HRC/22/17/Add.4), 11 janvier 2013.

En 2019, un certain nombre de gouvernements et de sociétés du secteur des TIC ont adopté l'*Appel de Christchurch pour supprimer les contenus terroristes et extrémistes violents en ligne*[24]. L'Appel de Christchurch engage les gouvernements et les entreprises du secteur des TIC à mettre sur pied une série de mesures pour prévenir et lutter contre l'extrémisme violent et le terrorisme en ligne. Ces mesures incluent l'élaboration d'outils pour prévenir le téléchargement de contenus à caractère terroriste et extrémiste violent ; la lutte contre les facteurs à l'origine de l'extrémisme violent ; une plus grande transparence concernant la suppression et la détection des contenus ; et l'examen de la manière dont les algorithmes des entreprises sont susceptibles d'orienter les utilisateurs vers des contenus extrémistes violents[25]. Lors du Sommet du G20 à Osaka en 2019, la Déclaration des dirigeants du G20 sur la prévention de l'utilisation d'internet à des fins de terrorisme et d'extrémisme violent pouvant mener au terrorisme a été adoptée à l'unanimité. Cette déclaration exhorte les plateformes en ligne à accroître l'ampleur et le nombre d'efforts déployés pour empêcher que du contenu terroriste soit diffusé, téléchargé ou à nouveau téléchargé, et engage à la poursuite de la collaboration pour faire face à ce problème[26].

La Global Network Initiative, à multiples parties prenantes, a élaboré une *Note de politique sur les contenus à caractère extrémiste et le secteur des TIC* comportant un certain nombre de recommandations à l'intention des gouvernements ainsi que des sociétés du secteur des TIC, sur les pratiques devant être évitées[27]. Par exemple, aucune restriction ne devrait être imposée aux journalistes et organes de presse souhaitant couvrir ou commenter des groupes terroristes ou des actes de terrorisme, et les lois et politiques doivent faire la distinction entre les discours visant à inciter à la commission d'actes de terrorisme, d'une part, et les discours visant à débattre, discuter ou rapporter de tels actes, d'autre part[28].

Les Principes de Camden sur la liberté d'expression et l'égalité (Principes de Camden)[29] rédigés par Article 19, approfondissent la réflexion sur la relation entre la liberté d'expression et les questions d'égalité. Les Principes de Camden affirment que la relation entre la liberté d'expression et l'égalité permet de soutenir et de renforcer mutuellement chacun de ces concepts, et formulent des recommandations pour résoudre les tensions pouvant surgir entre eux.

B : Conception des politiques

Lors de l'élaboration ou de la mise à jour de législations ou de politiques visant à s'attaquer à la disponibilité et à l'accessibilité de contenus à caractère extrémiste violent et terroriste en ligne, il convient d'inclure les éléments suivants, approfondis ci-après.

24 Voir https://www.appeldechristchurch.com.
25 Très honorable Jacinda Ardern, *Christchurch Call to eliminate terrorist and violent extremist online content adopted*, 16 mai 2019.
26 *Déclaration des dirigeants du G20 à Osaka sur la prévention de l'utilisation d'internet à des fins de terrorisme et d'extrémisme violent pouvant mener au terrorisme*, 2019.
27 Global Network Initiative, *Extremist Content and the ICT Sector, A Global Network Initiative Policy Brief*, novembre 2016.
28 *Ibidem*, 4.
29 Article 19, *The Camden Principles on Freedom of Expression and Equality*, avril 2009.

Garanties en matière de droits de l'homme

Une défaillance clé constatée dans la plupart des législations nationales est qu'elles ne mettent pas en exergue, ou pas assez, les droits de l'homme de manière générale et le droit à la liberté d'expression en particulier. Il convient que l'adoption et la mise en œuvre des lois permettant le blocage ou la suppression de contenus extrémistes violents ou terroristes en ligne soient effectuées en conformité avec le droit international des droits de l'homme. Dans la pratique, cet objectif peut passer par l'adoption de dispositions claires sur la suppression de contenus, fondées sur les conditions figurant à l'article 19(3) du PIDCP, tout en prévoyant suffisamment de souplesse pour que ces dispositions demeurent d'application au fil des évolutions technologiques.

L'adoption ou la mise à jour de la législation pertinente

Les législations nationales existantes sur l'extrémisme violent et le terrorisme, parce qu'elles ont été adoptées avant l'avènement du cyberespace, ne reflètent souvent pas les réalités technologiques actuelles. Or, sans législation adéquate, la prévention et la lutte contre l'extrémisme violent et le terrorisme en ligne pourraient engendrer des pratiques qui enfreignent le droit international des droits de l'homme et n'aboutissent qu'à des résultats limités ; en revanche, le fait de se doter de dispositions juridiques en la matière permet aux institutions de l'État d'appliquer la loi avec davantage de précision et, partant, de limiter le potentiel d'atteintes aux droits de l'homme. Par ailleurs, la demande par les forces de l'ordre de supprimer des contenus à caractère extrémiste violent ou terroriste en ligne uniquement sur la base des conditions générales d'une plateforme en ligne donnée est désormais une pratique très répandue. Or, cette pratique pourrait résulter en une non-conformité par les autorités étatiques au principe de légalité, lequel requiert que chaque acte réalisé par une institution de l'État soit explicitement fondé sur une disposition juridique en vigueur. Par conséquent il serait souhaitable que les États soit adoptent des lois et réglementations sur la manière d'endiguer la disponibilité et l'accessibilité de contenus extrémistes violents et terroristes sur Internet, soit actualisent la législation en vigueur en y incorporant des éléments spécifiquement liés à ces contenus.

La rédaction des dispositions juridiques

L'absence de définition, ou des définitions excessivement vagues ou générales en droit national de ce qu'il faut entendre par contenus extrémistes violents et terroristes risquent de déboucher sur des pratiques par trop zélées de suppression de contenus, fondées sur des motivations politiques, religieuses ou idéologiques. Ce risque peut être atténué par l'adoption de définitions précises concernant les contenus à caractère extrémiste violent et terroriste devant être bloqués ou supprimés. En outre, il convient de proposer aux membres des forces de l'ordre, de l'appareil judiciaire et d'autres autorités pertinentes sur le terrain, des formations sur les caractéristiques et les traits distinctifs des contenus de cette nature afin qu'ils acquièrent cette expertise.

Examen (judiciaire) indépendant et procédure d'appel

Différents textes législatifs nationaux autorisent les forces de l'ordre à signaler aux fournisseurs de service Internet (FSI), voire directement aux plateformes en ligne (parfois dénommées fournisseurs de services d'hébergement de contenus), des contenus qu'elles jugent illicites, ce qui renvoie la décision finale concernant ces contenus aux plateformes ou FSI concernés. Cette pratique présente une menace potentielle à la pleine jouissance des droits de l'homme par les utilisateurs individuels, dans la mesure où aucun contrôle indépendant ne surveille la procédure. Cette tendance risque de mener à des pratiques de suppression de contenus qui pourraient gravement porter atteinte aux droits de l'homme de personnes dont les contenus ont été bloqués ou retirés. C'est pourquoi toute législation en la matière adoptée par un État devrait comporter des règles décrivant les procédures à suivre par les organes de l'État qui demandent le blocage ou la suppression de contenus en ligne ainsi que les droits et obligations des sociétés du secteur des TIC en tant que destinataires de ces demandes.

Par ailleurs, il est nécessaire d'opérer une distinction entre les décisions portant sur la suppression de contenus prises par des organes de l'État (notamment, les forces de l'ordre et l'appareil judiciaire) et celles qui sont prises par les sociétés du secteur des TIC. Pour les premières, une décision de la justice peut être indispensable puisque c'est aux États qu'incombent au premier chef les obligations en matière de droits de l'homme et qu'il leur appartient de prendre toutes les précautions nécessaires pour empêcher les ingérences arbitraires dans l'exercice des droits de l'homme par leurs citoyens. Pour ce qui a trait au blocage, que l'OSCE définit comme « une activité à laquelle on a recours pour empêcher l'accès à des contenus sur Internet ou à des sites Web, y compris des plateformes de médias sociaux », le Manuel de l'OSCE sur « La liberté des médias sur Internet » recommande que les décideurs politiques « ne s'appuient sur le blocage que dans un strict cadre juridique, pour des contenus qualifiés d'illégaux par un tribunal »[30].

Les décisions des États doivent également pouvoir donner lieu à une procédure d'appel si les utilisateurs estiment que leurs droits de l'homme ont fait l'objet d'une restriction illégale. D'un autre côté, il convient que les sociétés du secteur des TIC adoptent une approche fondée sur le devoir de diligence, en établissant des mécanismes indépendants d'examen permettant aux utilisateurs de contester, sur la base de la législation nationale ou des conditions générales, une décision de suppression de contenus.

Mécanismes de mise en œuvre

Les actions d'application de la loi en lien avec la prévention et la lutte contre l'extrémisme violent et le terrorisme en ligne doivent, dans un premier temps, s'appuyer sur des mesures peu intrusives, telles que le signalement aux sociétés du secteur des TIC de contenus spécifiques comme étant violents ou extrémistes. Les mesures telles que le blocage de l'intégralité de sites Web ou de plateformes entières devraient n'être appliquées qu'en dernier ressort ; comme indiqué dans le Manuel de l'OSCE mentionné plus haut, « le blocage ne constitue pas une

30 Organisation pour la sécurité et la coopération en Europe (OSCE), *Media Freedom on the Internet: An OSCE Guidebook*, 9 mars 2016.

méthode efficace pour régler les problèmes associés aux contenus Internet, et risque au contraire d'avoir des effets secondaires graves, y compris le blocage injustifié »[31].

De manière générale, il pourrait devenir nécessaire de recourir à l'imposition d'amendes pour faire respecter la législation et s'assurer de la conformité des contenus. Cependant, dans le domaine de la réglementation des contenus, la perspective de payer des amendes potentiellement élevées, en particulier lorsqu'elle s'accompagne d'une formulation floue de leurs propres obligations, pourrait inciter les sociétés du secteur des TIC à bloquer ou à supprimer des contenus licites, afin de réduire au minimum, voire d'éviter complètement le risque de devoir payer une amende, ce qui se traduirait par des restrictions arbitraires à la liberté d'expression imposées avec un zèle excessif. Par ailleurs, des amendes élevées peuvent également mettre en péril l'existence même des plus petites sociétés du secteur des TIC présentes sur le marché. Par conséquent, les amendes devraient toujours être proportionnées, et n'être imposées qu'en relation à des obligations clairement définies.

Étude de cas : La loi allemande pour la mise en œuvre au niveau des réseaux

La loi allemande sur l'application du droit sur les réseaux sociaux (Netzwerkdurchsetzungsgesetz, en abrégé : NetzDG) est entrée en vigueur en octobre 2017 (avec une période transitoire jusqu'au 1er janvier 2018). Elle porte obligation aux réseaux des médias sociaux de supprimer les contenus manifestement illicites ou d'en bloquer l'accès et ce, dans les 24 heures après avoir été saisis d'une plainte, ou en l'espace de 7 jours lorsqu'il s'agit de contenus non manifestement illicites (la loi ne définit pas les caractéristiques des contenus manifestement illicites). Le réseau doit conserver le contenu illicite à des fins de preuve, et le stocker pendant une période de 10 semaines. Un non-respect réitéré ou systématique peut entraîner l'imposition d'amendes allant jusque 50 millions d'euros.

La loi établit un certain nombre de mécanismes de transparence, à savoir l'obligation de proposer aux utilisateurs une procédure facilement reconnaissable et accessible directement et en permanence, pour faire parvenir des plaintes concernant des contenus illicites ; l'obligation de notifier à la personne qui porte plainte ainsi qu'à l'utilisateur concerné toute décision ayant été prise, tout en donnant au plaignant ainsi qu'à l'auteur du contenu les raisons ayant motivé la décision finale ; et l'obligation, pour les réseaux sociaux recevant plus de 100 plaintes par an, de présenter des rapports semestriels sur la manière dont les plaintes ont été traitées.

De même, les mécanismes de supervision prévoient l'obligation de faire un suivi du traitement des plaintes par le biais de contrôles mensuels réalisés par la direction du réseau social et confient la surveillance de la procédure à une agence ad hoc constituée par le Bureau fédéral de la justice. La loi accorde également à l'utilisateur

31 *Ibidem.*

la possibilité de répondre à la plainte avant que la décision ne soit rendue par le réseau social, si le caractère illicite du contenu dépend de la non-véracité d'une allégation factuelle ou de circonstances factuelles. Enfin, elle exige de l'autorité administrative qui souhaite émettre une décision (notamment celle d'imposer une amende) reposant sur l'hypothèse que le contenu n'ayant pas été supprimé ou bloqué est illicite, d'obtenir préalablement une décision judiciaire déterminant ce caractère illicite.

La NetzDG a reçu un accueil mitigé. Alors que certains travaux de recherche indiquent qu'elle n'a pas entraîné de suppressions injustifiées de contenus, le Rapporteur spécial des Nations Unies sur la liberté d'expression a fait valoir sa préoccupation quant au caractère éventuellement disproportionné des délais stricts de suppression et du montant élevé des amendes, pouvant se traduire par la suppression de contenus parfaitement licites, et quant à l'absence de supervision judiciaire du retrait et de la suppression de contenus par les sociétés de médias sociaux[32]. Des préoccupations similaires avaient été exprimées par huit des dix experts invités à une audition sur le projet de loi.

Pour l'heure, les principaux réseaux sociaux (Facebook, Twitter et YouTube) passent en revue les plaintes reçues au titre de la NetzDG tout d'abord à l'aune de leurs normes respectives. Si une violation est avérée, le contenu est bloqué à l'échelle mondiale. Dans le cas contraire, la plainte est ensuite évaluée à l'aune de la NetzDG ; si le caractère illicite du contenu est alors confirmé, celui-ci est bloqué, mais seulement en Allemagne.

32 Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, lettre portant la cote OL DEU 01/2017, 1er juin 2017.

Réponses fondées sur les contenus :

2. Conception de mécanismes de transparence et de reddition de comptes

Ce chapitre vise à apporter un appui aux législateurs et décideurs politiques ainsi qu'aux praticiens dans leur élaboration de mécanismes de transparence et de reddition de comptes en vue de prévenir et de lutter efficacement contre l'extrémisme violent et le terrorisme sur Internet. Ces mécanismes consistent à : a) prévoir une procédure établie pour permettre à toute personne de contester une décision de suppression de contenus, et b) informer le grand public des pratiques et méthodes de signalement et de suppression de contenus utilisées tant par les sociétés privées que par les pouvoirs publics.

Ce chapitre vise également à préciser l'importance de mettre en place des cadres de suivi et d'évaluation en vue de promouvoir des pratiques efficaces de signalement et de suppression de contenus et d'en éviter les conséquences non intentionnelles. Ce chapitre comporte trois sections, à savoir : Mécanismes de transparence et de reddition de comptes ; Suivi et évaluation des réponses fondées sur le contenu ; et Procédures automatisées.

Bonnes pratiques pertinentes des Recommandations de Zurich-Londres

Bonne pratique no 4 : *Élaborer en collaboration avec d'autres parties prenantes compétentes un cadre commun de suivi et d'évaluation encourageant la transparence et permettant de mieux comprendre l'impact des mesures mises en œuvre.*

Bonne pratique no 7 : *Adopter des lois, des règlements et des politiques relatives à la disponibilité et à l'accessibilité des contenus extrémistes violents et terroristes sur l'internet.*

Bonne pratique no 8 : *Prendre en compte les normes et/ou principes internationaux en vigueur pertinents pour agir sur la disponibilité et l'accessibilité des contenus extrémistes violents et terroristes sur l'internet et sur les plateformes des médias sociaux.*

Bonne pratique no 10 : *Se référer aux lois et réglementations pertinentes qui justifient le signalement des contenus illicites aux entreprises du secteur des technologies de l'information et de la communication.*

Bonne pratique no 11 : *Admettre le rôle de secteur des technologies de l'information et de la communication dans le traitement efficace de la disponibilité et de l'accessibilité des contenus à caractère extrémiste violent et terroriste sur l'internet et sur les plateformes des médias sociaux.*

Bonne pratique no 12 : *Assurer le suivi et l'évaluation opérationnels des procédures automatisées utilisées pour limiter le redéploiement en ligne de contenus existants et/ou déjà identifiés comme étant à caractère extrémiste violent et terroriste.*

INTRODUCTION

Alors que le premier chapitre décrit l'élaboration et l'adoption de législations et de politiques relatives aux contenus, le présent chapitre se centre sur la transparence et la reddition de comptes dans leur mise en œuvre.

Dans certains pays, les législateurs et décideurs politiques ont substantiellement augmenté les ressources juridiques, humaines et financières dont dispose l'État en vue de procéder à l'analyse des contenus, au signalement de contenus et à leur suppression. Par ailleurs, les sociétés du secteur des réseaux sociaux sont soumises à une pression publique, économique et politique croissante qui leur exige d'empêcher que des groupes extrémistes violents et terroristes utilisent leurs services et plateformes ; elles ont répondu à ces pressions en collaborant à la fois avec les pouvoirs publics et la société civile dans le but de procéder à une modération des contenus et de supprimer les contenus à caractère extrémiste violent et terroriste. Enfin, il arrive de plus en plus souvent que des gouvernements exigent aux sociétés privées de retirer les contenus illicites en l'espace d'un délai restreint[33]. Ces différents éléments risquent d'accroître certains risques, tel celui de restreindre le discours en ligne de manière fortuite et non-intentionnelle (ce que l'on appelle « l'effet paralysant » sur la liberté d'expression). La modération, le signalement et la suppression transparents et responsables des contenus sont par conséquent essentiels pour protéger les droits de l'homme des utilisateurs légitimes d'Internet.

S'il est vrai que la suppression de contenus de quelque nature que ce soit, qu'elle relève de l'application de filtres lors du téléchargement vers l'amont, de l'automatisation de la prise de décisions ou du signalement, est une restriction de la liberté d'expression, certains types d'expression peuvent toutefois être légitimement restreints par les pouvoirs publics si les exigences évoquées au chapitre 1 sont respectées. La transparence n'en reste pas moins vitale pour s'assurer du respect du droit à la liberté d'expression. Les gouvernements ont certes un rôle premier à jouer dans le renforcement de la transparence et de la reddition de comptes pour tout ce qui a trait aux réponses fondées sur les contenus, mais les sociétés du secteur des TIC ont, elles aussi, un rôle crucial à jouer dans le renforcement de la transparence.

33 Voir, au chapitre 1, l'étude de cas sur la loi allemande *Netzwerkdurchsetzungsgesetz* ; Assemblée nationale française, *Proposition de loi visant à lutter contre la haine sur internet*, n° 1785, 20 mars 2019 ; et 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), 12 septembre 2018.

A : Mécanismes de transparence et de reddition de comptes

Surveillance des contenus

La surveillance des contenus en ligne est une manière supplémentaire de contrer l'extrémisme violent et le terrorisme en ligne : elle englobe la surveillance des données, leur interception, collecte et conservation. Tandis qu'une surveillance accrue des contenus en ligne est à même de contribuer à la détection de sympathisants extrémistes violents ou terroristes, de leurs recruteurs, ou de déceler des complots terroristes, il convient aussi de protéger en ligne les droits garantis hors ligne, y compris le droit à la vie privée et la liberté d'expression[34]. Comme souligné au premier chapitre, les États ne devraient pas adopter de lois ni de politiques interdisant le cryptage et l'anonymat ou affaiblissant les outils de sécurité numérique existants.

La surveillance des contenus en ligne exercée par les pouvoirs publics peut revêtir plusieurs formes. Par exemple, en Suède, le *Service suédois de sécurité nationale* (Säkerhetspolisen[35]) fait un suivi régulier des sites Web susceptibles de contenir des messages en lien avec le terrorisme. Le Service de sécurité est réglementé par la loi sur le secteur de la sécurité (Förordning (2002:1050) med instruktion för Säkerhetspolisen). Cette loi ne contient toutefois aucune disposition portant spécifiquement sur la surveillance des sites Web. Si le Service de sécurité détecte des contenus qui lui semblent illégaux, il peut les notifier à la société du secteur des TIC propriétaire du service sur lequel apparaît le contenu et lancer une enquête préliminaire, mais il n'est pas autorisé à prendre des mesures de suppression de quelque contenu que ce soit[36].

En Australie, le Commissaire à la sécurité électronique (eSafety Commissioner) et son équipe Cyber Report[37] procèdent à une enquête dès qu'une réclamation est reçue concernant du matériel prohibé, faisant par exemple la promotion ou donnant des instructions ou incitant à la commission de crimes ou de violences, ou encore faisant l'apologie de la commission d'actes terroristes. L'équipe Cyber Report évalue les contenus en ligne ayant fait l'objet du rapport, à l'aune du Système national de classification (le Système) et d'autres lois pertinentes, en donnant la priorité aux matériels graves, susceptibles par exemple d'être pro-terroristes, ou bien aux contenus qui constituent « un matériel violent particulièrement odieux ». Il s'agit dans ce dernier cas de contenus qui dépeignent un assassinat, un acte terroriste provoquant la mort ou des blessures graves, ou tout autre crime qui serait enregistré ou filmé par son auteur ou par ses complices. En vertu du Système, les contenus de ce genre se verront probablement refuser toute classification, ce qui signifie qu'ils seront réputés interdits si hébergés en Australie. À l'issue de l'évaluation des matériels, l'équipe Cyber Report peut en notifier le résultat au service fournisseur d'hébergement concerné pour que celui-ci procède au retrait. Une injonction de retrait de l'équipe Cyber Report adressée à un service d'hébergement australien est légalement exécutoire, et toute non-conformité est passible de lourdes sanctions.

34 Voir les résolutions du Conseil des droits de l'homme des Nations Unies sur *La promotion, la protection et la jouissance des droits de l'homme sur l'Internet* : 20/8 (A/HRC/20/L.13), 5 juillet 2012, et 26/13 (A/HRC/26/L.2), 26 juin 2014.
35 Voir https://www.sakerhetspolisen.se.
36 Institut suisse de droit comparé, *Étude comparative sur le blocage, le filtrage et le retrait de contenus illégaux sur internet*, p. 671 de la version anglaise, 20 décembre 2015.
37 Voir https://www.esafety.gov.au.

En Suisse, au sein de l'Office fédéral de la police, le Service national de coordination de la lutte contre la criminalité sur Internet (SCOCI) effectue des recherches actives sur Internet pour détecter les contenus illégaux, et reçoit également des notifications en la matière. Après avoir évalué les contenus respectifs et sécurisé les données pertinentes, le SCOCI renvoie l'affaire aux agences répressives compétentes[38].

Accroître la transparence et la reddition de comptes

La transparence et la reddition de comptes sont indispensables pour anticiper et atténuer les répercussions potentiellement négatives des réponses fondées sur les contenus en matière de prévention et de lutte contre l'extrémisme violent et le terrorisme en ligne, en particulier dans le contexte de la surveillance des contenus en ligne et de son éventuel impact sur la jouissance des droits de l'homme.

Les gouvernements sont encouragés à référencer la législation nationale pertinente sur laquelle se fonde le processus de signalement, lorsqu'il est demandé à une société du secteur des TIC de supprimer des contenus. Une telle transparence des processus décisionnels renforce la confiance envers chacun des acteurs concernés, et entre eux. À cet égard, les gouvernements sont encouragés à rendre accessibles toutes les lois et réglementations en la matière.

Il conviendrait également que des mécanismes forts de transparence et de reddition de comptes donnent des voies de recours aux individus dont des contenus ont été supprimés de manière erronée, notamment si les droits à la liberté d'expression ou à la protection de la vie privée ont été enfreints par un acteur, étatique ou non. Les Principes directeurs des Nations Unies sur les entreprises et les droits de l'homme réaffirment le principe de l'accès à des voies de recours, qui relève de l'obligation incombant aux États de « prendre des mesures appropriées pour assurer, par le biais de moyens judiciaires, administratifs, législatifs ou autres, que lorsque de telles atteintes se produisent sur leur territoire et/ou sous leur juridiction, les parties touchées ont accès à un recours effectif »[39]. De tels mécanismes de recours peuvent comporter l'obligation de proposer un accès à « des voies de recours et des dispositifs de réclamation pour faire en sorte que les utilisateurs puissent contester la suppression de leurs contenus », comme proposé par la Commission européenne[40].

La Commission européenne a commandité à l'Institut pour les droits de l'homme et les entreprises et à l'organisation de la société civile Shift l'élaboration d'un guide destiné spécifiquement au secteur des TIC sur la responsabilité des entreprises de respecter les droits de l'homme telle que prévue dans les Principes directeurs des Nations Unies sur les entreprises et les droits de l'homme. Ce guide a pour but d'apporter un appui aux sociétés du secteur des TIC lors de la transposition des principes identifiés par les Principes directeurs des Nations Unies dans leurs systèmes et cultures respectifs[41]. Ce guide fournit des orientations concrètes sur la manière dont les sociétés peuvent mettre en place des procédures internes systématiques en vue de se

38 Voir https://www.cybersecurityintelligence.com/cybercrime-coordination-unit-switzerland-cyco-2085.html.
39 Nations Unies, *Principes directeurs relatifs aux entreprises et aux droits de l'homme*, 2011.
40 Commission européenne, *Proposition de règlement relatif à la prévention de la diffusion de contenus à caractère terroriste en ligne*, 2018.
41 Shift et Institute for Human Rights and Business, *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights*, Commission européenne, juin 2013.

trouver mieux équipées pour traiter de manière adéquate et rapide les requêtes de suppression de données et/ou de contenus qui leur sont adressées par les pouvoirs publics, dans le respect des droits de l'homme. Il exhorte en outre les sociétés du secteur des TIC à communiquer sur ces efforts de manière effective et transparente, et leur donne des orientations à cette fin.

Les *Principes de Santa Clara sur la transparence et la responsabilité dans les pratiques de modération des contenus*, rédigés par plusieurs organisations universitaires et sans but lucratif dont Electronic Frontier Foundation, l'Union américaine pour les libertés civiles (ACLU) et le Centre pour la démocratie et la technologie, préconisent que les sociétés concernées publient le nombre de messages supprimés et de comptes suspendus temporairement ou définitivement, qu'elles notifient à chaque utilisateur les motifs ayant entraîné la suppression ou la suspension de son compte, et qu'elles lui accordent une réelle possibilité de se pourvoir d'un recours en temps opportun[42].

Étude de cas : Ranking Digital Rights

Ranking Digital Rights (RDR, classement des droits numériques) est un projet de recherche sans but lucratif qui relève de l'Open Technology Institute de New America. RDR publie un palmarès annuel des engagements et politiques des sociétés du secteur des TIC influant sur la liberté d'expression et la vie privée des utilisateurs, en se fondant sur le droit international des droits de l'homme. Par conséquent, l'indice de RDR montre clairement quelles sont les normes que les sociétés doivent suivre si elles veulent respecter leur engagement envers la liberté d'expression et la protection de la vie privée en tant que droits de l'homme, et promeut la transparence et la reddition de comptes chez ces sociétés par le biais de ses évaluations, qui sont d'accès public.

En 2019, l'Indice de responsabilité des entreprises[43] de RDR classait 24 sociétés à partir de 35 indicateurs qui portaient sur « les mécanismes de gouvernance des entreprises chargés d'identifier et de prévenir toute menace potentielle aux droits de l'homme de leurs utilisateurs », et rendait publiques les politiques qui affectent la liberté d'expression et la vie privée des utilisateurs[44]. En dépit d'une amélioration constatée au sein des sociétés ayant déjà fait l'objet d'une évaluation, des problèmes de transparence continuent de se poser pour ce qui a trait à la procédure de suppression des contenus. L'Indice a également mis en lumière que les sociétés ne prévoient toujours pas de mécanismes appropriés de réclamation et de recours qui pourraient contribuer à notifier tout problème et à y apporter réparation. Il convient cependant d'observer que les sociétés membres de la Global Network Initiative (voir ci-dessous) obtenaient un meilleur classement sur cet Indice que celles qui n'en font pas partie.

42 *The Santa Clara Principles On Transparency and Accountability in Content Moderation*, 2 février 2018.
43 Ranking Digital Rights, 2019 *Ranking Digital Rights Corporate Accountability Index*.
44 Voir https://rankingdigitalrights.org/about/our-work.

RDR inclut également, à la fin de son rapport, des recommandations spécifiques à l'intention des sociétés et des pouvoirs publics[45]. Les gouvernements peuvent en outre se référer aux rapports de RDR pour mieux comprendre les performances des sociétés concernées à l'aune des dispositions prévues dans le droit international des droits de l'homme.

Étude de cas : la Global Network Initiative

La Global Network Initiative (GNI) est une plateforme pluri-acteurs qui vise à protéger et faire progresser la liberté d'expression et la protection de la vie privée dans le secteur des TIC. Les Principes GNI, que toutes les sociétés membres de la GNI s'engagent à mettre en œuvre, fournissent un cadre évolutif pour la prise de décision responsable des sociétés, à l'appui des droits à la liberté d'expression et à la protection de la vie privée[46]. Vu que le nombre de sociétés adhérant à l'initiative GNI va croissant, l'on espère que les Principes « se confirment comme des normes mondiales en matière de droits de l'homme dans le secteur des TIC »[47], faisant dès lors progresser les droits de l'homme ainsi que la transparence et la responsabilité des sociétés du secteur des TIC.

Tous les deux ans, les sociétés participant à l'initiative GNI font l'objet d'une évaluation indépendante de leurs progrès dans la mise en œuvre des Principes GNI. Il s'agit de déterminer si les sociétés « déploient de bonne foi des efforts pour mettre en œuvre les Principes GNI, qui se traduisent par une amélioration progressive ». De cette manière, les sociétés sont évaluées par rapport à leur propre performance antérieure. L'évaluation porte sur les systèmes, politiques et procédures de la société, et s'accompagne d'un petit nombre d'études de cas pour déterminer de quelle manière la société concernée a traité des incidents particuliers et quelles améliorations pourraient être apportées en la matière. Ces évaluations sont conduites par un certain nombre d'institutions indépendantes[48] qui ont été habilitées par le conseil multipartite de l'initiative GNI, sur la base de critères d'indépendance et de compétence[49].

45 *Recommendations for governments*, in : Ranking Digital Rights, 2018 Corporate Accountability Index.
46 Global Network Initiative, *Principles on Freedom of Expression and Privacy*.
47 Voir https://globalnetworkinitiative.org/about-gni.
48 Voir https://globalnetworkinitiative.org/independent-assessors.
49 Global Network Initiative, *GNI Independence and Competency Criteria*. Mis à jour en août 2018.

Rapports de transparence

S'il est vrai que les gouvernements jouent un rôle de premier plan dans la promotion de la transparence et la reddition de comptes des réponses fondées sur les contenus en vue de prévenir et de lutter contre l'extrémisme violent et le terrorisme sur Internet, notamment en référence à un texte de loi ou à un code pénal, les sociétés du secteur des TIC peuvent à leur tour contribuer à renforcer la transparence et la reddition de comptes en la matière lorsque certains contenus leur sont signalés en vue d'être évalués.

La publication de rapports de transparence qui mettent en lumière la manière dont les entreprises ont traité la suppression de contenus dans leurs services peut constituer une étape importante pour que le grand public comprenne mieux la portée des suppressions de contenus et le type de contenus en ayant fait l'objet. En guise d'illustration d'une pratique gouvernementale, la loi allemande sur l'application du droit sur les réseaux sociaux (Netzwerkdurchsetzungsgesetz du 1er septembre 2017 (BGBl. I S. 3352), détaillée au premier chapitre, exige que les plateformes de réseaux sociaux recevant plus de 100 plaintes par année calendaire publient un rapport semestriel sur leur traitement des plaintes. Elle oblige également les sociétés concernées à notifier toute décision prise à la personne lui ayant adressé sa réclamation et à expliquer à l'utilisateur les raisons de la décision finale. Des dispositions similaires sont prévues par la Commission européenne dans sa proposition de Règlement relatif à la prévention de la diffusion de contenus à caractère terroriste en ligne. Des exigences de cette nature mettent sur pied des mécanismes qui réussissent à accroître la transparence sur la manière dont les sociétés concernées s'occupent de la réglementation des contenus sur les réseaux sociaux.

Étude de cas : Twitter

En vertu des règles et politiques de Twitter, « la transparence est vitale pour protéger la liberté d'expression »[50]. À cet égard, Twitter publie des rapports de transparence semestriels visant à mettre en exergue les nouvelles tendances et à fournir un espace ouvert de partage d'information[51].

Twitter a pour politique générale de prévenir ses utilisateurs dès la réception d'une demande d'information portant sur leur compte Twitter ou Periscope, en incluant une copie de la demande d'information, à moins que l'on ne lui ait interdit de le faire. Conformément à la politique de Twitter relative à la vie privée, il lui est possible aussi de divulguer aux forces de l'ordre des informations de compte en réponse à une requête officielle de divulgation d'urgence (par exemple au titre d'une décision de justice en vertu du Titre 18 du United States Code § 2702(b)(8), ou de la section 8 de la loi sur la protection des données de 1988 et 2003 en Irlande).

50 Voir https://help.twitter.com/fr/rules-and-policies/tweet-withheld-by-country.
51 Voir la dernière version : https://transparency.twitter.com/fr/information-requests.html#information-requests-jul-dec-2018.

Twitter coopère en outre avec diverses organisations telles que Parle-moi d'Islam (en France), Imams Online (au Royaume-Uni), ou True Islam (aux États-Unis), pour endiguer l'extrémisme violent sur sa plateforme. En vertu de sa politique sur l'appui aux forces de l'ordre, Twitter répond aux procédures judiciaires valides et conformes au regard de la législation applicable[52] et s'est doté de son propre site dédié pour les demandes émanant des forces de l'ordre[53].

Étude de cas : Boîte à outils pour la reddition de comptes et la transparence de l'Open Technology Institute

L'Open Technology Institute, qui fait partie de New America, une cellule de réflexion établie aux États-Unis, publie des boîtes à outils pour la reddition de comptes et la transparence qui lui permet d'évaluer les meilleures pratiques concernant les rapports de transparence des sociétés du secteur des TIC et de passer en revue les indicateurs utilisés par les principales sociétés dans leurs rapports[54].

Tout en reconnaissant que la pression publique en faveur de davantage de transparence a entraîné à une augmentation de la fréquence et de la portée des mesures prises par les sociétés du secteur des TIC à des fins de transparence, l'Open Technology Institute insiste sur la nécessité d'une plus grande normalisation dans la manière de présenter les rapports sur les suppressions de contenus ainsi que d'une définition du niveau de granularité des données incluses dans les rapports. La grande diversité des normes de présentation des rapports et des mesures constitue un obstacle à la comparabilité sectorielle entre toutes les entreprises, et donc empêche d'évaluer l'impact de la suppression des contenus sur la disponibilité et la propagation de l'extrémisme violent en ligne. Les mesures et indicateurs peuvent certes varier entre les différentes plateformes en raison de la diversité des contenus qu'elles hébergent, mais l'Open Technology Institute estime néanmoins qu'un ensemble uniforme de mesures à appliquer en fonction des besoins serait utile, et indispensable pour comparer les sociétés du secteur et procéder à des évaluations d'impact. En outre, les sociétés ne rapportent que rarement, et de manière hétéroclite, les suppressions qu'elles ont effectuées en violation de leurs propres conditions générales ou lignes directrices relatives aux contenus, même si Facebook, Google et Twitter (et, dans une moindre mesure, Microsoft) ont commencé à inclure cet indicateur dans leurs rapports en 2018.

52 Voir https://help.twitter.com/fr/rules-and-policies/twitter-law-enforcement-support.
53 Voir https://legalrequests.twitter.com/forms/landing_disclaimer.
54 New America Open Technology Institute, *The Transparency Reporting Toolkit: Content Takedown Reporting*, dernière mise à jour le 25 octobre 2018.

Pour attirer l'attention sur cette problématique, la fondation Electronic Frontier Foundation a lancé en mai 2019 son projet TOSsed out qui reprend certains des contenus retirés par les plateformes en vertu de leurs règles et conditions générales, perçues par cette fondation comme étant appliquées de manière trop inégale et inéquitable, et insuffisamment transparente[55].

B : Suivi et évaluation des réponses fondées sur les contenus

Cadres pour le suivi et l'évaluation

Pour garantir la légitimité et l'efficacité des mesures de prévention et de lutte contre l'extrémisme violent et le terrorisme en ligne, il est crucial d'en démontrer l'impact. Le suivi et l'évaluation continus des réponses fondées sur les contenus permettent d'éclairer les mesures législatives et politiques relatives aux procédures de signalement et de suppression de contenus, notamment par l'amélioration du ciblage et de l'identification des contenus et par la prise en compte des risques posés aux droits de l'homme lorsqu'ils se présentent.

L'insuffisance actuelle de travaux de recherche et de données empiriques concernant les réponses fondées sur les contenus et leur efficacité est particulièrement alarmante, puisqu'elle signifie que les pouvoirs publics et les sociétés du secteur des TIC pourraient mal affecter leurs précieuses ressources financières et humaines et mal utiliser leurs programmes, ce qui à son tour pourrait entraîner des conséquences imprévues, éventuellement dommageables pour les droits de l'homme. C'est pourquoi les gouvernements sont encouragés à s'inspirer des cadres de suivi et d'évaluation d'autres secteurs, dont ceux de la santé publique, de la publicité commerciale et du marketing, s'il y a lieu.

Établissement de cadres de suivi et d'évaluation

Les cadres de suivi et d'évaluation sont fondamentaux pour l'effectivité et l'efficacité des réponses à l'extrémisme violent et au terrorisme en ligne fondées sur les contenus, raison pour laquelle ils convient de les intégrer dans les législations et politiques pertinentes, ainsi que dès le départ dans leur mise œuvre concrète[56].

Les gouvernements sont encouragés à se doter, en coopération avec un grand nombre de parties prenantes y compris le secteur des TIC, la société civile et les institutions universitaires, de méthodes et moyens réalistes pour mesurer l'impact de la législation, des politiques et des programmes. Ceci signifie qu'afin de procéder aux évaluations d'impact il convient, dès le départ, de définir clairement les objectifs que l'on souhaite atteindre quant à l'impact des réponses spécifiques fondées sur les contenus (éventuellement sous-tendues par les théories du changement esquissées dans chacune des politiques) et de déterminer des points de référence objectifs. Le suivi et l'évaluation doivent être réalisés sur la base de données, de

55 Voir https://www.eff.org/tossedout.
56 Voir, par exemple, la *Proposition de Règlement relatif à la prévention de la diffusion de contenus à caractère terroriste en ligne* de la Commission européenne, en particulier les articles 21 et 23 sur le suivi et l'évaluation.

définitions, de méthodologies et d'indicateurs communiqués ouvertement, utilisés de manière uniforme, et comparables.

Mesures et outils quantitatifs

Compte tenu des vastes quantités de données disponibles, il est plus impératif que jamais que les cadres de suivi et d'évaluation soient centrés sur un ensemble déterminé de données pour que l'on puisse en déduire des informations utiles pour le législateur et les décideurs politiques. En outre, il convient d'établir des procédures de collecte de données et d'informations qui soient respectueuses des droits de l'homme tels que le droit à la liberté d'expression et à la protection de la vie privée, et du droit à une protection égale sans discrimination, ce qui pourrait restreindre la faculté de l'État de réunir certaines données ou, du moins, de les utiliser.

Sont énumérés ci-après, certains des éléments fondamentaux pouvant être envisagés pour le suivi et l'évaluation des réponses fondées sur les contenus ; tous ne sont pas forcément disponibles aux pouvoirs publics dans tous les pays.

- Nombre de signalements en vue d'une suppression, et le motif spécifique du signalement ;
- Base juridique du signalement (législation nationale et/ou conditions générales de la société du secteur des TIC) ;
- Nature de la personne physique ou morale à l'origine du signalement, notamment institutions gouvernementales (éventuellement en ventilant les données entre unités chargées du signalement des contenus et autres entités), système judiciaire, société civile, sociétés du secteur des TIC, particuliers ;
- Moyens utilisés pour effectuer le signalement (requête adressée à une unité chargée du signalement des contenus, outils à la disposition de signaleurs de confiance, formulaires accessibles au public) ;
- Nombre total de signalements par société du secteur des TIC ;
- Durée de l'examen par la société concernée du contenu lui ayant été signalé ;
- Nombre et pourcentage de signalements ayant entraîné une suppression ;
- Si possible et s'il y a lieu, nombre de vues du contenu avant sa suppression et nombre d'interactions auxquelles il a donné lieu, ainsi que durée de la présence du contenu en ligne avant d'être retiré ;
- Nombre total de suppressions, ventilé par motifs de la suppression ;
- Nombre de suppressions ayant donné lieu à une contestation, et mécanisme de recours spécifique utilisé (judiciaire, administratif, mécanisme de réclamation de la société concernée) ;
- Nombre de signalements respectivement acceptés et refusés ;
- Le cas échéant, aperçu des sanctions, notamment financière et pénales.

Outils et capacités pour le suivi et l'évaluation

La performance quantitative des réponses fondées sur les contenus peut faire l'objet d'un suivi général par le biais des mécanismes mis en place à cette fin par les pouvoirs publics et/ou le système judiciaire, mais aussi d'une analyse plus précise au moyen d'outils tels que ceux des sociétés du secteur des TIC.

Les signalements et suppressions de contenus sur injonction des tribunaux doivent apparaître dans les systèmes informatiques utilisés habituellement par l'appareil judiciaire, et par ailleurs les pouvoirs publics devraient être en mesure d'y accéder, comme c'est le cas pour d'autres procédures judiciaires. Il convient que le gouvernement définisse les vecteurs adéquats pour recevoir régulièrement les données mises à jour par les sociétés du secteur des TIC concernant les signalements reçus et les suppressions effectuées en vertu de leurs propres conditions générales ; les sociétés du secteur des TIC sont tenues de se conformer à ces demandes d'information de la part du gouvernement tant que celles-ci respectent le droit international des droits de l'homme et la législation nationale. Les unités chargées du signalement des contenus disposeront également d'un système leur permettant de consigner leurs signalements, et le gouvernement doit pouvoir y accéder également.

Même si l'on tient compte des considérations ci-dessus, la quantité de données à introduire dans le système de suivi et d'évaluation sera considérable. L'accroissement de la capacité gouvernementale d'absorber cette masse de données et de visualiser des ensembles complexes de données peut conférer une valeur ajoutée significative à l'adaptation permanente des réponses fondées sur les contenus et des garanties correspondantes en matière de droits de l'homme. Les gouvernements peuvent également juger bon de financer des projets menés par des institutions universitaires et par la société civile de façon à leur permettre d'élaborer des approches de suivi et d'évaluation innovantes.

Mesures et outils qualitatifs

Les approches quantitatives susmentionnées vont très probablement permettre de recueillir une ample gamme d'informations. Il est à prévoir cependant que les résultats de l'évaluation seront sensiblement supérieurs si ces informations sont conjuguées à des éléments qualitatifs. Pour ne citer qu'un exemple, les spécialistes des forces de l'ordre réalisent des évaluations qualitatives avec les unités chargées du signalement des contenus, lors de Journées conjointes d'évaluation, précisément pour déterminer la prévalence et les structures prédominantes observées dans l'utilisation d'une plateforme donnée par les extrémistes violents et les terroristes[57]. D'autres initiatives en ce sens pourraient par exemple s'appuyer sur des entretiens (semi)structurés avec des personnes qui produisent, partagent ou aiment l'extrémisme violent et le terrorisme en ligne, et chercher à comprendre (là aussi, par le biais d'interactions individualisées) de quelle manière les internautes sont exposés à ce type de contenus et comment ils y réagissent.

Une évaluation qualitative va non seulement permettre de structurer des masses de données autrement écrasantes, mais aussi d'accroître la transparence entre l'ensemble des acteurs des pratiques identifiées ; ainsi, le processus d'examen qualitatif deviendra partie intégrante de la réflexion sur les réponses fondées sur les contenus et contribuera à leur optimisation.

La valeur ajoutée de la transparence du suivi et de l'évaluation

Il conviendra d'afficher publiquement les résultats du suivi et de l'évaluation, dès que possible, de façon à ce que les acteurs non gouvernementaux tels que le secteur des TIC, les organisations de la société civile et les institutions universitaires soient en mesure de les examiner, de les

57 Europol, *Referral Action Day with six EU Member states and Telegram*, 5 octobre 2018.

analyser et de formuler des suggestions en vue de révisions potentielles. Il serait même possible d'aller plus loin, en fournissant un accès aux données par le biais de ce que l'on appelle les jeux de données ouverts ; l'examen de ces ensembles de données par des acteurs non gouvernementaux permettrait de comprendre les jeux de données de manière encore plus approfondie, et partant, de renforcer les cadres de suivi et d'évaluation.

Étant donné que même des institutions pleinement fonctionnelles n'échappent pas au défi posé par les biais analytiques intrinsèques, il conviendrait que le suivi et l'évaluation soient réalisés, si possible, par des organes autonomes du gouvernement (tels que les bureaux nationaux de la statistique), ou que l'on fasse au moins appel à leur expertise technique lors de la création des systèmes de suivi et d'évaluation. De surcroît, des évaluations régulières et indépendantes, portant à la fois sur les systèmes et sur les échantillons de données collectées, peuvent aider à y apporter un regard nouveau susceptible de contribuer à l'amélioration générale des cadres de suivi et d'évaluation.

Défis posés au suivi et à l'évaluation

Le suivi et l'évaluation de l'impact obtenu par les réponses fondées sur les contenus comportent un ensemble de défis intrinsèques. Tout d'abord, bien que cela soit difficile, il est nécessaire d'évaluer si la suppression du contenu entraîne la migration des contenus à caractère extrémistes violents et terroristes vers d'autres plateformes éventuellement moins réglementées. Par ailleurs, la diversité des expériences en matière de suppression de contenus parmi les plateformes souligne la nécessité d'adopter une approche pleinement sectorielle qui évalue la diminution globale de ce type de contenus plutôt que de se contenter d'un « succès » rencontré par l'une ou l'autre plateforme qui risquerait, par contre, de se traduire par une apparition renforcée de contenus à caractère terroriste dans d'autres plateformes, généralement de plus petite dimension, moins réglementées, ou utilisant des canaux pratiquant davantage le cryptage.

Si elle est conçue soigneusement, l'évaluation est à même de relever certains de ces défis. Cependant, il convient aussi d'assurer la transparence des cadres globaux de suivi et d'évaluation quant aux limites des méthodes qu'ils utilisent, aux problèmes concernant les données pouvant être collectées (tant au niveau technique qu'au regard des exigences relatives au respect de la vie privée), et par conséquent aux résultats de l'évaluation fondée sur ces méthodes et données.

C : Les procédures automatisées

Minimiser les risques associés aux procédures automatisées

À mesure qu'un nombre croissant d'entreprises mettent au point et utilisent des procédures automatisées qui accélèrent l'identification et la suppression des contenus, le rôle des sociétés du secteur des TIC dans la promotion de mécanismes effectifs de transparence et de reddition de comptes gagne en pertinence, en particulier compte tenu du risque d'atteintes au droit à la liberté d'expression que peuvent poser ces procédures automatisées. Il convient donc que les sociétés du secteur des TIC veillent à ce que les procédures automatisées soient révisées de manière efficiente et efficace et que des mécanismes de recours adéquats soient mis en place.

Les procédures automatisées peuvent entraîner de graves infractions aux droits de l'homme des utilisateurs concernés lorsque l'accès à des contenus est bloqué ou que ceux-ci sont supprimés. Par exemple, après l'introduction par YouTube d'une nouvelle technologie afin de détecter automatiquement et de supprimer les contenus enfreignant ses conditions générales, des militants des droits de l'homme se sont plaints que des milliers de vidéos qui avaient été postées pour documenter des allégations de crimes de guerre aient été retirées de YouTube parce que les procédures automatisées utilisées les avaient évaluées comme étant en violation des lignes directrice relatives aux contenus[58].

Exemples de procédures automatisées visant à détecter et supprimer des contenus à caractère extrémiste violent et terroriste

Les principales sociétés du secteur des médias sociaux utilisent de plus en plus des procédures automatisées dans le but de détecter, signaler et/ou supprimer des contenus sur leurs plateformes ; c'est le cas en particulier de Facebook, Twitter et YouTube. Chacune de ces plateformes utilise des types de procédures automatisées différents[59].

Facebook : Facebook a recours à l'apprentissage machine pour évaluer les messages susceptibles d'indiquer un soutien à Da'esh/EIIL ou Al-Qaïda. Afin d'aider l'équipe des analystes, cet outil génère une note indiquant la probabilité que le message enfreigne les politiques de Facebook en matière de lutte contre le terrorisme. En outre, Facebook a commencé à appliquer l'intelligence artificielle (IA)[60]. Celle-ci est utilisée en particulier pour diriger un nouveau contenu récemment téléchargé vers un analyste humain, pour identifier des pages regroupées, des messages, des groupes ou des profils dans lesquels figure du contenu à caractère terroriste, ainsi que pour recouper des photos et des vidéos avec une base de données existante. D'après le directeur de la politique de lutte contre le terrorisme de Facebook, cette société serait en train de démarrer le développement d'une IA fondée sur des textes. De plus, Facebook utilise l'IA pour réduire la durée durant laquelle les comptes de terroristes récidivistes sont actifs Facebook[61].

Twitter : Twitter se concentre de plus en plus sur l'identification proactive des comptes et des comportements susceptibles de poser un problème sur sa plateforme[62]. Un rapport indique que 91 % des suspensions de compte, sur un total de 205 156, avaient

58 Document remis par AccessNow à David Kaye, Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, apportant la réponse de cette organisation aux questions se rapportant à une « Étude sur la réglementation des contenus à l'ère numérique », janvier 2018.
59 Les entreprises figurant ici sont citées dans Nikita Malik, *The Fight Against Terrorism Online: Here's The Verdict*, Forbes, 20 septembre 2018.
60 *A View from the CT Foxhole: An Interview with Brian Fishman, Counterterrorism Policy Manager, Facebook*. Centre de lutte contre le terrorisme, Académie militaire des États-Unis. Septembre 2017, Volume 10, no 8.
61 Facebook, *Hard Questions: How We Counter Terrorism*, 15 juin 2017.
62 Twitter, *How Twitter is fighting spam and malicious automation*, 26 juin 2018.

été déclenchées de manière proactive par des outils internes privatifs. De fait, les signalements par les pouvoirs publics ont représenté moins de 0,1 % de toutes les suspensions durant la période en examen dans le rapport.

YouTube : En 2018, YouTube soulignait dans un message de blog que les « machines nous permettent de repérer à grande échelle les contenus à analyser, ce qui nous a aidé à supprimer des millions de vidéos en infraction avant même qu'elles ne soient vues ». D'après les statistiques fournies, d'octobre à décembre 2017, YouTube a supprimé 8 millions de vidéos, dont 6,7 millions avaient été détectées pour analyse par des machines ; de ces 6,7 millions, 76 % ont été supprimées avant d'être vues[63].

Droits de l'homme et intelligence artificielle : le rôle de l'État

Les sociétés du secteur des TIC recourent de de plus en plus souvent à l'intelligence artificielle (IA) à des fins de modération de contenus, en particulier par le biais de procédures automatisées. Des systèmes d'IA sont utilisés pour contrôler les contenus placés en ligne par les internautes et repérer les éventuelles violations à leur conditions générales d'utilisation. S'il est vrai que les systèmes d'IA peuvent être d'une grande efficacité à des fins de repérage de contenus à caractère terroriste ou extrémiste violent, les algorithmes d'IA pourraient néanmoins signaler par erreur comme étant illicite un contenu légitime, ce qui, si l'accès au contenu est bloqué ou si celui-ci est supprimé, pourrait mener à une grave atteinte aux droits de l'homme ou à d'autres droits des utilisateurs affectés. C'est pourquoi il est nécessaire de légiférer afin de réglementer l'utilisation des outils s'appuyant sur l'IA à des fins de modération des contenus ainsi que les paramètres que ces outils utilisent. Cette réglementation doit inclure l'obligation de proposer des outils de signalement ou de remontée d'information aux internautes qui estiment que leur contenu a été supprimé de manière illicite[64].

Le Rapporteur spécial des Nations Unies sur la liberté d'expression recommande aux « États [de] veiller à ce que les droits de l'homme occupent toujours une place centrale dans la conception, la mise en place et la mise en œuvre des systèmes d'IA du secteur privé »[65]. Le Rapporteur spécial a également indiqué que les États peuvent s'acquitter de leurs obligations en matière de droits de l'homme « en prenant des mesures juridiques destinées à restreindre ou à influencer la création et la mise en œuvre des applications d'IA, en adoptant des politiques réglementant les marchés publics pour l'acquisition d'applications d'IA auprès d'entreprises du secteur privé, en établissant des mécanismes d'autorégulation et de corégulation et en renforçant la capacité des entreprises du secteur privé à reconnaître l'importance du droit à la liberté d'opinion et d'expression et à lui donner la priorité dans leurs activités[66].

63 Voir https://youtube.googleblog.com/2018/04/more-information-faster-removals-more.html.
64 Voir, par exemple, Commission européenne, *Proposition de règlement relatif à la prévention de la diffusion de contenus à caractère terroriste en ligne*, en particulier les articles 9 et 10 sur les sauvegardes spécifiques à mettre en place lors du recours à des outils automatisés.
65 Assemblée générale des Nations Unies, *Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, technologies de l'intelligence artificielle et répercussion sur l'environnement de l'information*, (A/73/348), § 63, 29 août 2018.
66 *Ibidem*, § 20.

Enfin, il faudrait toujours assortir les procédures automatisées d'un examen par un être humain lorsqu'une décision de suppression de contenus doit être prise au motif qu'il s'agirait d'un contenu promouvant l'extrémisme violent ou le terrorisme, ainsi que lors du traitement des recours interposés. La législation nationale peut définir les responsabilités à cet égard.

Réponses fondées sur les contenus :

3. La collaboration pluri-acteurs à l'appui des réponses fondées sur les contenus

Ce chapitre vise à apporter un appui aux législateurs et décideurs politiques ainsi qu'aux praticiens en illustrant par des études de cas et des pratiques existantes ce que peut être la collaboration entre pouvoirs publics, sociétés du secteur des TIC et société civile. Ce chapitre accordera son attention en particulier à trois types de collaboration : entre pouvoirs public, sociétés du secteur des TIC et société civile ; entre les différentes sociétés du secteur des TIC ; et entre sociétés du secteur des TIC et la société civile. Ce chapitre comporte deux sections, à savoir : Collaboration pluri-acteurs, et Autres initiatives.

Bonnes pratiques pertinentes des Recommandations de Zurich-Londres :

Bonne pratique no 3 : *Mettre en place une stratégie claire de lutte contre l'extrémisme violent et le terrorisme en ligne, basée sur une approche à la fois sociétale et pangouvernementale et coordonnant des mesures fondées tant sur les contenus que sur la communication, ainsi que des activités hors ligne portant notamment sur l'éducation et sur la participation des organisations de la société civile, suivant les besoins.*

Bonne pratique no 6 : *Adopter une approche pluri-acteurs intégrant les gouvernements, le secteur des technologies de l'information et de la communication et les organisations de la société civile pour prévenir et lutter contre l'extrémisme violent et le terrorisme en ligne.*

Bonne pratique no 9 : *Mettre en place, chaque fois que nécessaire, une collaboration efficace et promouvoir le renforcement de la participation du secteur des technologies de l'information et de la communication, ainsi que la coopération avec les organisations de la société civile dans le traitement des contenus à caractère extrémiste violent et terroriste sur l'internet et sur les plateformes des médias sociaux.*

Bonne pratique no 11 : *Admettre le rôle de secteur des technologies de l'information et de la communication dans le traitement efficace de la disponibilité et de l'accessibilité des contenus à caractère extrémiste violent et terroriste sur l'internet et sur les plateformes des médias sociaux.*

INTRODUCTION

Il ressort clairement des déclarations de mission des principales entreprises des technologies de l'information et de la communication que le secteur, et en particulier les entreprises des médias sociaux, est devenu pour la société un outil essentiel au regard de l'accès à l'information ainsi que du partage et de la discussion de l'information. Le PDG de Facebook a décrit la mission de l'entreprise comme suit : « rapprocher [les personnes] et édifier une communauté mondiale »[67]. VKontakte définit ainsi sa mission : « réunir des gens, services et entreprises en créant des outils de communication faciles et pratiques[68]. L'objectif de Google est « d'organiser les informations à l'échelle mondiale pour les rendre accessibles et utiles à tous »[69]. Tencent s'emploie à « améliorer la qualité de la vie par le biais de services à valeur ajoutée sur Internet »[70].

En raison de leur contrôle effectif sur une partie significative de l'infrastructure sur laquelle repose Internet, les sociétés privées du secteur des TIC jouent un rôle croissant dans les efforts visant à contrer et prévenir l'extrémisme violent et le terrorisme à l'ère du numérique. Compte tenu du rôle extraordinaire qui est le leur, ainsi que de la nature transnationale de l'espace numérique, une collaboration efficace entre tous les acteurs concernés (pouvoirs publics, secteur des TIC et société civile) est primordiale pour prévenir et lutter contre l'extrémisme violent et le terrorisme sur Internet. Toutefois, ces entreprises privées sont très souvent confrontées à de nombreux défis en matière de corégulation et d'autorégulation de leurs plateformes, en particulier en matière de droits de l'homme[71].

L'accroissement des efforts déployés en vue de prévenir et de lutter contre l'extrémisme violent et le terrorisme en ligne, qui conjuguent des mécanismes publics, public-privé et privés, sont révélateurs d'une évolution plus fondamentale dans la manière dont les entreprises mènent leurs activités au niveau mondial. À la lumière de cette tendance, il est possible de voir la coopération entre une ample gamme d'acteurs (qu'il s'agisse de pouvoirs publics, d'entreprises ou de la société civile) comme une réaction concrète destinée à combler certaines des lacunes constatées en matière de gouvernance dans les approches plus traditionnelles de la réglementation. Les initiatives de cette nature visent en effet à étayer une gouvernance efficace, en faisant en sorte que les acteurs du secteur commercial inscrivent leurs activités dans le cadre posé par l'état de droit et le respect des droits de l'homme. Ensemble, des groupes composés d'acteurs variés peuvent forger de meilleures approches et solutions que ne le ferait chaque groupe de parties prenantes œuvrant de manière isolée.

67 Mark Zuckerberg, Building Global Community, 16 février 2017.
68 Voir https://vk.com/about.
69 Voir https://www.google.com/about.
70 Voir https://www.tencent.com/en-us/abouttencent.html.
71 Institut danois pour les droits de l'homme, Submission to Special Rapporteur on Freedom of Expression, 28 janvier 2016.

A : Collaboration pluri-acteurs

Le rôle clé dévolu aux institutions publiques dans la collaboration pluri-acteurs

Il incombe au premier chef aux États de lutter contre l'extrémisme violent et le terrorisme. Comme précisé au premier chapitre, le législateur et les décideurs politiques ont de ce fait la responsabilité de mettre sur pied les cadres adéquats, conformément aux obligations de l'État en vertu du droit international mais également en conformité avec son droit interne. Les pouvoirs publics encadrent les sociétés du secteur des TIC pour veiller à ce que la corégulation et l'autorégulation soient en cohérence avec le droit international des droits de l'homme et le droit interne des États.

Au-delà de cet angle strictement juridique, les pouvoirs publics ont un rôle important à jouer en matière de coordination et d'interaction avec le secteur des TIC et la société civile, en créant et soutenant des plateformes collaboratives. Celles-ci sont particulièrement pertinentes au regard des unités nationales de signalement de contenus, chargées de la recherche et de la détection de contenus à caractère terroriste et extrémiste violent en ligne et des requêtes de suppression de ces contenus aux sociétés du secteur des TIC par le biais de procédures de signalement. Les plateformes collaboratives peuvent apporter des contributions précieuses aux pouvoirs publics et, partant, aider à favoriser un processus décisionnel plus inclusif dans le cadre des réponses fondées sur les contenus. Des vecteurs de communication ouverts entre les parties prenantes compétentes permettent en outre d'identifier les lacunes dans les activités de prévention et de lutte contre l'extrémisme violent et le terrorisme en ligne, et de tenter de les combler, ainsi que de désamorcer les conflits d'intérêt potentiels. L'institutionnalisation et la coordination des efforts peuvent également favoriser le lancement d'actions complémentaires par les diverses parties prenantes ainsi que la mobilisation commune de ressources humaines et financières.

Étude de cas : Unités chargées du signalement des contenus sur internet à l'échelon européen et national

L'Unité chargée du signalement des contenus sur internet de l'Union européenne (UE) fait partie du Centre européen de lutte contre le terrorisme d'Europol. Elle regroupe une équipe d'experts dans les domaines du terrorisme d'inspiration religieuse, des langues, des développeurs informatiques et des représentants des forces de l'ordre spécialisées dans la lutte contre le terrorisme[72]. Elle est entrée en fonction en 2015 avec le mandat suivant :

- Apporter un appui aux autorités compétentes de l'UE au moyen d'analyses stratégiques et opérationnelles ;
- Signaler les contenus à caractère terroriste et extrémiste violent en ligne et les partager avec les partenaires compétents ;

72 Voir https://www.europol.europa.eu/about-europol/eu-internet-referal-unit-eu-iru.

- Détecter les contenus Internet utilisés par les réseaux de passeurs pour attirer les migrants et les réfugiés et en demander la suppression ;
- Procéder rapidement au signalement et apporter un appui à la procédure, en étroite coopération avec le secteur[73].

L'Unité chargée du signalement des contenus sur internet est chargée de l'évaluation des contenus en ligne et de les signaler aux sociétés respectives du secteur des TIC hébergeant un contenu devant être supprimé. D'après le rapport de transparence de 2017 de l'Unité de l'UE chargée du signalement des contenus sur internet, « la coopération avec le secteur privé est fondamentale pour la prévention »[74]. Depuis le début de ses activités en juillet 2015 jusqu'en décembre 2017, l'Unité de l'UE chargée du signalement des contenus sur internet a procédé à l'analyse de 46 392 éléments de contenus à caractère terroriste, contenus qui ont déclenché 44 807 décisions de signalement, avec un taux de suppression des contenus de 92 pour cent[75]. La Directive de l'UE sur la lutte contre le terrorisme prévoit un certain nombre de sauvegardes en matière de suppression de contenus, précisées en son article 21 (3) : « Les mesures visant à supprimer des contenus et à bloquer leur accès doivent être établies à la suite de procédures transparentes et fournir des garanties suffisantes, en particulier pour veiller à ce que ces mesures soient limitées à ce qui est nécessaire et proportionné, et que les utilisateurs soient informés de la raison de ces mesures. Les garanties relatives à la suppression ou au blocage incluent aussi la possibilité d'un recours juridictionnel. »[76] Lorsque le contenu analysé est déclaré en infraction en vertu du mandat d'Europol, les contenus concernés sont signalés à la société du secteur des TIC détentrice de la plateforme sur laquelle ils ont été détectés. Cependant, la décision de supprimer ou non le contenu signalé incombe en dernier ressort à la société concernée, après l'avoir évalué à l'aune de ses conditions générales d'utilisation. L'Unité de l'UE chargée du signalement des contenus sur internet n'est pas compétente du point de vue juridique pour demander aux sociétés concernées de retirer des contenus.

Des unités similaires chargées de signaler les contenus existent au Royaume-Uni, en France et aux Pays-Bas. Europol a déclaré par ailleurs que des mécanismes parallèles ont été mis sur pied en Belgique, en Allemagne et en Italie[77].

En vue de promouvoir une approche coordonnée entre les pouvoirs publics et les sociétés du secteur des TIC, l'Unité de l'UE chargée du signalement des contenus sur internet organise des journées d'action conjointes en matière de signalement, connues sur le nom de Referral Action Days, qui réunissent des représentants des

73 *Ibidem*.
74 Unité de l'UE chargée du signalement des contenus sur internet, *Transparency Report 2017*.
75 *Ibidem*.
76 *Ibidem*.
77 Europol, *Referral Action Day*, 2018.

unités spécialisées nationales en matière de signalement des contenus sur Internet des forces de l'ordre de différents pays, de l'Unité de l'UE chargée du signalement des contenus sur internet et de sociétés du secteur des TIC[78].

Le recours croissant aux signalements par les unités spécialisées a fait l'objet de critiques de différentes organisations de la société civile telles que la Global Network Initiative (GNI), dans la mesure où ces signalements ne sont pas accompagnés d'un accès adéquat à des voies de recours pour les utilisateurs et le public, ni d'un système de reddition de comptes et de transparence[79]. La GNI a en outre fait état dans une déclaration de son inquiétude face au fait que certaines unités spécialisées dans le signalement pourraient être autorisées à détecter et signaler des contenus qui certes enfreignent les conditions générales d'utilisation de la société du secteur des TIC, mais sans pour autant déterminer si le contenu est en violation de la législation nationale[80].

Collaboration pluri-acteurs : tirer parti des forces de chacune des parties prenantes

Une approche à multiples parties prenantes a beaucoup plus de probabilités de réussir durablement si tous les acteurs impliqués partagent une même vision de leurs rôles et responsabilités respectifs et reconnaissent leurs points forts tout comme leurs limites. Une telle approche sera en mesure de fédérer le savoir-faire et l'expertise au niveau politique, juridique, sociétal et technique qui sont nécessaires pour s'attaquer à la disponibilité et à l'accessibilité de contenus à caractère extrémiste violent et terroriste sur Internet.

Étude de cas : Les signaleurs de confiance chez YouTube, et son programme de contributeurs

En 2012, YouTube a mis au point un programme de signaleurs de confiance[81]. Ce programme permet à des bénévoles invités à titre individuel, à des agences gouvernementales et à des organisations non gouvernementales, particulièrement actifs dans le signalement de contenus en violation des lignes directrices de la communauté YouTube, d'accéder à des outils qui les aideront à être plus efficaces dans leur action (à noter que le programme des signaleurs de confiance n'inclut pas

78 Europol, *EU Law Enforcement and Google Take on Terrorist Propaganda in Latest Europol Referral Action Days*, 16 juillet 2018. Europol, Referral Action Day, 2018.
79 Voir Global Network Initiative, *Extremist Content and the ICT Sector*, 2016, et Jason Pielemeier et Chris Sheehy, *Understanding the Human Rights Risks Associated with Internet Referral Units*, Global Network Initiative, 25 février 2019.
80 Global Network Initiative, *Understanding the Human Rights Risks Associated with Internet Referral Units*. 25 février 2019.
81 Voir https://support.google.com/youtube/answer/7554338?hl=en&ref_topic=2803138.

le signalement de contenus qui exigeraient la fermeture immédiate du compte en vertu du droit national). Une fois ces contenus signalés, les équipes de modération de contenus de YouTube formées à cette fin examinent les contenus afin de déterminer s'il convient ou pas de supprimer les vidéos signalées. Puisque les signaleurs de confiance sont censés détecter les contenus avec un degré élevé d'exactitude, les contenus sur lesquels ils attirent l'attention sont examinés en priorité. Ils reçoivent aussi un outil qui leur permet de signaler plusieurs vidéos en même temps, ont un meilleur accès aux informations sur les décision prises par l'équipe de YouTube quant à la suppression de contenus et, dans le cas des organisations de la société civile, reçoivent des formations en ligne.

Comme indiqué dans le rapport de transparence de YouTube, au cours de la période allant de janvier à mars 2019, les signaleurs de confiance à titre privé ont été à l'origine du signalement du plus grand nombre de vidéos détectées par des personnes et ayant ensuite été supprimées (1 396 945 vidéos supprimées, à comparer aux 4 022 signalées par des ONG et 16 par des agences gouvernementales), ce qui représente environ un sixième des contenus retirés à la suite d'un signalement automatique (6 372 936 vidéos)[82].

B : Autres initiatives

Initiatives menées par le secteur des TIC et la société civile

Les plateformes des médias sociaux sont devenues pour la société un outil essentiel au regard de l'accès à l'information ainsi que du partage et de la discussion de l'information. Les sociétés du secteur des TIC sont très souvent confrontées à de nombreux défis en matière de corégulation et d'autorégulation de leurs plateformes, en particulier en matière de droits de l'homme tels que liberté d'expression et droit à la protection de la vie privée. En réponse à ces défis, le secteur des TIC a lancé diverses initiatives portant notamment sur : le partage entre entreprises des connaissances et des technologies ; la création de plateformes interactives pour la modération des contenus, dotées d'outils et de ressources ad hoc ; des stages de formation sur les différentes approches à la suppression des contenus, organisés par les plus grandes entreprises à l'intention des plus petites. Ces initiatives peuvent devenir des mécanismes efficaces de prévention et de lutte contre les contenus à caractère terroriste et extrémiste violent sur Internet.

Les sociétés du secteur des TIC peuvent envisager librement d'introduire et de mettre en œuvre des pratiques individuelles de traitement de l'extrémisme violent et du terrorisme en ligne, telles que codes de conduite ou codes déontologiques la diffusion d'images, de vidéos et d'autres supports d'information visuels ; ces pratiques pourraient également figurer dans leurs conditions générales. Outre le fait de contribuer à la sensibilisation et la responsabilisation des entreprises concernées, ces pratiques apporteraient un complément à la législation nationale.

82 Voir https://transparencyreport.google.com/youtube-policy/removals?hl=fr.

Étude de cas : Le Forum mondial de l'Internet contre le terrorisme

En 2017, YouTube, Facebook, Microsoft et Twitter ont fondé le Forum mondial de l'Internet contre le terrorisme, qui s'est donné pour mission de « perturber substantiellement l'aptitude des terroristes à faire l'apologie du terrorisme, à diffuser de la propagande à caractère extrémiste violent et à exploiter ou glorifier sur nos plateformes des actes de violence commis dans le monde réel »[83]. En 2019, Dropbox a rejoint le Forum.

Le Forum vise à partager des technologies et des outils et à organiser des stages de formation à l'intention des plus petites entreprises du secteur, en partenariat avec Tech Against Terrorism qui relève de l'ONU, concernant la manière de traiter les contenus à caractère terroriste. Par exemple, le Forum a constitué une banque de données qui permet aux entreprises du secteur de créer une « empreinte numérique » pour tout contenu à caractère terroriste mis en ligne (« banque de données de partage des empreintes numériques »). En juin 2019, cette base de données contenait plus de 200 000 empreintes numériques[84].

À la suite de l'adoption en mai 2019 de l'Appel de Christchurch pour supprimer les contenus terroristes et extrémistes violents en ligne, le Forum s'est engagé à se centrer également sur les réponses aux crises en « introduisant des protocoles conjoints pour les incidents relatifs à des contenus, dans le but d'apporter une réponse à des événements émergents ou actifs tels que l'ignoble attentat de Christchurch, de sorte que l'information pertinente puisse être partagée et traitée avec célérité et efficacité pour donner lieu aux actions qui s'imposent par toutes les entreprises membres du Forum »[85].

New America a fait valoir ses préoccupations quant aux initiatives de partage des connaissances du Forum. D'après cette organisation, le Forum n'a pas les capacités nécessaires pour évaluer et contrôler le succès des initiatives, alors que celles-ci risquent d'évincer l'élaboration de pratiques innovantes par de plus petites entreprises susceptibles d'œuvrer avec plus d'efficacité. Étant donné que pour l'essentiel ce sont les membres du Forum qui établissent les bonnes pratiques partagées ensuite avec les plateformes plus petites, sans une évaluation soignée et stratégique la faculté des plateformes de petite dimension de développer et mettre en œuvre de nouvelles stratégies innovantes devient limitée[86].

83 Voir https://www.gifct.org/about.
84 *Ibidem*.
85 Voir Facebook, *Global Internet Forum To Counter Terrorism: An Update on Our Progress Two Years on*, 24 juillet 2019, et Microsoft, *The Christchurch Call and Steps to Tackle Terrorist and Violent Extremist Content*, 15 mai 2019.
86 Spandana Singh, *Taking Down Terrorism: Strategies for Evaluating the Moderation and Removal of Extremist Contents and Accounts*. New America.

Étude de cas : Tech Against Terrorism

Tech Against Terrorism, initiative lancée sous l'égide des Nations Unies, est un partenariat public-privé[87]. Tech Against Terrorism se charge depuis 2016 du suivi de l'usage d'Internet par les terroristes ; ses travaux de recherche ont montré que parmi les 50 principales plateformes utilisées par les groupes terroristes et extrémistes violents, près de la moitié sont de petite taille, voire des micro-plateformes. Tech Against Terrorism entend se tourner en particulier vers ces plus petites entreprises, qui souvent ne disposent pas des ressources financières, humaines et techniques nécessaires pour prévenir efficacement et lutter contre l'utilisation abusive de leurs plateformes par l'extrémisme violent et le terrorisme.

Les entreprises qui adhèrent à Tech Against Terrorism conviennent de respecter l'Engagement de Tech Against Terrorism[88], qui comporte six principes directeurs pour les bonnes pratiques, simples et accessibles : respecter la liberté d'expression ; respecter le droit des internautes à exprimer des avis et des opinions différents ; garantir la vie privée des utilisateurs ; communiquer de manière transparente sur les suppressions de contenus et sur les contenus admissibles ; fournir un accès à un mécanisme de recours ; s'engager à poursuivre la collaboration. L'Engagement de Tech Against Terrorism entend servir de « point de départ à partir duquel les entreprises pourront construire leurs propres systèmes et politiques ». Il s'appuie sur les instruments de droit international existants ainsi que sur les principes de la Global Network Initiative.

Dans le but d'apporter un soutien aux plus petites entreprises, Tech Against Terrorism a lancé sa « plateforme de partage des connaissances » en 2017, permettant aux plus petites sociétés du secteur des TIC d'accéder à des outils spécifiques et à des boîtes à outils, tels qu'un modèle de conditions générales d'utilisation et des propositions de lignes directrices pour les rapports de transparence, dotant ainsi ces petites sociétés des outils dont elles ont besoin pour mieux prévenir et lutter contre l'exploitation de leurs services par les terroristes et extrémistes violents.

87 Voir https://www.techagainstterrorism.org
88 Tech Against Terrorism, *The Pledge for Smaller Tech Companies*.

Étude de cas : INHOPE – Enseignements à tirer en vue de la réglementation des contenus en ligne à caractère extrémiste violent et terroriste

L'Association internationale des centres de signalement pour contenus illégaux (INHOPE), présente dans 43 pays du monde, vise à contribuer à un Internet « libre de pédocriminalité »[89]. Elle a pour mission de « renforcer les efforts déployés au niveau international pour combattre les abus sexuels d'enfants »[90]. INHOPE agit en partenariat avec une grande diversité d'acteurs, y compris Interpol, Europol, Twitter, Crisp Thinking, Microsoft, Google, Facebook et Trend MICRO.

INHOPE est composée de 48 lignes téléphoniques spéciales proposant à la population un mécanisme pour signaler des contenus ou des activités en ligne suspectés d'illégalité. INHOPE a pour première priorité les matériels relatifs aux abus sexuels d'enfants, mais s'occupe aussi des discours de haine et des contenus xénophobes en ligne. S'il est vrai que l'Association propose une définition du discours de haine, elle reconnaît toutefois que la question des discours de haine est « extrêmement complexe » car ceux-ci ne sont pas toujours qualifiés comme illégaux en droit pénal. De ce fait, chaque signalement de discours de haine à une ligne téléphonique sera évalué à l'aune de la législation nationale du pays où le contenu concerné est hébergé[91].

Une autre leçon tirée des activités de INHOPE concerne l'importance de prendre en considération le bien-être du personnel chargé de la modération des contenus, et la reconnaissance du lourd tribut psychologique payé par les analystes responsables des contenus violents et terroristes. Un livre blanc rédigé et publié par le centre d'appel français Point de Contact vise à créer un socle commun de bonnes pratiques professionnelles en matière de traitement opérationnel des contenus choquants et potentiellement illicites qui mettent en jeu la sécurité physique et l'équilibre psychologique des professionnels[92].

89 Voir http://88.208.218.79/gns/home.aspx.
90 Voir http://88.208.218.79/gns/who-we-are/our-mission.aspx.
91 Voir http://88.208.218.79/gns/internet-concerns/overview-of-the-problem/hate-speech.aspx.
92 Point de Contact, réactualisation du Guide d'usage pour la lutte contre la pédopornographie de 2014 : *Pédopornographie et propagande terroriste en ligne - Traitement des contenus et protection des professionnels*.

Réponses fondés sur la communication :

4. Élaboration, adoption et évaluation des politiques

Ce chapitre vise à proposer aux décideurs politiques des bonnes pratiques et des études de cas sur l'élaboration, l'adoption et l'évaluation de politiques et de programmes ayant un impact dans le domaine des réponses fondées sur la communication figurant dans les stratégies pertinentes menées par les gouvernements et dans les plans d'action nationaux. Ce chapitre comporte trois sections : Conception des politiques ; Suivi et évaluation ; Risques éthiques et pour la sécurité.

Bonnes pratiques pertinentes des Recommandations de Zurich-Londres :

Bonne pratique no 1 : *Adopter et mettre en place à l'échelle nationale des cadres législatifs et politiques destinés à prévenir et à lutter contre le terrorisme et l'extrémisme violent en ligne.*

Bonne pratique no 2 : *Être en mesure d'appréhender en permanence les menaces actuelles et les risques potentiels à venir posés par l'extrémisme violent et le terrorisme en ligne, quelle que soit la configuration nationale et locale.*

Bonne pratique no 3 : *Mettre en place une stratégie claire de lutte contre l'extrémisme violent et le terrorisme en ligne, basée sur une approche à la fois sociétale et pangouvernementale et coordonnant des mesures fondées tant sur les contenus que sur la communication, ainsi que des activités hors ligne portant notamment sur l'éducation et sur la participation des organisations de la société civile, suivant les besoins.*

Bonne pratique no 4 : *Élaborer en collaboration avec d'autres parties prenantes compétentes un cadre commun de suivi et d'évaluation encourageant la transparence et permettant de mieux comprendre l'impact des mesures mises en œuvre.*

Bonne pratique no 5 : *Renforcer la coopération internationale en tant qu'élément clé de la prévention et de la lutte contre l'extrémisme violent et le terrorisme en ligne.*

Bonne pratique no 16 : *S'assurer que chaque campagne a une finalité globale, qui peut être très simple, par exemple promouvoir le dialogue et la participation ; qu'elle vise un ensemble réaliste d'objectifs mesurables ; et qu'elle est assortie d'une méthode d'évaluation robuste pour déterminer son impact sur les publics cibles.*

Bonne pratique no 17 : *Prendre conscience des risques éventuels associés à la stratégie des campagnes de communication et à leur diffusion et prendre les mesures nécessaires pour atténuer ces risques.*

INTRODUCTION

Des politiques proactives fondées sur la communication devraient faire contrepoids aux réponses fondées sur les contenus. Ces politiques devraient s'inscrire dans un cadre global de prévention et de lutte contre l'extrémisme violent et le terrorisme en ligne comme hors ligne, et traiter tous les facteurs de l'extrémisme violent pouvant conduire au terrorisme, tant internes qu'externes [93]. Conformément à la Résolution 2354 du Conseil de sécurité des Nations Unies qui précise le cadre international de lutte contre la propagande terroriste, toutes les mesures prises par les États pour lutter contre le terrorisme et l'extrémisme violent doivent respecter l'ensemble des obligations qui leur incombent en vertu du droit international, notamment le droit international des droits de l'homme, ainsi que l'état de droit, la protection de la vie privée et les libertés d'expression, d'association, de réunion pacifique et de religion ou conviction[94].

Les stratégies et politiques en matière de communication ne peuvent que bénéficier de la formulation et adoption de définitions officielles ou juridiques claires de termes clé tels que « (la lutte contre) l'extrémisme violent » et « terrorisme » dans toute législation ou stratégie ou plan d'action adoptés à l'échelon national[95]. Les définitions peuvent jouer le rôle important de façonner la perception du problème par les États, de délimiter concrètement et cibler les réponses qu'ils y apportent et d'aider à faire en sorte que toutes les parties prenantes adoptent une approche coordonnée pour relever le défi. Il est primordial que les pouvoirs publics communiquent de manière effective sur l'esprit et la lettre de leurs politiques dans le domaine de la prévention et de la lutte contre l'extrémisme violent et le terrorisme en ligne. Il convient que la communication en ligne vienne compléter et renforcer les messages et activités hors ligne en la matière, faute de quoi la crédibilité à la fois du gouvernement et de ses politiques s'en trouverait sapée.

93 *Examen de la Stratégie antiterroriste mondiale des Nations Unies* (A/RES/70/291), § 39, 19 juillet 2016.
94 Résolution 2354 (2017) du Conseil de sécurité des Nations Unies.
95 Sans préjuger d'autres définitions ou termes figurant ailleurs, y compris dans la législation nationale, une référence à retenir éventuellement pour ce qui a trait à ce que l'on entend communément par « actes terroristes » est fournie par la Résolution 1566 du Conseil de sécurité des Nations Unies (2004) en son paragraphe 3 : « [...] actes criminels, notamment ceux dirigés contre des civils dans l'intention de causer la mort ou des blessures graves ou la prise d'otages dans le but de semer la terreur parmi la population, un groupe de personnes ou chez des particuliers, d'intimider une population ou de contraindre un gouvernement ou une organisation internationale à accomplir un acte ou à s'abstenir de le faire, qui sont visés et érigés en infractions dans les conventions et protocoles internationaux relatifs au terrorisme, ne sauraient en aucune circonstance être justifiés par des motifs de nature politique, philosophique, idéologique, raciale, ethnique, religieuse ou similaire [...] ».

A : Conception des politiques

Combattre toutes les formes d'extrémisme violent et de terrorisme

Les politiques relatives aux réponses fondées sur la communication doivent combattre l'extrémisme violent et le terrorisme sous toutes leurs formes, et mettre en exergue que l'extrémisme violent et le terrorisme ne sont l'apanage d'aucune ethnicité, religion, nationalité ou croyance. Les groupes extrémistes violents et terroristes utilisent une vaste palette de tactiques différentes, des types de contenus destinés à une grande diversité de publics, y compris le grand public, des groupes de population particulièrement à risque ou vulnérables, et leurs sympathisants engagés. Les groupes extrémistes violents et terroristes conçoivent aussi de plus en plus de contenus spécifiquement adaptés à la radicalisation et au recrutement ainsi que des stratégies de mobilisation ciblant les femmes et les filles. Les réponses holistiques fondées sur la communication devraient donc en tenir compte, avec des stratégies et des politiques conçues précisément pour prévenir et contrer ces tactiques.

Pour faire face de manière exhaustive à toute la gamme de contenus à caractère extrémiste violent et terroriste disponibles en ligne, il convient de mettre en place une grande diversité de réponses fondées sur la communication. Aux fins de la présente Boîte à outils, l'on divise globalement les réponses fondées sur la communication en approches « en amont » et « en aval » (*se reporter à la figure 1, chapitre 5*) :

- **Les approches en amont** sont préventives et destinées à un large public. Elles visent à construire une résilience aux discours à caractère extrémiste violent ou terroriste, à informer l'opinion publique des politiques gouvernementales et des services d'appui proposés par les pouvoirs publics, et à démentir les fausses informations au moyen de l'éducation ou de réponses narratives positives ou alternatives.
- Au contraire, **les approches en aval** visent plus directement à démentir, réfuter ou contrer les discours des groupes extrémistes violents ou terroristes ou leurs tentatives de justifier les actes terroristes, d'inciter à en commettre ou d'en faire l'apologie. Ces approches sont conçues pour des publics très spécifiques, notamment les personnes déjà radicalisées ou se réclamant déjà de la mouvance produisant des discours à caractère extrémiste violent ou terroriste en ligne, ou qui sont considérées comme les plus à risque de radicalisation ou de recrutement, les plus vulnérables. Les approches en aval incluent des campagnes de contre-discours ciblant les publics spécifiques les plus à risque, ainsi que des interventions personnalisées en ligne auprès de participants de communautés Internet relevant de l'extrémisme violent et du terrorisme.

Approches sociétales

Les politiques fondées sur la communication devraient avoir pour but de limiter l'impact des communications à caractère extrémiste violent ou terroriste, et œuvrer à traiter les motifs internes et externes sous-jacents de l'extrémisme violent et du terrorisme. Partant, la prévention et la lutte contre l'extrémisme violent et le terrorisme par le biais de réponses fondées sur la communication ne doivent pas être vues comme une question strictement sécuritaire, mais plutôt comme un défi à multiples facettes qui pour être relevé exige des approches

multidisciplinaires, pluri-institutionnelles et sociétales. Les gouvernements devraient jouer un rôle moteur dans la promotion des approches sociétales. Par conséquent, leurs politiques et stratégies devraient encourager les acteurs compétents, y compris les sociétés du secteur des TIC et les organisations de la société civile, si besoin est, à œuvrer à la coordination et à coopérer au sein des approches fondées sur la communication.

Ces approches devraient être conçues et adoptées en cohérence avec les stratégies nationales globales et les cadres politiques plus amples de prévention et de lutte contre l'extrémisme violent et le terrorisme, afin de veiller à l'harmonisation en ligne et hors ligne des efforts engagés. Les efforts hors ligne peuvent inclure des initiatives visant à renforcer la pensée critique, la culture numérique et la résilience au moyen de la sensibilisation et de l'éducation du public, de la mobilisation des communautés de base et d'autres approches combattant les motifs internes et externes susceptibles de mener des individus à soutenir l'extrémisme violent et le terrorisme.

Les chercheurs, les milieux académiques et les praticiens peuvent apporter un éclairage concernant la communication à caractère extrémiste violent et terroriste et inspirer de possibles réponses à cette communication. Les approches réussies feront fond sur le savoir-faire recoupant une grande diversité de secteurs et de domaines interconnectés, y compris mais sans s'y limiter : la technologie, le marketing, la publicité, la production de contenus, les études de communication, la psychologie, la sociologie, les sciences politiques, l'éducation et la politique publique. Outre ces compétences professionnelles, il conviendrait également de prendre en considération les avis et les valeurs des principaux groupes cibles, et de faire intervenir, si possible, des publics spécifiques (par exemple les jeunes femmes) dans la conception et l'application des réponses.

Les États devraient déterminer si l'efficacité et l'effectivité des approches holistiques de prévention et de lutte contre l'extrémisme violent et le terrorisme en ligne sont susceptibles d'être renforcées grâce à l'établissement d'un organe national de coordination interagences chargé d'orchestrer et d'intégrer les initiatives et programmes sociétaux du gouvernement en ligne comme hors ligne, d'affiner les stratégies et les politiques et de mettre en commun les résultats des travaux de recherche ainsi que du suivi et de l'évaluation.

Étude de cas : Centre canadien d'engagement communautaire et de prévention de la violence[96]

Le Centre canadien d'engagement communautaire et de prévention de la violence, fondé en 2017, dirige les efforts du gouvernement du Canada pour lutter contre la radicalisation menant à la violence. Les activités du Centre comprennent l'orientation stratégique, la promotion de la coordination et de la collaboration avec un éventail d'acteurs, le financement, la planification et la coordination de travaux de recherche. Le Centre est axé en particulier sur la promotion des efforts communautaires, avec

96 Voir https://www.securitepublique.gc.ca/cnt/bt/cc/index-fr.aspx.

la création notamment d'un Comité national de spécialistes qui par son expérience guide et apporte un éclairage particulier aux politiques et activités. Le Fonds pour la résilience communautaire du Centre canadien offre un soutien financier aux initiatives de prévention ; il a contribué pour l'heure à vingt-quatre projets pour une valeur totale de plus de 16 millions de dollars canadiens[97].

En 2018, le Centre canadien a lancé la *Stratégie nationale de lutte contre la radicalisation menant à la violence*, qui décrit les trois priorités du gouvernement en matière de prévention et de lutte contre la radicalisation :

1. Acquérir, communiquer et mettre en application des connaissances ;
2. S'attaquer à la radicalisation menant à la violence en ligne ;
3. Soutenir les interventions.

La Stratégie fournit des définitions claires et détaillées de la radicalisation et de la radicalisation menant à la violence et à l'extrémisme violent, et reconnaît la multiplicité des facteurs contribuant à ces processus, y compris l'exposition à des discours terroristes ou extrémistes violents en ligne et hors ligne. *La Stratégie nationale* énonce clairement l'engagement du gouvernement du Canada « envers la protection des droits de la personne et des libertés fondamentales, y compris la liberté d'expression et le droit à la protection de la vie privée garantis par la Charte canadienne des droits et libertés » et envers « la diversité et l'inclusion sociale pour tous les Canadiens »[98].

La Stratégie nationale englobe les efforts de prévention et de lutte contre la radicalisation qui sont répartis en trois volets pour traiter de toutes les étapes du processus de radicalisation, de la prévention précoce à la prévention auprès de personnes à risque et au désengagement. La radicalisation en ligne, qui est l'un des trois domaines prioritaires du gouvernement, reçoit une attention particulière ; à cet égard il convient de souligner la nécessité d'encourager la communication entre le gouvernement, la société civile, les entreprises technologiques et les acteurs internationaux, et l'importance de soutenir la recherche permettant d'établir une base de données probantes sur la manière dont les groupes extrémistes violents et terroristes agissent en ligne.

Le Fonds pour la résilience communautaire, prévu pour apporter un appui aux initiatives de la société civile de promotion de la culture numérique et des discours alternatifs, a financé plusieurs programmes, y compris :

- *Canada Redirect* (Moonshot CVE) pour offrir un contenu de remplacement positif aux personnes vulnérables qui cherchent activement du contenu extrémiste

97 Voir https://www.canada.ca/fr/securite-publique-canada/nouvelles/2018/12/lancement-de-la-strategie-nationale-sur-la-lutte-contre-la-radicalisation-menant-a-la-violence-et-mise-a-jour-sur-la-menace-terroriste-pour-le-cana.html.
98 Voir https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ntnl-strtg-cntrng-rdclztn-vlnc/index-fr.aspx.

violent en ligne, en les redirigeant au moyen de publicités et de chaînes vidéo en ligne.

- *Lutter contre la haine au sein des communautés en ligne* (HabiloMédias) pour examiner le niveau de compréhension et d'expérience, par rapport aux discours de haine en ligne et à la radicalisation, des étudiants du secondaire, afin d'éclairer les réponses des écoles et des parents.
- *Portail multimédia SOMEONE (Social Media Education Every Day)* (Université Concordia) pour augmenter la résilience contre le discours de haine et la radicalisation menant à la violence chez les jeunes en mettant à la disposition des éducateurs, des médias, du gouvernement et du public une série de ressources fondées sur des données prouvées en vue d'améliorer leurs réponses à ces défis dans une grande diversité de contextes pédagogiques, du primaire au post-secondaire[99].

Étude de cas : Les lignes directrices politiques nationales pour la lutte contre l'extrémisme – Autorité nationale de lutte contre le terrorisme, Pakistan

Approche pangouvernementale et sociétale

Les lignes directrices politiques nationales pour la lutte contre l'extrémisme (sigle anglais : NCEPG) du gouvernement du Pakistan ont été élaborées au long de 34 cycles de réunions avec 305 parties prenantes, et s'appuient « sur une approche pangouvernementale et sociétale »[100]. Figuraient parmi les parties prenantes consultées : des membres des gouvernements provinciaux, des universitaires, des représentants des médias, des érudits religieux et des organisations de la société civile. Les 34 cycles de discussions s'inspiraient du cadre normatif de la Constitution de la République islamique du Pakistan afin de garantir le respect des droits de l'homme, des communautés minoritaires et marginalisées et des femmes.

La stratégie politique prend note du rôle capital dévolu aux survivants d'attentats et aux anciens extrémistes violents pour lutter contre les discours à caractère extrémiste violent et terroriste, et vise à soutenir la création d'une plateforme pour faire connaître leurs histoires. Le NCEPG reconnaît la difficulté de trouver des messagers « crédibles et convaincants » de ces récits, et se centre donc sur les messagers ayant un profil similaire à celui du public cible.

99 Voir https://www.securitepublique.gc.ca/cnt/bt/cc/fpd-fr.aspx.
100 Autorité nationale de lutte contre le terrorisme – Pakistan, National Counter Extremism Policy Guidelines, janvier 2018.

Les réponses fondées sur la communication, partie intégrante de la Stratégie nationale

Le NCEPG reconnaît l'importance de la mobilisation des médias en ligne et hors ligne, non seulement en tant que moyen de diffuser de l'information mais aussi en tant qu'outil actif du travail de lutte contre l'extrémisme fondé sur la communication. Ce travail inclut le recours aux médias pour tenter d'humaniser les récits des victimes de l'extrémisme violent et de déconstruire les discours des extrémistes violents.

Le document du NCEPG comporte également des recommandations en vue de la création, par le ministère de l'Information et de la radiodiffusion en partenariat avec l'Autorité nationale de lutte contre le terrorisme, d'une cellule chargée des médias dans la lutte contre l'extrémisme violent, pour veiller à la « synchronisation de la mise en œuvre de la stratégie de communication pour la prévention de l'extrémisme violent dans la société ». Il est prévu que cette cellule travaille en conjonction avec les Départements de l'information au niveau des provinces pour s'assurer que les populations locales sont maintenues informées des programmes de lutte contre l'extrémisme violent menés dans leur région.

Exemples de campagnes de communication soutenues par le NCEPG

PurAzm Pakistan est un exemple de programme soutenu par la stratégie politique nationale décrite dans le NCEPG. PurAzm est une campagne médiatique qui met en avant le vécu de simples citoyens pakistanais mais aussi d'officiers de police, d'agents sanitaires luttant contre la poliomyélite, de médecins des hôpitaux et d'agents de la fonction publique, en vue de diffuser le message que les Pakistanais « rejettent les méfaits de l'extrémisme violent et, malgré ses effets pernicieux, restent résilients et ne perdent pas espoir »[101].

Cette initiative a produit 30 courts métrages depuis 2014. Le programme PurAzm inclut également des prix qui sont décernés pour soutenir la durabilité du programme, en aidant les étudiants universitaires et les jeunes professionnels à créer « des contenus audiovisuels et écrits originaux, autochtones, sur les thématiques couvertes par PurAzm Pakistan ».

Le rôle des médias

Les stratégies et politiques globales fondées sur la communication peuvent également prendre en considération le rôle et l'impact potentiels des médias en vue de « renforcer le dialogue et [...] favoriser une meilleure compréhension » ainsi que « dans la promotion de la tolérance et de la coexistence et dans l'instauration d'un climat qui ne favorise pas l'incitation au terrorisme, tout comme dans la lutte contre les discours terroristes »[102]. Les gouvernements ne devraient

101 Voir http://purazm.gov.pk/about/.
102 Résolution 2354 (2017) du Conseil de sécurité des Nations Unies, préambule, §13.

pas adopter de politiques qui s'opposent à la liberté, au pluralisme ou à l'égalité des points de vue au sein des médias. Les approches lancées dans ce domaine ne devraient pas tenter de réglementer les médias et les tentatives de collaborer avec les médias doivent se faire sur une base volontaire et indépendante. Les gouvernements peuvent également jouer un rôle de soutien à la diversité des sources et de promotion de l'accès aux médias[103].

Le Conseil de l'Europe, dans sa Déclaration sur la liberté d'expression et d'information dans les médias dans le contexte de la lutte contre le terrorisme, invite les journalistes et les médias à garder à l'esprit leurs responsabilités particulières afin de ne pas contribuer par inadvertance aux objectifs poursuivis par les terroristes. Ce qui inclut de veiller à ne pas accentuer le climat de peur entretenu par le terrorisme, et de ne pas offrir de tribune aux terroristes en leur donnant une place démesurée. Le Conseil de l'Europe encourage les médias à envisager d'adopter des bonnes pratiques, lorsqu'elles n'existent pas, ou à adapter les approches existantes afin qu'elles répondent effectivement aux questions déontologiques soulevées par la couverture médiatique de l'extrémisme violent et du terrorisme[104]. Une illustration de cette approche est le Code de conduite (Règles de conduite des mass-médias en cas d'attentat terroriste et d'opération de lutte contre le terrorisme) adopté volontairement par les mass-médias en Russie en 2003[105]. Ce Code porte essentiellement sur les meilleures pratiques à mettre en œuvre par les médias durant un incident terroriste en cours pour éviter de compromettre la sécurité des opérations ou de mettre en danger de nouvelles vies, mais il souligne également l'importance des droits à la liberté d'expression et de permettre la discussion publique sur des questions telles que le terrorisme. On trouve un exemple de soutien gouvernemental à une action qui envisage le rôle éventuel des médias dans la lutte contre l'extrémisme violent et les discours à caractère terroriste dans un des programmes du Département d'État aux États-Unis relevant de l'International Visitors Leadership Program (IVLP), toujours en vigueur : « Lutte contre l'extrémisme violent – Messages et stratégies relatifs aux médias ». Ce projet spécifique s'adressait à des journalistes, des experts et des agents de la fonction publique du monde entier pour mettre en exergue les rôles et responsabilités positifs dévolus aux médias (en ligne comme dans la presse écrite) dans la promotion de la démocratie et la prévention et la lutte contre l'extrémisme violent et le terrorisme[106]. Ce projet examinait en outre le rôle des gouvernements en matière de respect de l'état de droit et de la liberté de la presse.

Compte tenu de la nature transnationale à la fois de la menace et du monde en ligne, la coopération internationale est indispensable à la prévention et à la lutte contre l'extrémisme violent et le terrorisme en ligne. La coopération internationale facilite le renforcement des capacités grâce au partage de bonnes pratiques qui contribuent à faire en sorte que les réponses nationales visant à limiter l'impact de la propagande à caractère extrémiste violent et terroriste (en ligne comme hors ligne) et à lutter contre cette propagande soient complémentaires et s'inscrivent dans la durée.

103 Article 19, 'Hate Speech' Explained A Toolkit, 2015.
104 Cf. *Déclaration sur la liberté d'expression et d'information dans les médias dans le contexte de la lutte contre le terrorisme*, adoptée par le Comité des Ministres le 2 mars 2005.
105 *Anti-Terrorism Convention (Rules Of Conduct For The Mass Media In Case Of A Terrorist Attack And An Anti-Terrorism Operation*, 11 avril 2003.
106 Chiemelie Ezeobi, *Nigeria: Countering Violent Extremism*, allAfrica, 13 juin 2018.

Les forums internationaux peuvent contribuer à mettre en place des synergies au sein de la communauté internationale en vue de porter à leur maximum les efforts collectifs et de mutualiser les savoir-faire en matière de prévention et de lutte contre l'extrémisme violent et le terrorisme en ligne. En outre, ces forums peuvent créer un climat de confiance mutuelle, contribuer à la mise sur pied de plateformes pour améliorer la communication et veiller à une utilisation efficiente et efficace des ressources. Par conséquent, les gouvernements sont encouragés à poursuivre constamment le partage des meilleures pratiques et des informations sur les programmes et politique nationaux d'évaluation, et à œuvrer à l'adoption de cadres communs de suivi et d'évaluation et d'instruments de mesure du succès des actions menées (*voir B : Suivi et évaluation des réponses fondées sur la communication*).

Étude de cas : Organisation pour la sécurité et la coopération en Europe (OSCE), Exercice national de simulation de lutte contre l'utilisation d'Internet à des fins terroristes[107]

En janvier 2019, le coordonnateur des projets de l'OSCE en Ouzbékistan et l'Unité d'action contre le terrorisme ont organisé un exercice de simulation de trois jours sur la lutte contre l'utilisation d'Internet à des fins terroristes, sur la base des Recommandations de Zurich-Londres du GCTF. Cette activité faisait suite à des travaux préalables effectués par l'OSCE, en les étendant à de nouveaux acteurs de la société civile, tout en se centrant également sur l'inclusion des droits de l'homme et des questions de genre. L'exercice de simulation visait à recourir à une approche « sociétale » en incluant 45 représentants des pouvoirs publics, des forces de l'ordre, des médias, des milieux académiques, des organisations de jeunesse et du secteur des TIC.

À l'ouverture de l'exercice, les organisateurs ont présenté une étude de cas fictive mais fondée sur les tendances observées dans le monde réel en matière de sécurité, et facilité la discussion et le dialogue entre participants, qui avaient aussi entendu des exposés par divers experts internationaux et conseillers de l'OSCE. Un thème particulier était attribué à chaque journée de l'exercice (intervention, prévention, élaboration de la politique) et un *Guide du facilitateur* avait été rédigé pour encadrer les discussions et s'assurer d'aboutir à des résultats concrets.

Des objectifs clairs :

La finalité de l'exercice était de produire un document de *Réponses politiques et recommandations exécutables (RPRE)* et un Plan d'action national d'amélioration de l'efficacité des mesures prises pour faire face aux menaces posées par l'utilisation d'Internet à des fins de terrorisme. Le RPRE fait la synthèse des sujets et problématiques abordés durant l'exercice en les structurant en thèmes cohérents et en des « réponses politiques exécutables ». Les objectifs sous-jacents étaient

107 Voir https://polis.osce.org/national-tabletop-exercise-countering-use-internet-terrorist-purposes.

d'illustrer les possibilités de coopération et de collaboration entre les différentes parties prenantes et de faire en sorte que les recommandations politiques soient conformes au droit et aux engagements internationaux, en particulier en matière de droits de l'homme.

Une approche sociétale :

L'exercice de simulation était conçu pour représenter une approche sociétale, et incluait des membres du gouvernement de l'Ouzbékistan, des représentants de la société civile et du secteur des TIC ainsi que des experts internationaux. Le succès de l'exercice dépendait de la clarté de la communication entre toutes les parties, et les activités quotidiennes de l'exercice de simulation étaient structurées de sorte à garantir la communication et la compréhension mutuelle. Les facilitateurs avaient pour instruction de poser aux participants des « questions exploratoires » et reçu un jeu de modèles de questions et de problèmes clés. Ce cadre a permis non seulement de tenir un dialogue fructueux, mais aussi de donner une place aux solutions appropriées à mesure que des problèmes étaient soulevés. Par exemple, l'exercice ne prévoyait pas, au départ, de se centrer sur des réponses fondées sur la communication, mais lorsqu'il est devenu évident que l'on était en présence d'un « manque de compréhension » flagrant au sujet de l'efficacité et de la mise en œuvre de ces approches, les organisateurs se sont saisis du problème et ont décidé d'inclure ce thème dans le déroulement de l'exercice.

Une communication soutenue et efficace était également l'une des composantes importantes de chacun des trois thèmes inclus dans le RPRE, dont les sections deux et trois mentionnaient respectivement la *collaboration* et la communication stratégique de manière explicite. Eu égard aux questions juridiques, la synthèse des débats déclare que les lois nationales et internationales ayant trait à l'utilisation d'Internet par les extrémistes violents et les terroristes « devaient être suffisamment détaillées » pour informer les citoyens, et contribuer à la mise en place de garanties « contre toute immixtion arbitraire ou illicite dans le droit à la vie privée ». De même, en faisant intervenir des représentants des médias, les organisateurs se sont assurés que le RPRE prévoie des stages à l'intention des journalistes afin que « la couverture médiatique des menaces et attentats terroristes soit efficace ».

Politique exécutable :

L'achèvement du RPRE et du Plan d'action national permet la poursuite de la collaboration entre la société civile, le gouvernement et le secteur des TIC en décrivant les buts politiques et les futurs projets réunissant des représentants de chacun de ces groupes. Le RPRE recense trois thèmes fondamentaux : les cadres juridiques pour les infractions en lien avec les utilisations d'Internet de nature extrémiste violente et terroriste ; les partenariats public-privé et la collaboration avec le secteur mondial des TIC ; la communication stratégique, les médias, l'éducation et la recherche. Pour

chacun de ces thèmes, les recommandations comportaient un calendrier d'exécution, un projet de répartition de la responsabilité de la mise en œuvre entre les différents acteurs et une liste d'indicateurs mesurables en vue d'en évaluer l'efficacité.

Transparence et prise en considération des risques :

Le fait que l'un des principes directeurs de l'exercice de simulation et des recommandations politiques qui en ont découlé eut été la reconnaissance des problèmes en matière de droits de l'homme s'est traduit par la discussion et la prise en considération des risques de la lutte contre l'utilisation d'Internet par les extrémistes violents et les terroristes. Les facilitateurs de l'exercice ont expliqué à quel point des campagnes mal orchestrées sont susceptibles, entre autres, d'accroître le risque de radicalisation ou de promouvoir par inadvertance des interprétations de la religion particulières et favorisant l'exclusion.

Compte tenu de la complexité technique d'Internet et de sa constante et rapide évolution, il serait bon de concevoir les stratégies et politiques nationales en ayant clairement à l'esprit à la fois les possibilités offertes par les réponses fondées sur la communication, et leurs vulnérabilités, dont les extrémistes violents et les terroristes pourraient titrer parti. Les gouvernements devraient par conséquent veiller à la souplesse des politiques et des stratégies qu'ils conçoivent, sur la base des résultats actualisés de la recherche, et à leur évaluation, révision périodique et actualisation permanente, en vue de suivre le rythme des changements survenant dans le cyberespace et dans les tactiques numériques des extrémistes violents et des terroristes.

Les Plans d'action nationaux ou les stratégies font l'objet de mises à jour qui peuvent être annuelles, alors que souvent les tendances en ligne évoluent sensiblement plus vite. L'analyse des tendances au sein des publics en ligne pertinents, des plateformes et des contenus populaires, ainsi que la compréhension de l'infrastructure et de l'architecture d'Internet (par exemple les « chambres d'écho » en ligne et les « bulles filtrantes » algorithmiques) sur lesquelles s'appuient les politiques fondées sur la communication, devraient aussi être soumises à des révisions régulières et à des actualisations itératives, afin que les politiques ne perdent pas leur efficacité[108].

La communication en ligne à caractère extrémiste violent et terroriste qui cherche à radicaliser des individus, à les recruter pour commettre des actes violents et à polariser les communautés, a pour caractéristique intrinsèque d'être hautement adaptative et prompte à exploiter tout changement dans l'environnement numérique et culturel. C'est pourquoi les gouvernements devraient investir dans la recherche et les outils analytiques, afin de toujours cerner les

108 Les « chambres d'écho » en ligne désignent le phénomène par lequel les personnes sont exposées à des idées et opinions à teneur conformiste au détriment d'opinions alternatives ou dissidentes. Les « bulles filtrantes » se réfèrent aux effets probables de la personnalisation des résultats des moteurs de recherche ou des flux d'actualités dans les réseaux sociaux grâce à des modèles d'apprentissage automatique et à des algorithmes, qui vont mettre en avant des contenus spécifiques en se basant sur la localisation de l'individu, sur son profil démographique et sur l'historique de son comportement en ligne, de manière à ce que les résultats générés aient une forte probabilité de correspondre aux opinions préalables de l'utilisateur.

évolutions des intentions en ligne et hors ligne et de comprendre l'impact de la communication à caractère terroriste et extrémiste violent, ainsi que des tendances plus générales observées en ligne en termes de public concerné, de plateformes et d'influenceurs.

B : Suivi et évaluation

La mesure de l'impact devrait se trouver au cœur de toutes les approches fondées sur la communication visant à remettre en cause les messages en ligne à caractère extrémiste violent ou terroriste. Il est fondamental d'intégrer dans la conception des approches fondées sur la communication et dans toute campagne spécifique, des mécanismes par le biais desquels les gouvernements pourront mesurer les effets de leur communication, que ceux-ci soient positifs ou négatifs. Cette conception du suivi et de l'évaluation permettra de mieux comprendre l'effet sur le long terme en ligne des réponses fondées sur la communication, puis d'adapter en conséquence les futures réponses à l'échelon tant national qu'international.

Investir régulièrement et durablement dans le suivi et l'évaluation, y compris, en cas de besoin, par le biais d'une collaboration avec le secteur des TIC, les universités et la société civile, permettra une affectation effective des ressources aux programmes les plus efficaces. Par ailleurs, des systèmes complets, intégrés et permanents de mesure des impacts contribueront également à une plus grande transparence et une meilleure reddition de comptes car ils aideront à identifier à la fois les résultats que l'on cherchait à obtenir par les réponses mises en œuvre et leurs effets non intentionnels.

Cadres pour le suivi et l'évaluation

Compte tenu de la complexité et de la vaste palette d'impacts potentiels des réponses fondées sur la communication, les gouvernements devraient mettre au point un cadre commun et complet pour le suivi et l'évaluation, comportant des indicateurs et des outils de mesure clairs s'appliquant à toute la variété des approches. Il est primordial de démontrer les effets des mesures prises en matière de prévention et de lutte contre l'extrémisme violent et le terrorisme en ligne pour en assurer la légitimité et l'efficacité.

En outre, il convient aussi de concevoir les cadres de suivi et d'évaluation de manière à superviser et cerner l'impact des réponses sur toute une gamme de publics en vue de veiller à ce qu'elles n'exercent pas de discrimination et qu'elles parviennent aux résultats escomptés de manière égale pour l'ensemble du public cible. Étant donné que les réponses à l'extrémisme violent et au terrorisme en ligne fondées sur la communication constituent un domaine encore émergent, les gouvernements sont encouragés à s'inspirer des cadres de suivi et d'évaluation d'autres secteurs, dont ceux de la santé publique, de la publicité commerciale et du marketing, s'il y a lieu.

Théories du changement, buts et objectifs

Les politiques gouvernementales devraient s'appuyer sur une théorie du changement bien définie qui explique comment et pourquoi une réponse fondée sur la communication quelle qu'elle soit contribuera aux buts et objectifs du Plan d'action national ou de la stratégie. La

théorie du changement doit faire partie intégrante de la conception et de la mise en œuvre de toute réponse fondée sur la communication et fournir un cadre en vertu duquel son impact pourra être évalué.

En commençant par l'impact souhaité sur le comportement ou les attitudes du public cible, la théorie du changement devrait décrire les étapes nécessaires à prévoir pour que les réponses fondées sur la communication atteignent les résultats escomptés et obtiennent l'impact souhaité, et décrire également la manière dont ces derniers seront évalués. Une théorie du changement efficace et réaliste doit s'appuyer sur des concepts clé clairement définis. Toute divergence quant à la compréhension des définitions devra être aplanie afin d'obtenir l'adhésion entière des principales parties prenantes et de mesurer l'impact avec exactitude.

Avant même les phases de conception et de diffusion d'une campagne, il convient d'en fixer la finalité générale à long terme et la série d'objectifs plus immédiats s'y rapportant. L'on se dotera ainsi d'une série de points de référence à l'aune desquels l'impact sur le public cible prévu pourra être évalué. Les objectifs devraient être clairement définis en tant que mesures quantifiables d'un effet désiré. Ils doivent être mesurables, dotés de références et d'indicateurs permettant d'en cerner le niveau de succès, et réalistes quant aux ressources disponibles et à la performance obtenue précédemment.

Les dénommés « appels à l'action », c'est-à-dire les campagnes auxquelles il est demandé au public cible de répondre au moyen d'une action, peuvent constituer une méthode efficace de mobilisation du soutien et de promotion et renforcement d'un changement de comportement ou d'attitude, tout en conférant un élément concret à partir duquel mesurer l'impact. Les appels à l'action peuvent également être un moyen de mobiliser le soutien non seulement en ligne mais aussi hors ligne, empêchant de la sorte que les campagnes de communication ne soient perçues par le public cible comme étant superficielles ou manquant de profondeur. De telles approches doivent s'inscrire dans la durée afin d'éviter que l'enthousiasme initial ne s'estompe, ce qui entraînerait un certain scepticisme parmi les participants concernant la valeur de la campagne, lequel à son tour réduirait la possibilité d'une mobilisation ultérieure.

Étude de cas : Le Global Engagement Center, Département d'État, États-Unis

Le Global Engagement Center (GEC) est à la tête des efforts consentis par le gouvernement des États-Unis en vue de mettre en échec la communication des organisations terroristes internationales et de pays étrangers. Le GEC a été établi en 2016 par le Secrétaire d'État, avec pour mandat de « mener, synchroniser et coordonner les efforts du gouvernement fédéral en vue de reconnaître, comprendre, exposer et lutter contre la propagande et la mésinformation ayant pour but de saper les intérêts des États-Unis en matière de sécurité nationale »[109]. Le GEC fait suite, en l'élargissant, à une précédente initiative interagences étatsunienne, le Centre pour la

109 Voir https://www.state.gov/about-us-global-engagement-center/.

communication stratégique de lutte contre le terrorisme (CSCT), qui relevait lui aussi du Département d'État.

Stratégie claire :

L'approche interagences permet au GEC de coordonner l'ensemble des efforts déployés en matière de communication au sein du gouvernement des États-Unis. La coordination avec les départements nationaux chargés de la sécurité contribue à tenir à jour les objectifs des activités du GEC sur la base d'analyses et du renseignement. Cette communication interagences garantit que les efforts du GEC soient alignés sur les autres activités et mesures de lutte contre le terrorisme du gouvernement.

Production de contenus :

Le GEC et ses partenaires ont mis sur pied une programmation en plusieurs langues sur de multiples plateformes, y compris les médias sociaux, la télévision par satellite, la radio, le cinéma, et la presse.

Activités de mesure et évaluation :

Le GEC a été établi dans le but de disposer d'une réponse flexible à opposer à la communication à caractère terroriste, qui conjugue l'expertise de la science des données à celle du domaine de la lutte contre le terrorisme. D'après son site web officiel, le GEC « entreprend de saper l'idéologie terroriste en partant de l'hypothèse que les personnes et les groupes les plus proches du champ de bataille des discours seront les plus efficaces pour les contrer ». Le travail du GEC englobe par conséquent quatre pans d'activités : la science et la technologie, l'interaction interagences, l'interaction avec les partenaires et la production de contenus. L'intégration de la composante science et technologie a permis l'élaboration de bonnes pratiques pour mesurer et évaluer les campagnes de communication en procédant à « l'expérimentation d'hypothèses », méthode qui applique le cadre « créer/mesurer/apprendre » aux activités afin d'en obtenir l'efficacité maximale, notamment à partir de tests A/B et d'analyses à plusieurs variables[110]. En outre, le rapport du Cadre national pour la communication stratégique de 2010 observe que toutes les communications stratégiques du gouvernement « devaient également inclure une prévision budgétaire et une allocation de ressources spécifiquement axées sur les activités de mesure nécessaires pour en évaluer la réussite »[111].

Transparence et reconnaissance des risques et des défis :

Le Cadre national pour la communication stratégique de 2010 détaille par ailleurs de manière transparente les difficultés à surmonter pour évaluer le succès en termes de changement d'attitudes des réponses fondées sur la communication : « Tout

110 *Ibidem.*
111 The White House, *National framework for strategic communication*, 2010, p. 13.

d'abord, ces efforts ciblent souvent la perception du public, qui n'est pas facilement observable et donc pas aisément mesurable … Ensuite, il est difficile d'isoler l'effet de la communication et des interactions par rapport à d'autres influences et décisions politiques. Enfin, les effets de la communication et des interactions se voient sur la durée et exigent donc d'être mesurés de manière continue »[112]. Compte tenu de ces défis, il y a lieu d'élaborer des plans comportant diverses phases et niveaux pour mesurer le succès spécifique d'un plan ou d'un programme donné.

Outils de mesure

Les gouvernements sont encouragés à concevoir, en collaboration avec le secteur des TIC, les organisations de la société civile et les institutions de recherche, des indicateurs réalistes permettant de mesurer le succès d'une politique ou d'un programme donné en matière de prévention et de lutte contre l'extrémisme violent en ligne. Ces indicateurs doivent être conformes aux dispositions relatives aux droits de l'homme, notamment le droit à la liberté d'expression, la liberté de religion ou de conviction, et l'interdiction de toute immixtion arbitraire ou illicite dans la vie privée, tels que consacrés par la Déclaration universelles des droits de l'homme et par le Pacte international relatif aux droits civils et politiques[113].

Les indicateurs ou les outils de mesure permettant d'évaluer les réponses fondées sur la communication devraient être alignés sur les objectifs et sur la théorie du changement déterminés dès la phase de conception. Il conviendrait d'utiliser, dans la mesure du possible, des données de référence et des groupes témoins en vue de déterminer si des changements (positifs ou négatifs) surviennent dans des paramètres clé, et délimiter ainsi l'impact que peut avoir la campagne sur le public cible. De manière générale, ces indicateurs relèvent des catégories suivantes : sensibilisation, mobilisation et impact. Ils peuvent être combinés et analysés afin de fournir une représentation précise et complète de la performance et de l'impact de la campagne.

Sensibilisation, mobilisation et impact

La mesure de la sensibilisation illustre la portée de la campagne, ou le nombre de personnes exposées à la campagne et leurs caractéristiques. Les éléments communément utilisés pour mesurer la sensibilisation incluent les affichages (nombre d'écrans sur lesquels apparaît le contenu) et les vues (nombre de personnes ayant consommé activement le contenu). La mesure de la sensibilisation peut également inclure des données démographiques telles que l'âge, le sexe et la localisation approximative des publics, ainsi que des informations relatives aux intérêts de ce public.

112 *Ibidem*., p. 13.

113 Comme observé dans la Résolution 2354 (2017) du Conseil de sécurité des Nations Unies, le droit à la liberté d'expression est énoncé à l'article 19 de la Déclaration universelle des droits de l'homme, adoptée par l'Assemblée générale en 1948, et à l'article 19 du Pacte international relatif aux droits civils et politiques (PIDCP) adopté par l'Assemblée générale en 1966. La résolution souligne que toute restriction dont il serait l'objet doit être édictée par la loi et être nécessaire pour les motifs exposés au paragraphe 3 de l'article 19 du PIDCP.

La mesure de la mobilisation illustre le volume et le type d'interactions entre le public et les chargés de campagne ou le contenu de la campagne. La mesure de la mobilisation porte notamment sur les interactions sur les médias sociaux telles que likes, réactions, commentaires ou partages, qui peuvent être positives comme négatives. Le nombre et la nature de ces interactions peuvent aider les chargés de campagne à comprendre dans quelle mesure la campagne a mobilisé son public ainsi que les réactions de ce public à la campagne et à son contenu.

La mesure de l'impact illustre l'évolution mesurable des connaissances, des attitudes ou du comportement du public cible susceptible d'être attribuée à l'exposition à la campagne ou à l'interaction avec son contenu. La mesure de la sensibilisation et celle de la mobilisation, lorsqu'elles sont correctement analysées, peuvent être réunies pour aider les évaluateurs à cerner l'impact de leur campagne. Des indicateurs complémentaires tels que les preuves d'une action hors ligne, les réponses à un appel à l'action ou l'évaluation qualitative des commentaires en ligne peuvent aussi contribuer à l'évaluation globale de l'impact de la campagne.

Outils de suivi et d'évaluation

Il est possible de faire le suivi de la performance des réponses en ligne fondées sur la communication en utilisant une vaste palette d'outils analytiques en ligne, y compris l'analyse en arrière-plan proposée par nombre de plateformes des médias sociaux. Ces outils peuvent fournir une série de mesures et d'informations permettant de déterminer la portée de l'impact de ces réponses sur le public auxquelles elles étaient destinées ainsi que la manière dont ces publics interagissent avec le contenu des campagnes. Ils habilitent les procédures itératives grâce auxquelles une campagne peut être optimisée et adaptée pour s'assurer qu'elle atteigne ses buts et objectifs.

Les réponses à l'extrémisme violent et au terrorisme en ligne fondées sur la communication, et en particulier celles qui sont mises en place par la société civile, en sont encore à leurs premiers pas, et rares sont les organisations de la société civile qui connaissent les meilleures pratiques du suivi et de l'évaluation en ligne. De ce fait, les gouvernements pourraient encourager l'adoption d'approches plus sophistiquées en les finançant et en apportant un appui aux méthodes innovantes de collecte de données, d'analyse et de recherche, de manière à pouvoir aller au-delà de l'analyse et des mesures de base proposées par défaut par les plateformes des médias sociaux.

Il existe une ample gamme d'outils analytiques, qui vont d'options gratuites en open-source jusqu'aux outils plus perfectionnés disponibles dans le commerce :

- Les outils de **veille sociale** peuvent apporter une assistance pour concevoir et mesurer efficacement les réponses fondées sur la communication. Ces outils permettent d'identifier des contenus publics sur les médias sociaux des principales plateformes des médias sociaux, telles que Twitter, ou sur des forums et blogs comme Reddit ou 4Chan. Ce contenu peut être trié par sujet, par période ou par langue. Les mesures fournies par ces outils peuvent aider à faire le suivi des tendances narratives, à déceler des relations entre sujets et à révéler les contenus, plateformes, influenceurs et termes utilisés en ligne par les extrémistes violents et les terroristes, ou bien ceux utilisés par les publics cibles.

- Les outils de **cartographie des réseaux** permettent de visualiser les réseaux en ligne des groupes extrémistes violents ou terroriste ainsi que la relation entretenue par ces groupes avec les différents publics. Les outils de cartographie peuvent en outre aider à comprendre les publics qui interagissent avec les réponses fondées sur la communication, et à déterminer dans quelle mesure le contenu de la compagne touche les publics cibles. L'analyse des réseaux peut également servir à mettre en lumière les influenceurs en ligne susceptibles d'accroître l'expositions des publics cibles aux campagnes.
- **L'analyse des sentiments** conjugue l'extraction de données au traitement automatique des langues naturelles (TALN) pour réunir des échantillons de textes et les analyser en recherche de signification en utilisant une procédure automatisée. On peut ainsi lancer des logiciels de traitement des langues naturelles pour classer, analyser et déterminer la signification de volumes importants de mots, d'expressions ou de phrases figurant dans l'échantillon de texte en ligne. Cette approche peut aider au traitement de données trop massives pour être analysées manuellement, et permet de générer une analyse quantitative plus approfondie des données recueillies au cours d'une campagne, et d'en déterminer l'impact.

Méthodes qualitatives

Parallèlement aux capacités proposées par les outils en ligne et les logiciels d'analyse, il existe une grande diversité d'approches qualitatives, en ligne comme hors ligne, pouvant jouer un rôle important dans le suivi et l'évaluation des réponses fondées sur la communication. Ces approches vont de l'évaluation qualitative des interactions en ligne (par exemple, les commentaires) aux sondages, groupes de discussion et entretiens réalisés hors ligne auprès de publics cibles. S'il est vrai que les approches qualitatives peuvent être plus onéreuses et chronophages que les méthodes quantitatives, elles peuvent néanmoins apporter des éclairages précieux tout au long d'une campagne. Ces approches sont communément utilisées dans d'autres domaines, de la recherche sociale ou politique à la psychologie, et il conviendrait d'appliquer les meilleures pratiques identifiées dans ces domaines, s'il y a lieu.

Il convient que les gouvernements gardent à l'esprit que de telles approches peuvent se révéler inapplicables à certaines catégories de public cible, notamment les personnes nourrissant des griefs à l'encontre de l'État ou exprimant leur appréciation des groupes extrémistes violents ou terroristes ou de leurs discours. Lorsqu'ils recourent à des approches qualitatives basées sur des entretiens en personne, les gouvernements devraient toujours agir dans la transparence, réfléchir aux personnes les mieux à même d'agir en tant que facilitateur ou médiateur et permettre aux participants, en vue de garantir des échanges ouverts et honnêtes, d'apporter leur contribution sous couvert de l'anonymat.

Défis en matière de suivi et d'évaluation

Le suivi et l'évaluation efficaces des réponses à l'extrémisme violent et au terrorisme en ligne fondées sur la communication se heurtent à un certain nombre de défis intrinsèques. Pour les réponses destinées à un public se trouvant plutôt en aval, ce sont les petites dimensions de l'échantillon qui peuvent limiter la valeur statistique des résultats. L'impossibilité d'accéder

à certains publics peut aussi se traduire par une disponibilité insuffisante des éléments de mesure nécessaires, avec pour résultat une évaluation incomplète de l'impact de certaines catégories de réponses. Il en résulte un biais en faveur des méthodes numériques d'évaluation, plus accessibles, une absence de données qualitatives et donc une évaluation finale peu nuancée.

Même lorsque des méthodes qualitatives sont employées, le phénomène de « désirabilité sociale » peut inciter les participants à fournir les résultats que, d'après eux, les évaluateurs attendent, ou qui sont considérés comme étant socialement acceptables. Si l'évaluation est conçue avec soin et que les acteurs appropriés mettent en œuvre efficacement les méthodes adéquates, l'on pourra réduire certains de ces effets potentiels. C'est pourquoi les cadres exhaustifs d'évaluation doivent être transparents quant aux limites des méthodes employées, et tout obstacle insurmontable devrait être reconnu lors du rapport final d'évaluation. Dans le but d'éviter un biais et de fournir une évaluation externe objective, il faudrait envisager, s'il y a lieu, de procéder à des évaluations indépendantes.

Risques en matière de suivi et d'évaluation

Tout comme des défis peuvent se poser pour l'évaluation des réponses fondées sur la communication, celles-ci peuvent comporter des risques en matière d'éthique, par exemple dans le cas d'un partage ou d'une publication par inadvertance de données d'utilisateurs identifiables. Il est par conséquent important de réfléchir au contexte juridique dans lequel a lieu une campagne, y compris les lois relatives à la vie privée, au traitement des données et à la protection des données. Les gouvernements doivent s'assurer de l'existence de garanties appropriées pour toute réponse de cette nature menée par le gouvernement, mais aussi veiller à ce que des processus similaires soient obligatoires lors de réponses non gouvernementales recevant un financement ou un soutien du gouvernement.

Dans l'intérêt de la transparence, les évaluations des réponses fondées sur la communication devraient être partagées avec les parties prenantes concernées, dans la mesure du possible, en vue de mettre en commun les enseignements, d'améliorer l'efficacité des réponses et de renforcer la confiance et la crédibilité. Cependant, il est nécessaire de garantir la protection de la vie privée de ceux qui sont chargés du programme et du public cible, au moyen de l'anonymisation de toute information identifiable. Il s'agit par exemple de noms d'utilisateur ou de compte, d'images de profils ou de données de géolocalisation. De même, il conviendrait de suffisamment modifier le texte publié par des publics, lors de leur extraction, pour empêcher leur identification au moyen de fonctions de recherche dans les médias sociaux ou de moteurs de recherche.

Études de cas : Cadre d'évaluation du service de la communication gouvernementale, Government Communication Service, et Guide de la planification des campagnes de communication gouvernementales[114]

Cadre national commun et intégral :

Le Cadre d'évaluation 2016 du gouvernement britannique, Government Communication Service (GCS), est un outil à la disposition des parties prenantes au sein du gouvernement britannique pour aider les chargés de communication à mesurer et démontrer l'impact des activités de communication institutionnelle du gouvernement. Ce cadre est conçu non seulement pour la communication publique relative à la prévention de l'extrémisme violent et du terrorisme, mais aussi pour les activités tournées vers toute une gamme d'objectifs de service public.

S'inspirer d'autres secteurs :

Le Cadre fait fond sur les dernières normes et pratiques du secteur, et tire des enseignements de l'expérience du secteur privé en matière d'évaluation des campagnes de communication. À ce titre, des méthodes ont été intégrées pour tenir compte de la diversité des mécanismes de communication, y compris les médias et les plateformes numériques, et prendre en considération l'importance des mesures et de l'évaluation dès le lancement d'une initiative de communication.

Outils de mesure :

Le Cadre d'évaluation GCS encourage à l'utilisation d'un « assortiment de méthodes qualitatives et quantitatives (telles que sondages, retours d'information par entretien, groupes de discussion, analyses de médias sociaux, et méthodes de traçage) » pour mesurer les résultats et l'impact d'une campagne de communication. Le guide suggère également d'utiliser des mesures d'étalonnage pour veiller à obtenir une évaluation rigoureuse du changement[115].

Mesures permanentes et optimisation :

Le Cadre GCS inclut des suggestions d'ajustement itératif pour les campagnes, sur la base de mesures permanentes et de travaux de recherche sur l'évaluation. Le Cadre suggère aux utilisateurs de « passer en revue la performance et de veiller à ce que les résultats de l'évaluation alimentent les activités en cours et soient intégrés dans la planification »[116].

114 Government Communication Service (GCS), *GCS Evaluation Framework*, janvier 2016 ; GCS, *A guide to campaign planning*.
115 GCS, GCS *Evaluation Framework*, p. 3.
116 *Ibidem.*, p. 2.

Évaluation du cycle de vie :

Le Guide de la planification de la communication publique au Royaume-Uni est un outil destiné à tous les employés de la fonction publique pour leur indiquer les différentes étapes à suivre concrètement lors de la planification et du déploiement des campagnes de communication publiques, avant même le démarrage de la production et de la diffusion des contenus. Le guide propose des étapes d'identification des objectifs et des publics cibles de la communication, des idées de contenus, des mécanismes de mise en œuvre et des procédures d'évaluation : ce sont les « étapes clé OASIS »[117]. Il fournit en outre des liens vers des outils susceptibles d'améliorer la perception des publics et la mesure de l'efficacité des campagnes de communication, par exemple vers les outils analytiques et les lignes directrices de médias sociaux.

C : Risques en matière de déontologie et de sécurité

Approches pluri-acteurs

Il arrive parfois que la communication publique ne soit pas accueillie comme prévu, ou qu'elle touche un public différent de celui pour lequel elle avait été lancée. Compte tenu de ces risques, c'est surtout de manière préventive, ou en amont, que la communication publique sera le plus efficace et à même de promouvoir la cohésion sociale et d'édifier la résilience. Dans ce type d'initiatives de communication, les conséquences potentielles des risques évoqués plus haut seront moins graves que dans la communication en aval. C'est pourquoi les gouvernements peuvent travailler aux côtés du secteur des TIC et des organisations pertinentes de la société civile, sur une base volontaire, pour apporter un soutien et donner un plus grand pouvoir d'action à des voix crédibles, veillant à ce qu'elles se fassent entendre en ligne. Les gouvernements peuvent ainsi proposer à la fois des messages alternatifs positifs aux personnes présentant des vulnérabilités face aux contenus à caractère extrémiste violent et terroriste, et des interactions en ligne avec des individus qui expriment sur Internet des opinions extrémistes violentes ou un soutien au terrorisme.

Transparence

Lorsque ce sont les pouvoirs publics qui mettent en place directement les réponses fondées sur la communication, il est important que les campagnes de ce type fassent preuve de transparence concernant leur origine ou leur financement, pour éviter d'exacerber tout ressentiment susceptible d'être exploité par les groupes extrémistes violents et terroristes. Tout type de message, en ligne ou hors ligne, doit s'aligner sur les politiques générales et la conduite du gouvernement, faute de quoi la crédibilité du gouvernement s'en trouverait amoindrie.

117 GCS, *A guide to campaign planning*, pp. 1-2.

Une approche transparente peut aider à édifier la confiance entre les citoyens et l'État, réduisant ainsi les risques évoqués plus bas. Lorsque le gouvernement apporte son appui à des organisations non gouvernementales ou de la société civile, la transparence quant au financement et au soutien est importante pour éviter de saper la crédibilité et l'impact des réponses mises en œuvre par ces organisations ; il sera important également d'encourager entre toutes les parties prenantes la mise en commun des meilleures pratiques et l'instauration d'une culture de l'apprentissage et du partage.

Conséquences non intentionnelles

Les réponses gouvernementales fondées sur la communication peuvent avoir des répercussions variées, parfois complexes et pas toujours positives. Au cours de la conception d'une réponse fondée sur la communication, il conviendra toujours de pondérer les impacts positifs potentiels avec les impacts potentiellement négatifs ou les impacts non intentionnels, pour en comprendre l'éventuelle importance et entreprendre les efforts nécessaires pour atténuer toute répercussion négative potentielle.

En conséquence, les gouvernements peuvent entreprendre de travailler avec une diversité de parties prenantes, en vue de déterminer dans quel domaine chaque acteur aura le plus d'impact, d'intégrer les activités hors ligne et en ligne et d'adopter une approche « *Do no harm* » (ne pas nuire) comportant les garanties nécessaires pour faire en sorte que les réponses fondées sur la communication soient proportionnées, ne créent pas de risques inutiles ni n'entraînent de répercussion non intentionnelle.

Ces dernières pourraient inclure :

- Une incompréhension ou une trivialisation des griefs au sein du public cible ;
- Un renforcement de l'attrait des discours à caractère extrémiste violent ou terroriste ;
- Le risque de stigmatiser certains groupes de la population comme étant « à risque », ou de renforcer l'aliénation ou l'exclusion de certains groupes qui expriment leur méfiance envers l'État ;
- La décrédibilisation ou la perte de légitimité d'une campagne qui vise à mettre en échec les discours à caractère extrémiste violent ou terroriste si celle-ci présente des liens avec des marques ou des messagers qui ne jouissent pas d'une crédibilité suffisante dans les publics cibles.

Les risques en matière de sécurité

Les réponses aux contenus à caractère extrémiste violent ou terroriste fondées sur la communication peuvent placer tant les publics que les chargés de campagne dans une position risquée, en exposant potentiellement les participants à des abus en ligne ou, dans des cas extrêmes, à un danger physique. Par le recours à une approche « Do no harm », la sécurité des personnes qui mettent en œuvre les réponses fondées sur la communication devient primordiale, et tous ceux qui participent à l'approche devraient recevoir une évaluation rigoureuse des risques auxquels ils pourraient être exposés.

Cette évaluation devrait servir de fondement à un cadre déontologique et de sécurité, lequel devrait prévoir des mesures d'atténuation des risques identifiés. Un tel cadre devrait être convenu entre toutes les parties prenantes durant la phase de conception de la campagne et faire l'objet de révisions et de mises à jour régulières, en tant que de besoin, durant la phase d'exécution de la campagne puis dans celle du suivi et de l'évaluation.

Dans de très rares cas, les gouvernements optent pour ne pas révéler leur soutien à certaines réponses fondées sur la communication en raison de préoccupations sécuritaires, notamment lorsqu'il s'agit d'une campagne « en aval » (voir la Figure 1 au chapitre 5) où la population visée par la campagne pourrait prendre pour cible ou menacer ceux qui la diffusent. Ces inquiétudes renvoient aussi à un risque déontologique, dans le sens où des parties prenantes non gouvernementales verraient s'accroître leur niveau d'exposition à des risques à cause de leur participation à la campagne.

Les risques qui se poseront spécifiquement en matière de déontologie ou de sécurité et qui devront être pris en considération varieront en fonction du type de campagne réalisée, ainsi que d'autres facteurs tels que le contexte dans lequel s'inscrit la campagne et les populations qu'elle cible. Il est possible toutefois d'atténuer ces risques si l'on procède avec soin à la planification et à l'exécution de la campagne, notamment avec un choix plus précis du public cible et plus prudent des contenus utilisés.

Risques découlant des interactions

Enfin, même si nombre de réponses fondées sur la communication ne visent pas à interagir directement avec des individus à risque ou présentant des vulnérabilités face à l'extrémisme violent ou au terrorisme, ou qui sont déjà membres de groupes extrémistes violents et terroristes, toutes les campagnes devraient se doter au préalable de lignes directrices prévoyant la possibilité que ces interactions surviennent. Il s'agirait alors de lignes directrices portant sur la phase du déroulement de la campagne comme sur celle du bilan (à travers, par exemple, des groupes de discussion ou des sondages).

Agir de manière appropriée lors des interactions avec des individus susceptibles de présenter des vulnérabilités n'est pas seulement une obligation morale, mais aussi une occasion à saisir pour renforcer l'impact positif de certains types de campagnes visant à contrer le recrutement extrémiste violent et terroriste en ligne. Certaines des considérations pertinentes pourraient être :

- Comment répondre aux personnes vulnérables de manière à réduire le risque qui les affecte à titre personnel et tenir compte avec sensibilité et efficacité de leurs besoins spécifiques ;
- Comment éviter de finir par entreprendre des activités pour lesquelles les chargés de campagne ne sont pas qualifiés ;
- Quelles sont les autorités compétentes, les options relevant de la société civile ou du soutien communautaire auxquelles renvoyer la personne vulnérable, si besoin est.

Les fonctions d'un directeur de campagne peuvent aider à identifier les réactions à une campagne de communication potentiellement négatives, dangereuses, inattendues ou contreproductives lorsqu'elles surviennent, et à y répondre. Cette figure du directeur de campagne est assez courante dans les campagnes de communication n'ayant pas trait aux contenus terroristes ou extrémistes violents, par exemple dans les campagnes publicitaires, et a démontré son utilité tant pour identifier les commentaires, réactions ou activités en rapport avec le contenu de la campagne, que pour y répondre, le cas échéant.

En outre, la plupart des principales plateformes des médias sociaux donnent à leurs annonceurs ou à leurs utilisateurs la possibilité de voir, analyser et répondre aux commentaires et réactions à un contenu publié en ligne. Il existe par ailleurs dans le commerce une véritable batterie d'outils de rationalisation de la gestion de campagnes à l'intention des équipes chargées de produire simultanément un grand nombre de campagnes de communication en ligne ou d'en analyser l'impact.

Enfin, la transparence est primordiale pour les approches prévoyant la modération des interactions. Les agences gouvernementales devraient envisager de publier leur politique relative aux médias sociaux dans chaque page ou site sur lesquels elles communiquent, décrivant les lignes directrices relatives au contenu qui pourrait être soumis à une modération par un directeur de campagne. Par exemple, des menaces ou du contenu violent.

Réponses fondées sur la communication :

5. Collaboration avec le secteur des TIC et mobilisation des organisations de la société civile

Ce chapitre vise à proposer aux décideurs politiques des pratiques et des études de cas pour inciter à des collaborations effectives entre gouvernements, secteur privé et société civile, le cas échéant, en vue de concevoir et de mettre en place une ample gamme de réponses efficaces fondées sur la communication traitant de tous les aspects de la menace posée par l'extrémisme violent et le terrorisme en ligne. Ce chapitre comporte deux sections, à savoir : Partenariats du gouvernement avec le secteur des TIC et la société civile, et Partenariats dans toute la panoplie des réponses fondées sur la communication.

Bonnes pratiques pertinentes des Recommandations de Zurich-Londres :

Bonne pratique no 6 : *Adopter une approche pluri-acteurs intégrant les gouvernements, le secteur des technologies de l'information et de la communication et les organisations de la société civile pour prévenir et lutter contre l'extrémisme violent et le terrorisme en ligne.*

Bonne pratique no 13 : *Agir sur tous les aspects de l'extrémisme violent et du terrorisme en concevant des interventions en ligne sur mesure, englobant une large palette de réponses en matière de communication, y compris des programmes préventifs et des campagnes de contre-discours.*

Bonne pratique no 14 : *Encourager les collaborations volontaires visant à générer des initiatives authentiques et innovantes fondées sur la communication pour affronter le problème des contenus extrémistes violents et terroristes en ligne, avec la participation du secteur des TIC, des organisations de la société civile et d'autres acteurs.*

Bonne pratique no 15 : *Veiller à ce que les campagnes s'adressent à un ou à plusieurs publics distincts, qu'elles poursuivent un objectif spécifique (par exemple, réduire le risque de radicalisation menant à la violence ou promouvoir des alternatives pacifiques au discours violent) et proposer des messages précisément ciblés, distincts et spécifiques à leur contexte. L'analyse du ou des publics spécifiques permet de choisir des porte-parole appropriés et crédibles aux yeux du public cible.*

INTRODUCTION

Compte tenu de la nature transnationale d'Internet, la prévention et la lutte contre l'extrémisme violent et le terrorisme en ligne gagneront en efficacité avec la mise en place d'une collaboration efficace entre les gouvernements et un éventail d'intervenants, y compris le secteur des TIC et les organisations pertinentes de la société civile. Les Recommandations de Zurich-Londres soulignent : « Il est entendu que la responsabilité principale de la lutte contre l'extrémisme violent et le terrorisme relève des États eux-mêmes. Le choix de l'approche la plus efficace est une décision relevant des prérogatives de l'État, en conformité avec ses obligations en vertu du droit international et de la législation nationale »[118].

Une approche pluri-acteurs conjuguant les savoir-faire politique, technique et contextuel de chacun et s'appuyant sur des travaux de recherche actualisés et rigoureux sur la nature des facteurs poussant des personnes à soutenir l'extrémisme violent ou le terrorisme peut jouer un rôle primordial pour l'efficacité des réponses fondées sur la communication. Ces collaborations permettent de fédérer la créativité, l'expertise et les ressources et encouragent la mise en place de campagnes innovantes et durables, dotées de stratégies claires et soutenues par une planification et des moyens de diffusion et d'évaluation efficaces.

A : Partenariats du gouvernement avec le secteur des TIC et la société civile

Approches pluri-acteurs : la société civile

Les gouvernements souhaitant mettre en place des stratégies de communication dans le but de mettre en échec les contenus à caractère extrémiste violent ou terroriste en ligne devraient reconnaître la contribution susceptible d'être apportée par la société civile et d'autres organisations civiques assumant une fonction de création, de mise en œuvre ou de direction de campagnes de communication et non plus seulement en tant que partenaires ou intervenants dans la diffusion des messages de la campagne. Les organisations de la société civile, qui par nature ont un ancrage profond au sein des communautés locales, auront plus de probabilités d'être perçues comme crédibles par les publics cibles clé et pourront dès lors être des partenaires efficaces pour mettre sur pied des initiatives de communication fructueuses et durables au niveau communautaire.

Les organisations de la société civile peuvent faire entendre des voix authentiques à une palette de publics cibles dans le cadre des réponses fondées sur la communication, apportant notamment le point de vue particulier d'un des sexes ou d'une tranche d'âge, ou celui de groupes communautaires tels que les organisations confessionnelles ou les institutions pédagogiques. Aussi les partenariats avec les organisations de la société civile peuvent-ils faire en sorte que les réponses fondées sur la communication tiennent compte de dimensions importantes dans la dynamique de recrutement extrémiste violent ou terroriste, la dimension hommes-femmes

118 GCTF, *Recommandations de Zurich-Londres sur la prévention et la lutte contre l'extrémisme violent et le terrorisme en ligne*, 2017, p. 4.

par exemple, et qu'elles s'emploient à résoudre les inquiétudes et vulnérabilités spécifiques de publics cibles pertinents.

Les approches pluri-acteurs gagnent en efficacité dès lors que tous les participants ont une vision commune de leurs responsabilités et rôles respectifs, ainsi que de leurs limitations et atouts particuliers en matière de réponse à l'extrémisme violent et au terrorisme en ligne. Compte tenu des limites qui peuvent s'appliquer à l'intervention de l'État pour faire face à ces défis (*voir chapitre 4, C : Risques en matière de déontologie et de sécurité dans les réponses fondées sur la communication*), les gouvernements peuvent encourager des groupes de la société civile très divers à contribuer à favoriser une plus grande autonomie au sein des communautés et à réfuter les discours et repousser les tactiques de radicalisation et de recrutement des groupes extrémistes violents et terroristes.

Compte tenu de la multiplicité des approches possibles pour les réponses fondées sur la communication, les gouvernements peuvent s'efforcer de mettre sur pied des partenariats avec des organisations de la société civile qui ne s'occupent pas de la prévention et de la lutte contre l'extrémisme violent. Il pourrait s'agir notamment d'organisations qui se consacrent essentiellement à la défense des droits de l'homme, au travail auprès des jeunes, à l'aide sociale et la prestation de services sociaux ou à la tenue d'activités culturelles. Ces organisations n'ont probablement pas estimé que la prévention et de la lutte contre l'extrémisme violent faisait partie de leur mandat, ou n'ont pas conscience du rôle vital qu'elles sont susceptibles de jouer dans le cadre d'une ample approche sociétale de la prévention et la lutte contre l'extrémisme violent et le terrorisme en ligne.

Dès lors, les gouvernements peuvent soutenir et renforcer les capacités des acteurs de la société civile en proposant des formations, des ressources (telles que des boîtes à outils) et/ou des financements dans le but de favoriser une plus grande participation à la prévention et la lutte contre l'extrémisme violent d'organisations bien établies, qu'elles fassent ou non partie du secteur. Il convient que ces initiatives de soutien s'inscrivent dans la durée car les efforts civiques s'améliorent inéluctablement avec le temps. Il est possible, notamment dans les cas d'organisations débutant dans la sphère de la prévention et de la lutte contre l'extrémisme violent, que les programmes prennent du temps au départ avant d'évoluer et de faire la preuve de leur succès. C'est pourquoi il serait bon que les gouvernements investissent dans le suivi et l'évaluation à la fois de leurs propres efforts de renforcement des capacités et des programmes de la société civile auxquels ils apportent leur appui.

Édifier la confiance

Si l'on veut parvenir à une collaboration efficace et durable en matière de prévention et de lutte contre l'extrémisme violent et le terrorisme en ligne, il est crucial de mettre en place un dialogue ouvert et franc entre toutes les parties prenantes. Les gouvernements devraient être conscients des sensibilités existantes et éviter de trop faire peser le volet sécuritaire dans la relation pluri-acteurs, en particulier dans les situations où la société civile s'inquiète de la stigmatisation de communautés spécifiques.

En conséquence, la participation des organisations de la société civile dans une campagne de contre-discours aux côtés du gouvernement doit être volontaire et se fonder sur la confiance, la confidentialité, et la progressivité de l'adhésion et de l'engagement. Lors de la mise sur pied de nouveaux partenariats, il faut aborder de manière ouverte et transparente les discussions sur les critiques possibles à l'égard d'organisations de la société civile qui reçoivent des pouvoirs publics un financement direct ou des commandes pour réaliser un travail de communication. Cela permettra aux organisations de la société civile de décider en connaissance de cause si elles vont collaborer avec le gouvernement pour répondre aux défis posés par l'extrémisme violent et le terrorisme en ligne.

Étude de cas : Building a Stronger Britain Together

Le programme Building a Stronger Britain Together (BSBT) vise à apporter un appui aux organisations de la société civile et communautaires au Royaume-Uni qui œuvrent à créer une capacité de résistance contre l'extrémisme et à proposer des alternatives positives au recrutement par des terroristes. Financé par le ministère de l'Intérieur et géré conjointement par UK Community Foundations et l'agence privée de communication M&C Saatchi, le programme permet aux organisations communautaires de répondre à des appels à propositions en vue de recevoir une assistance en nature ou des subventions financières allouées à leurs activités relevant des objectifs qui rentrent dans le champ d'application des buts CONTEST fixés par le gouvernement britannique pour les communautés locales[119]. Ce programme s'inscrit donc dans une stratégie nationale de prévention et de lutte contre l'extrémisme violent et le terrorisme, ce à quoi encourage le chapitre 4. En février 2019, 233 organisations communautaires avaient bénéficié d'une subvention ou d'une assistance en nature octroyées par le programme BSBT[120]. Quant aux accomplissements concrets communiqués en été 2017, ils incluaient : 20 stratégies de communication complètes, 15 constructions de sites Web, 33 modules de formation et 5 campagnes dans les médias sociaux[121].

Approche sociétale :

Le programme BSBT vise globalement à combattre « l'extrémisme sous toutes ses formes » et à apporter un appui à un large éventail d'organisations communautaires, « indépendamment de la race, la religion, l'orientation sexuelle, l'âge et l'appartenance sexuelle » de ceux qui les composent[122]. L'on trouve, parmi les organisations en partenariat avec le programme BSBT, des centres communautaires, des associations confessionnelles, culturelles et de jeunesse, et des programmes sportifs. Le programme BSBT convient par ailleurs que la tendance à utiliser Internet à des fins d'extrémisme violent et de terrorisme est constante, et encourage donc

119 Home Office, *Guidance Building a Stronger Britain Together*, 16 septembre 2016.
120 Voir https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/777653/Building_a_Stronger_Britain_Together_partners.pdf.
121 Home Office, *Partnership Support Programme Summer 2017 Update*.
122 Home Office, *Building a Stronger Britain Together*.

les candidatures d'organisations qui visent à « promouvoir des discours alternatifs positifs pour s'opposer aux contenus extrémistes en ligne et/ou remettre en cause les activités en ligne des extrémistes »[123].

La décision d'apporter un appui à une gamme si vaste d'organisations communautaires s'appuie sur le constat que les organisations locales et les acteurs de la société civile « ont une compréhension inégalée des besoins et des défis à l'échelon local, et sont les mieux placés pour octroyer les subventions aux organisations locales »[124]. Les projets s'adressent à une grande diversité de publics cibles, prévoyant par exemple un soutien communautaire à l'intention de femmes vulnérables et isolées de groupes ethniques minoritaires, et des ateliers abordant les valeurs britanniques et l'extrémisme dans un contexte local[125]. Cette approche inclusive ayant recours à des porte-parole crédibles non liés au gouvernement contribue à faire en sorte que les projets atteignent les populations à risque et marginalisées.

Le programme BSBT s'efforce également de consolider la relation entre ses organisations membres et de faciliter le partage de bonnes pratiques par la tenue de rencontres régionales dans le cadre desquelles des formations sont proposées dans des domaines tels que l'utilisation des médias sociaux et les relations publiques[126]. Le Fonds du BSBT est géré par M&C Saatchi, une agence de communication privée, ce qui garantit la présence de l'expertise du secteur commercial aux côtés des acteurs gouvernementaux et de la société civile.

Stratégie claire :

Le programme BSBT apporte son soutien à de nombreuses organisations qui œuvrent à la défense des valeurs britanniques de « démocratie, liberté d'expression, respect mutuel et égalité des chances pour tous ». Dans ce cadre, la procédure de sélection des projets par BSBT veille à ce que les candidats retenus s'alignent spécifiquement sur la stratégie gouvernementale en vigueur en matière de lutte contre l'extrémisme violent, et la respectent[127]. Les organisations souhaitant travailler avec BSBT doivent évaluer la pertinence de leur projet par rapport à quatre résultats escomptés :

1. Diminuer le nombre de personnes dont les attitudes, croyances et sentiments vont à l'encontre des valeurs communes ;
2. Augmenter le sentiment d'appartenance et la participation civique à l'échelon local ;
3. Renforcer la résilience des communautés ;
4. Combattre les activités extrémistes recensées à l'échelon local[128].

123 Voir https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759649/bsbt-inkind-guidance-applicants.pdf, p. 1.
124 https://www.efc.be/news/new-programmeme-building-stronger-britain-together-deliver-800000-grants/.
125 Home Office, *Partnership Support Programme Summer 2017 Update*.
126 *Ibidem*.
127 Home Office, *Applying for grant support Guidance for applicants*, 2019.
128 *Ibidem*, pp. 13-15.

Si elles veulent être retenues pour une subvention ou une assistance en nature, les propositions doivent prévoir des activités correspondant au quatrième résultat ci-dessus et à au moins l'un des trois autres résultats[129].

Mesure et évaluation :

Les candidatures présentées au programme BSBT doivent également s'assurer que le projet a un public cible bien défini et des résultats mesurables, notamment en se dotant de procédures de suivi des résultats et d'outils de mesure des résultats comportant des indicateurs clé de performance[130]. Les organisations doivent identifier leur finalité globale ainsi que leurs objectifs, mais aussi préciser les objectifs spécifiques du projet qu'ils souhaitent voir soutenu par BSBT en indiquant le lien entre ces objectifs et les quatre résultats escomptés du programme BSBT.

Transparence :

Les candidats retenus doivent déclarer ouvertement, sur leur site Web et dans d'autres matériels de communication pertinents, qu'ils sont bénéficiaires d'un financement du gouvernement, faute de quoi leur financement sera annulé[131]. En outre, une liste des organisations bénéficiaires est publiée tous les ans et mise à la disposition du public.

Coopération proactive et volontaire avec les sociétés du secteur des TIC

Une collaboration volontaire et transparente entre le gouvernement et les sociétés du secteur des TIC peut favoriser une meilleure compréhension de la menace posée par la communication à caractère extrémiste violent et terroriste en ligne, et améliorer l'impact des réponses fondées sur la communication. Comme pour les partenariats avec les organisations de la société civile, les partenariats du gouvernement avec les sociétés du secteur des TIC concernant les réponses fondées sur la communication doivent reposer sur la transparence et la confiance, dans le respect de la législation nationale.

Les gouvernements peuvent inciter les sociétés du secteur des TIC à être proactives dans la prévention et la lutte contre l'extrémisme violent et le terrorisme sur leurs plateformes, et à mieux protéger leurs utilisateurs en soutenant les approches innovantes de communication mises en place par la société civile. Ainsi conçue, la collaboration avec les principales sociétés du secteur des TIC peut contribuer à étendre la portée et à améliorer l'impact des initiatives afin qu'elles puissent contrer de manière effective et durable la menace posée par la communication à caractère extrémiste violent et terroriste en ligne.

On peut citer parmi les exemple de collaborations de cette nature un partenariat entre le PNUD et le programme YouTube Creators for Change qui apporte un appui à des OSC locales

129 *Ibidem*, p. 13.
130 *Ibidem*, p. 16.
131 *Ibidem*, p. 7.

en Malaisie, en Indonésie, en Thaïlande et aux Philippines au moyen de petites subventions, d'un programme de mentorat et de la constitution d'un réseau, afin d'encourager de jeunes influenceurs à créer des contenus en ligne s'opposant aux messages à caractère terroriste et extrémiste violent et proposant des discours alternatifs positifs[132]. Le PNUD a mis en place un partenariat similaire dans la région avec Facebook dans le but de faire circuler en ligne une série de vidéos présentant d'anciens extrémistes violents[133]. Au niveau national, le gouvernement australien a établi un partenariat avec un éventail de sociétés privées du secteur technologique y compris Facebook, Google, Microsoft (dont Xbox), Oath, Twitter, Instagram, Periscope et Yahoo pour accueillir DIGI Engage 2018 en conjonction avec le Sommet extraordinaire ANASE-Australie[134]. Cet événement a réuni 80 jeunes dirigeants de la région en vue de renforcer leurs compétences et de leur donner des outils pour leur permettre de mieux contribuer à la lutte contre l'extrémisme violent en ligne. Il s'agit d'une initiative menée tous les ans depuis 2017 et qui continue de susciter l'intérêt des jeunes de la région Asie-Pacifique[135].

Outre les plateformes de médias sociaux de grande envergure telles que Facebook, YouTube or Twitter, les gouvernements devraient s'efforcer d'interagir aussi avec les centaines de sociétés du secteur des TIC de dimensions plus réduites, qui peuvent également jouer un rôle clé dans l'écosystème de l'extrémisme violent ou du terrorisme en ligne. La gamme des plateformes utilisées par les groupes extrémistes violents et terroristes tend à varier en fonction de leur contexte géographique et des langues qu'ils utilisent, mais elle peut inclure des plateformes de médias sociaux, forums, services de messagerie instantanée ou plateformes de contenus audio et vidéo de taille plus modeste. Les gouvernements devraient tenir compte du fait que même lorsque les petites plateformes souhaitent contribuer aux efforts de prévention et de lutte contre l'extrémisme violent et le terrorisme en ligne, elles n'ont probablement pas autant de ressources ou de savoir-faire en interne que les plus grandes entreprises, et auront sans doute besoin de recevoir un appui supplémentaire de la part d'autres membres du secteur des TIC.

Coordination internationale

Les gouvernements ont la possibilité de passer par des forums existants, qu'ils soient gouvernementaux ou sectoriels, pour partager les meilleures pratiques et, si possible, fédérer des ressources ; la Direction exécutive du Comité contre le terrorisme (DECT) de l'ONU, le Forum mondial de l'Internet contre le terrorisme ou le Forum de l'UE sur l'internet en sont des exemples. De telles plateformes peuvent contribuer à fixer des objectifs et mettre en place des cadres communs, ouvrir des voies de communication entre les participants, renforcer les capacités, désamorcer les conflits d'intérêt et identifier les lacunes critiques. Des efforts coordonnés permettent de rationaliser les initiatives pluri-acteurs et de s'assurer de la complémentarité des actions entreprises.

132 Voir http://www.asia-pacific.undp.org/content/rbap/en/home/operations/projects/overview/creators-for-change0.html.
133 Voir http://www.asia-pacific.undp.org/content/rbap/en/home/programmes-and-initiatives/extremelives.html.
134 Voir https://digiengage2018.splashthat.com/.
135 Voir https://digiengage2019.splashthat.com/.

Étude de cas : Le Forum de l'UE sur l'internet

Coopération volontaire :

Le Forum de l'UE sur l'internet a été lancé en décembre 2015 par le commissaire chargé de la migration, des affaires intérieures et de la citoyenneté dans le but de combattre l'exploitation de l'internet par des groupes terroristes. Le Forum de l'UE sur l'internet réunit les ministres de l'intérieur de l'UE, les entreprises du secteur de l'internet et d'autres parties prenantes (telles qu'Europol, le Réseau européen pour la communication stratégique et le Réseau de sensibilisation à la radicalisation) dans un partenariat de coopération volontaire. Le Forum a pour but de combattre l'utilisation de l'internet par les terroristes et, ce faisant, de mieux protéger les citoyens de l'UE. À cet effet, le Forum de l'UE sur l'internet a deux objectifs clé : réduire la disponibilité et l'accessibilité en ligne des contenus à caractère terroriste, et renforcer les moyens d'action de ses partenaires de la société civile pour augmenter le volume et l'efficacité des récits alternatifs en ligne. En décembre 2018, le Forum de l'UE sur l'internet a donné l'occasion aux représentants des États membres de l'UE de débattre des problématiques liées à l'utilisation de l'internet par les terroristes et les extrémistes violents avec un grand nombre d'entreprises du secteur des TIC, notamment Baaz, Dropbox, Facebook, Google, Justpaste.it, Microsoft, Snap et Twitter.

Appui aux réponses de la société civile fondées sur la communication :

En décembre 2016, Le Forum de l'UE sur l'internet a lancé le Programme visant à renforcer les moyens d'action de la société civile, dans le but d'aider au lancement de campagnes de diffusion en ligne de contre-discours et de récits alternatifs[136]. Ce Programme mobilise désormais près de 12 millions d'euros pour financer des groupes de la société civile et soutenir la conception et mise en ligne de campagnes s'opposant à l'extrémisme et au terrorisme. Le Programme reconnaît que nombre d'organisations de la société civile s'emploient déjà activement à formuler des discours alternatifs, mais qu'elles manquent souvent des capacités et des ressources pour le faire de manière efficace en ligne. Le Programme met en place des partenariats avec des créatifs et des experts du marketing et de la communication afin qu'ils dispensent des formations à des boursiers de la société civile, et renforce ses partenariats déjà existants avec les grandes entreprises des médias sociaux, qui proposent aussi des formations et les meilleures pratiques du monde du marketing et de la création de contenus en ligne. Le matériel pédagogique du Programme visant à renforcer les moyens d'action de la société civile sont disponibles en ligne dans plusieurs langues[137].

136 Voir https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network/civil-society-empowerment-programme_en.
137 *Ibidem*.

Transparence :

La liste des organisations de la société civile qui reçoivent un financement et l'appui du Programme visant à renforcer les moyens d'action de la société civile figure dans une base de données en ligne, avec le titre de leur projet et le montent de la subvention octroyée[138].

L'expertise du secteur privé

Le secteur des TIC peut proposer aux gouvernements comme à la société civile son important savoir-faire, des formations et des ressources, en vue de soutenir la mise en œuvre réussie des réponses fondées sur la communication. Cela comprend les activités de conseil pour déterminer quelle est la meilleure manière d'atteindre et de mobiliser des publics spécifiques sur des plateformes TIC spécifiques (notamment par le biais de la publicité ciblée) et pour évaluer correctement l'impact de la communication en ligne. Les sociétés du secteur des TIC peuvent aussi jouer un rôle crucial en finançant et soutenant les travaux de recherche sur l'utilisation de leurs plateformes par des groupes extrémistes violents et terroristes. Les résultats de ces travaux pourront ensuite être utilisés par des partenaires de différents secteurs lors de la conception de leurs campagnes de communication afin qu'elles s'adaptent parfaitement à l'écosystème en ligne.

Lorsqu'ils travaillent avec le secteur privé pour contrer la communication à caractère extrémiste violent ou terroriste en ligne, les gouvernements devraient s'efforcer également de s'inspirer du travail d'experts de nombreux autres domaines tels que l'analyse des données, la communication en ligne, la publicité, le marketing et la production de contenus, et de coopérer avec eux. L'expertise acquise dans ces domaines peut contribuer à améliorer les réponses de prévention et de lutte contre l'extrémisme violent, leur permettant de dépasser l'approche du simple marketing de contenus pour devenir de véritables campagnes en ligne, plus sophistiquées, se rapprochant de celles du secteur commercial.

Ainsi, de nombreuses marques s'écartent d'une approche centrée sur des produits spécifiques pour entreprendre des campagnes davantage fondées sur les valeurs, et capter l'intérêt des plus jeunes publics. D'autres lancent des campagnes d'immersion, proposant de multiples versions d'un contenu ce qui permet au public de toujours trouver un message ayant une résonance particulière. Une autre formule utilisée par de nombreuses entreprises, au vu de l'écho amoindri des grandes campagnes publicitaires, passe par le recours aux « influenceurs » qui, dans le cadre de micro-campagnes ciblées, feront la promotion d'un produit à un public hautement spécifique. Ces formules ont été mises au point en s'appuyant sur des études de marché approfondies et en appliquant les systèmes d'analyse en ligne pour mieux comprendre le public qu'elles veulent cibler. Dans certains cas, les campagnes et leur contenu commencent à être développés et renouvelés en recourant à l'intelligence artificielle.

138 Voir https://ec.europa.eu/home-affairs/sites/homeaffairs/files/financing/fundings/security-and-safeguarding-liberties/internal-security-fund-police/union-actions/docs/isfp-list-proposals-selected-for-funding-during-2018_en.pdf.

Les initiatives de communication menées par les gouvernements et la société civile adoptent souvent sur le tard ces approches novatrices, et tendent à favoriser des campagnes à grande échelle pour un public de masse. Sachant que dans ces domaines le coût du savoir-faire peut être prohibitif pour les organisations de la société civile, les gouvernements pourraient apporter une contribution en incitant le secteur privé à proposer un soutien en nature ou sous forme de bénévolat dans le cadre des systèmes de responsabilité sociale des entreprises (RSE) en vue de relever les défis posés par l'extrémisme violent et le terrorisme en ligne.

B : Partenariats dans toute la panoplie des réponses fondées sur la communication

L'on observe souvent un manque de clarté conceptuelle concernant toute la panoplie des possibles réponses fondées sur la communication en vue de prévenir et de lutter contre l'extrémisme violent et le terrorisme en ligne. Dans certains cas, on parle de « contre-discours », terme fourre-tout désignant une série d'approches de communication utilisées dans la pratique pour la prévention et la lutte contre l'extrémisme violent. Il devient par conséquent essentiel d'effectuer une distinction précise et cohérente entre les différents types de réponses fondées sur la communication, pour veiller à les employer de manière adéquate, sans cibler des publics inappropriés, de sorte à éviter d'engendrer des conséquences imprévues. Aux fins de la présente Boîte à outils, l'on divise globalement les réponses fondées sur la communication entre approches « en amont » et « en aval » (*voir chapitre 4 : Combattre toutes les formes d'extrémisme violent et de terrorisme*).

Il convient toutefois d'observer qu'en dépit de cette catégorisation, les réponses fondées sur la communication relèvent de toute une panoplie et ne sont pas distinctement segmentées. De ce fait, certaines campagnes ou certains programmes peuvent incorporer des éléments provenant d'un ou de plusieurs types de réponses. En outre, les réponses fondées sur la communication sont très fortement liées au contexte dans lequel elles s'inscrivent, et ne sont donc par forcément comparables d'un environnement national ou local à un autre. Le tableau ci-dessous (*Figure 1*) met en lumière les différences entre les approches de campagnes de communication en amont et en aval, notamment pour ce qui a trait à leurs objectifs, au type de messager qu'elles requièrent et au type de public qu'elles ciblent.

Figure 1 : Approches en amont et en aval des réponses fondées sur la communication

	Approches en amont		**Approches en aval**	
Type de réponse	Sensibilisation publique	Discours positifs ou alternatifs	Contre-discours	Mobilisation et interventions en ligne
Buts	Mener des activités de prévention et renforcer la résilience		Dissuader d'interagir avec des contenus extrémistes violents ou terroristes, ou inverser les stades précoces de la radicalisation	Encourager la déradicalisation ou la démobilisation par rapport aux groupes ou idéologies à caractère extrémiste violent ou terroriste

Objectifs	• Communiquer sur la politique et la stratégie du gouvernement et sur la législation • Faire connaître les services d'appui • Réfuter toute désinformation ou fausse information • Répondre aux inquiétudes publiques, édifier la confiance publique et établir des relations avec les principaux intéressés • Construire un sentiment fort et inclusif d'identité et d'appartenance • Sensibiliser sur les droits et les responsabilités des citoyens	• Faire la promotion de valeurs positives telles que droits de l'homme, démocratie, tolérance, diversité, pluralisme • Promouvoir des canaux de participation citoyenne en faveur de la société • Mettre au défi les stéréotypes ou préjugés négatifs	• Contester, déconstruire, discréditer et démystifier directement les messages et idéologies à caractère extrémiste violents ou terroristes, par le biais de contenus comportant une charge émotive, mettant à nu l'hypocrisie, les mensonges, la désinformation ou les fausses informations	• Interagir directement avec des membres de groupes extrémistes violents ou terroristes ou avec leurs communautés en ligne
Messagers	• Pouvoirs publics • Agents de la fonction publique • Politiciens	• Société civile • Communautés • Jeunesse • « Influenceurs », par exemple des personnalités du monde des sports et du spectacle • Secteur privé • Figures ou institutions religieuses • Anciens extrémistes / terroristes et/ou survivants de la violence extrémiste ou terroriste		• Praticiens formés aux interventions et/ou anciens extrémistes / terroristes
Public cible	Larges publics, notamment l'opinion publique, les parents et les familles, les agents de la fonction publique, les praticiens, les jeunes en âge de suivre des études secondaires		Publics à risque ou vulnérables, à savoir ceux qui regardent activement ou qui recherchent des contenus extrémistes violents ou terroristes en ligne	Membres de groupes extrémistes violents ou terroristes ou de leurs communautés en ligne

Les gouvernements doivent être conscients qu'ils risquent de saper la crédibilité d'une campagne auprès de certains publics s'ils exécutent eux-mêmes des réponses fondées sur la communication en aval, s'ils y participent directement, ou s'ils leur apportent ouvertement leur caution. Il faudrait au contraire que les gouvernements contribuent au renforcement des capacités des organisations actives dans ce domaine, et encouragent d'autres acteurs (le secteur privé, ou des fondations de la société civile) à se charger de leur apporter un appui direct.

Étude de cas : UNESCO, Prévention de l'extrémisme violent par l'autonomisation des jeunes :

Le 1er février 2018, l'UNESCO a lancé un projet de deux millions de dollars d'une durée de deux ans en vue de mobiliser la jeunesse dans la prévention de l'extrémisme violent en Tunisie, au Maroc, en Lybie et en Jordanie. L'UNESCO et le Centre des Nations Unies pour la lutte contre le terrorisme ont présenté officiellement ce projet, intitulé « Prévention de l'extrémisme violent par l'autonomisation des jeunes en Jordanie, Lybie, au Maroc et en Tunisie » et qui bénéficie d'un cofinancement du gouvernement canadien, lors d'un événement tenu au siège de l'UNESCO à Paris en avril 2018. Ce projet vise non pas à diffuser directement des contre-messages s'opposant à des discours et contenus extrémistes spécifiques, mais à contribuer à l'autonomisation des jeunes afin d'accroître leur résilience face à l'extrémisme violent.

L'autonomisation des jeunes qui deviennent des messagers crédibles pour les récits alternatifs :

Ce projet de l'UNESCO est axé sur le rôle des jeunes dans la formulation de la réponse à apporter à l'extrémisme violent dans la région. L'événement de lancement a fait intervenir le témoignage de six jeunes de la région qui ont été affectés par l'extrémisme violent. Ce projet soutient des initiatives menées sur le terrain par des jeunes dans les domaines de l'éducation, des sciences, de la culture et des médias pour prévenir l'extrémisme violent. Des organisations de jeunesse, des acteurs du monde de l'éducation et des professionnels des médias seront mobilisés dans ce projet pluri-acteurs autour d'un ensemble d'activités telles que des dialogues à destination des jeunes, des formations sur la couverture médiatique des conflits ou encore des laboratoires destinés à développer la pensée critique[139].

Ce projet propose des formations sur « la lutte contre les discours de haine en ligne » et vise, entre autres éléments, la « création de nouveaux espaces médiatiques pour diffuser des récits alternatifs par et pour les jeunes ». À cette fin, il mobilise des professionnels des médias et des communautés en ligne de jeunes, au travers de stages de formation et de l'élaboration de campagnes en ligne d'envergure nationale et régionale[140]. L'objectif déclaré de l'UNESCO est de « créer des opportunités qui permettent aux jeunes femmes et hommes de s'engager en tant qu'acteurs du changement et de la consolidation de la paix dans leurs communautés et la société en général, et promouvoir une vision positive des jeunes en tant que leaders »[141]. Conformément à la Résolution 2250 du Conseil de sécurité des Nations Unies et en ligne avec le Programme onusien de développement durable à l'horizon 2030, le

139 UNESCO, *Lancement d'un projet sur la prévention de l'extrémisme violent en Jordanie, en Libye, au Maroc et en Tunisie*, 19 avril 2018.
140 UNESCO, *Un nouveau projet pour lutter contre l'extrémisme violent en Jordanie, en Libye, au Maroc et en Tunisie*, 5 février 2018.
141 Voir https://fr.unesco.org/preventing-violent-extremism/youth/project.

projet vise à édifier des compétences susceptibles d'être utilisées tant en ligne que hors ligne.

Coopération avec de multiples parties prenantes :

L'UNESCO travaillera en étroite collaboration avec des partenaires tels que les ministères de la jeunesse, de l'éducation et du travail, des sociétés du secteur des TIC, mais aussi avec des organisations de la société civile qui s'adressent aux jeunes et les incluent, des réseaux éducatifs et culturels, des chefs religieux locaux et des universités. L'UNESCO intègrera, dans l'ensemble de ces partenariats, les principes des droits de l'homme et la transparence.

Dans le cadre d'un événement tenu en novembre 2018 au Canada, l'UE et l'UNESCO ont organisé un séminaire sur les médias, le journalisme et la culture en faveur des droits de l'homme, en lien avec le projet. Les participants ont inclus des organisations de la société civile et des étudiants en journalisme, communication et médias. Les trois sessions du séminaire portaient sur : l'initiation aux médias et la maîtrise de l'information, le journalisme conscient des droits de l'homme, et le rôle des illustrateurs et caricaturistes comme vecteurs de tolérance et d'ouverture[142].

Messages, publics et messagers

Il convient que les réponses fondées sur la communication s'appuient sur des messages strictement définis, distincts et adaptés au contexte, s'attachant à créer des récits et des contenus captivants. Pour que les campagnes conçues pour renforcer la résilience face aux contenus à caractère extrémiste violent ou terroriste aient un impact, tant le message qu'elles délivrent que leurs messagers doivent être différents de ceux des campagnes destinées à démobiliser ou déradicaliser les partisans ou les sympathisants de groupes extrémistes violents ou terroristes.

Si la conception d'une campagne n'est pas suffisamment cohérente, il est probable qu'elle entraîne des conséquences imprévues, par exemple qu'elle soutienne ou qu'elle aide par inadvertance à diffuser des discours à caractère extrémiste violent ou terroriste vers des campagnes en aval[143]. Lors de la conception d'une campagne, il est primordial de ne pas oublier que les efforts visant à démystifier ou à réfuter des messages à caractère extrémiste violent ou terroriste risquent au contraire d'ancrer ces discours plus profondément encore dans l'esprit du public cible[144]. Le fait d'être exposé à une information qui porte atteinte au point de vue d'un

142 UNESCO, *Canada, EU and UNESCO host media, journalism and culture for human rights youth seminar*, 18 novembre 2018.

143 Nicholas J. Cull, *Counter Propaganda: Cases from US Public Diplomacy and beyond*, Legatum Institute Transitions Forum, juillet 2015.

144 C.R. Sunstein, On *Rumors: How Falsehoods Spread, Why We Believe Them, and What Can Be Done* (Princeton, Princeton University Press, 2014), pp. 47-53. Une autre étude a conclu récemment que durant la campagne présidentielle américaine de 2012, « (...) Twitter avait aidé les diffuseurs de rumeurs à faire circuler de fausses informations au sein des réseaux suivis par un public uniforme, mais avait rarement fonctionné comme un creuset d'idées capable de s'auto-corriger ». Cf. J. Shin, L. Jian, K. Driscoll, F. Bar, *Political rumoring on Twitter during the 2012 US presidential election: Rumor diffusion and correction*, New Media & Society, 8 mars 2016, p. 2, doi: 10.1177/1461444816634054 (2016-10-23).

individu peut en fait ancrer ce point de vue préexistant[145]. C'est pourquoi le message doit être conçu en ayant à l'esprit le public spécifique auquel il s'adresse et en s'y ajustant parfaitement, tout en ayant conscience des effets potentiels de ce message sur ceux qui ne font pas partie du public cible mais qui pourraient néanmoins être exposés à la campagne.

Les messagers doivent être authentiques et crédibles au sein du public cible afin que le message ait une résonance efficace, et d'ailleurs un membre du groupe cible pourrait même faire partie des messagers. Il est important aussi de prendre en considération la dimension homme-femmes, car les campagnes seront perçues différemment par les hommes et les femmes, ou les garçons et les filles.

Certaines campagnes parmi les plus efficaces interagissent directement avec leur public ou le font intervenir durant la phase de conception dans des groupes de discussion ou des sondages, dans le but de tester, façonner et affiner les messages, les contenus ou les plans de diffusion ; en effet, le public cible a souvent une expérience personnelle pertinente, une connaissance de l'environnement local et une bonne perception de la meilleure manière de mobiliser et d'influencer ses pairs. Il convient d'envisager à l'avance les questions déontologiques et les répercussions en termes de sécurité et de risques posés par de telles interactions, en réfléchissant notamment aux mesures d'incitation qui peuvent être proposées et à comment préserver l'anonymat des participants, ainsi qu'à la manière dont les résultats sont recueillis et enregistrés. Les mesures nécessaires devront être prises pour protéger les coordonnées personnelles et l'identité de tous les participants.

Étude de cas : Afrika Moja – Autorité intergouvernementale pour le développement (IGAD), Centre d'excellence pour la prévention et la lutte contre l'extrémisme violent

En septembre 2017, l'IGAD a réuni des jeunes de pays de la Corne de l'Afrique et d'Afrique de l'Est, dont la Somalie, Djibouti, le Kenya, la Tanzanie et l'Ouganda, dans le but de concevoir et de lancer une plateforme de la société civile pour promouvoir une série de campagnes de contre-discours et de récits alternatifs fondées sur des expériences vécues dans la région[146].

Cet atelier, d'une durée de deux jours, faisait suite à une formation organisée précédemment à l'intention de jeunes militants afin de leur faire acquérir les compétences nécessaires pour produire des campagnes avec des contenus image et vidéo innovants et efficaces. La formation utilisait une approche de pair à pair pour veiller à ce que le public cible soit inclus dans la création des contenus. L'atelier a débouché sur la création de la plateforme Afrika Moja, qui vise à contrer les messages

145 Amanda Ripley, *Complicating the Narratives – The Whole Story*, The Whole Story, 27 juin 2018. Téléchargé le 18 septembre 2018 du site https://thewholestory.solutionsjournalism.org/complicating-the-narratives-b91ea06ddf63.

146 IGAD, Centre d'excellence de l'IGAD pour la prévention et la lutte contre l'extrémisme violent (ICEPCVE), *IGAD Launches Afrika Moja, An Umbrella Platform For Civil Society Campaigns To Counter Violent Extremism*, 20 septembre 2017.

à caractère extrémiste violent dans la région en amplifiant des histoires vraies locales positives et en soulignant l'hypocrisie des groupes extrémistes violents. La première campagne produite par la plateforme, « La diversité fait la force » a aussi été créée au cours de l'atelier. Elle visait à mettre en exergue les valeurs communes à l'ensemble du continent. Après la tenue de l'atelier, la campagne a été diffusée à travers les médias sociaux (Facebook, Twitter et Instagram). Par la suite, le Centre a poursuivi son soutien aux organisations de la société civile et aux jeunes de la région qui créent des campagnes efficaces de diffusion de contre-discours, notamment au moyen de nouveaux ateliers en Ouganda, au Kenya, en Éthiopie et à Djibouti centrés respectivement sur la manière de faire entendre la voix des jeunes leaders, sur la création d'illustrations et d'infographies réfutant le discours extrémiste, sur la mise en place de partenariats efficaces pour la communication stratégique et sur l'utilisation efficace de la vidéo[147].

Une autre façon de procéder pour les campagnes est de tirer parti des « influenceurs » existants, c'est-à-dire de personnes ayant la capacité d'être entendues et réellement suivies par certains publics, tant lors de la conception que du déroulement de la campagne. Ainsi, en fonction du public, on choisira d'inclure des personnalités de la communauté locale ou de la sphère culturelle (du monde de la musique ou du sport, par exemple).

Les campagnes devraient donc être étayées par une analyse rigoureuse du public cible, par une compréhension hors ligne du public souhaité et par des tests A/B concernant les messages, pour définir des approches efficaces et créatives pour les contenus. Ces données avérées devraient être prises en compte durant les phases de planification créative, d'élaboration des contenus et de réalisation de tests, puis intégrées au sein de plans de contenus détaillés pour s'assurer de l'efficacité de la conception et du déroulement des campagnes ainsi que de la réalisation de leurs buts et objectifs.

Les supports de communication

Outre le contenu et les intervenants dans la mise en œuvre, le support de communication choisi pour les campagnes de communication sera important pour en garantir l'efficacité. Les supports incluent non seulement le type de contenus (par exemple, texte, audio, vidéo, etc.) mais aussi le canal de communication ou plateforme par le biais desquels ils seront diffusés (médias sociaux, plateformes de jeux, radio ou télédiffusion, presse, etc.)

La conception d'une campagne devrait toujours être fondée sur une connaissance approfondie des tendances pertinentes, y compris de ce qui est bien reçu par le public cible et des raisons expliquant cet accueil. Il arrive parfois que le meilleur choix ne soit pas une plateforme ou un

147 ICEPCVE, *Yali Workshop – 13th To 16th November 2018: Amplifying The Voices Of Young African Leaders*, 2 octobre 2018 ; ICEPCVE, *Using Illustrations And Infographics To Communicate Violent Extremism*, 7 juillet 2019 ; ICEPCVE, *Partnerships To Strenghten Strategic Communications*, 30 mai 2019 ; ICEPCVE, *Tell Me A Story: Video Messages To Challenge And Undermine Violent Extremist Ideologies*, 21 mai 2019.

type de contenu en ligne. Certaines démarches hors ligne et des contenus déjà existants (par exemple des programmes télévisuels ou radiodiffusés, ou des publications imprimées) peuvent en effet se révéler nettement plus influents. Cette réflexion doit être au cœur des décisions sur les plans de diffusion de chaque campagne.

Étude de cas : Duta Damai – Ambassadeurs pour la paix

Le directeur adjoint à la prévention, à la protection et à la déradicalisation de l'Agence nationale indonésienne de lutte contre le terrorisme a créé le Centre des médias pour la paix (Pusat Media Damai) afin qu'il apporte son appui aux efforts consentis au niveau national pour contrer et mettre en échec l'utilisation d'Internet par les extrémistes violents et les terroristes. Par la suite, en 2016, l'Agence a lancé son initiative des Ambassadeurs pour la paix (Duta Damai)[148].

Travailler avec les jeunes :

Duta Damai est une communauté de bloggeurs jeunesse, créateurs de sites Web et designers dont le travail s'inscrit dans la stratégie globale de l'Agence nationale de lutte contre le terrorisme, à l'appui des objectifs de lutte contre le terrorisme du gouvernement et contribuant à la promotion de la culture numérique, de la démocratie et de la paix[149].

Le programme des Ambassadeurs enseigne aux jeunes qui en font partie à créer et diffuser, en ligne et hors ligne, leurs propres contre-discours et récits positifs. Ces jeunes Ambassadeurs partagent leurs contenus entre eux et avec le public en ligne en utilisant des sources variées. Depuis sa création, le programme des Ambassadeurs pour la paix s'est étendu à 13 provinces et a inclus 780 jeunes[150].

La mise à l'échelle et la pérennisation du programme passe par la possibilité accordée aux jeunes Ambassadeurs de devenir formateurs à leur tour, aidant ainsi d'autres personnes au sein de leur communauté à acquérir des compétences similaires.

Coopération internationale :

L'initiatives des Ambassadeurs pour la paix s'est étendue à un nombre croissant de provinces chaque année, et cette année elle s'est internationalisée, accueillant des jeunes de Malaisie, Singapour, du Cambodge, de Laos, des Philippines, de Brunei Darussalam, du Myanmar et de la Thaïlande[151]. Une conférence de trois jours s'est tenue à l'appui du travail international de l'initiative, dans l'objectif de « Propager la paix dans le cyberespace ». Cette rencontre a réuni 116 jeunes âgés de 20 à 30 ans d'Indonésie et d'autres pays de l'ANASE.

148 Asmak Abdurrahman, *ASEAN Youth Ambassador for Peace 2019 Resmi dibuka*, Duta Damai NTB, 2019.
149 Voir https://dutadamainusatenggarabarat.id/tentang-kami-2/.
150 Dyah Dwi Astuti, *Duta Damai Dunia Maya direncanakan diperluas hingga antarbenua*, ANTARANEWS.com, 24 avril 2019.
151 Asmak Abdurrahman, ASEAN *Youth Ambassador for Peace 2019 Resmi dibuka*.

Le premier objectif de cette conférence était d'éduquer les participants aux dangers de la radicalisation en ligne et de leur faire comprendre la manière dont les discours à caractère extrémiste et terroriste sont diffusés sur Internet. La finalité recherchée était de doter les jeunes des moyens d'utiliser le cyberspace pour mettre au défi ces discours en leur opposant leurs propres contre-discours positifs et pacifiques. Le programme proposé aux participants portait tant sur les compétences écrites que techniques (graphisme et conception de sites Web, montage vidéo, etc.)[152].

152 *Ibidem.*

Réponses fondées sur la communication :

6. Autonomisation des jeunes et renforcement de la résilience en agissant sur la prévention et la lutte contre l'extrémisme violent, la sécurité en ligne et la citoyenneté numérique à travers l'éducation

Ce chapitre vise à proposer aux législateurs et aux acteurs sur le terrain des pratiques et des études de cas sur le rôle de l'éducation dans les réponses à l'extrémisme violent et au terrorisme en ligne fondées sur la communication. Il décrit les attributions respectives du gouvernement et d'autres parties prenantes, notamment le secteur éducatif, la société civile et le secteur privé, ainsi que la gamme des approches envisageables en vue de protéger les jeunes en ligne. Ce chapitre comporte trois sections : Conception des politiques pour les réponses éducatives ; Panoplie des réponses éducatives ; Mise en œuvre des réponses éducatives.

Bonnes pratiques pertinentes des Recommandations de Zurich-Londres :

Bonne pratique no 3 : *Mettre en place une stratégie claire de lutte contre l'extrémisme violent et le terrorisme en ligne, basée sur une approche à la fois sociétale et pangouvernementale et coordonnant des mesures fondées tant sur les contenus que sur la communication, ainsi que des activités hors ligne portant notamment sur l'éducation et sur la participation des organisations de la société civile, suivant les besoins.*

Bonne pratique no 14 : *Encourager les collaborations volontaires visant à générer des initiatives authentiques et innovantes fondées sur la communication pour affronter le problème des contenus extrémistes violents et terroristes en ligne, avec la participation du secteur des TIC, des organisations de la société civile et d'autres acteurs.*

INTRODUCTION

L'éducation est amenée à jouer un rôle crucial au sein d'une stratégie globale, fondée sur la communication, de prévention et de lutte contre l'extrémisme violent et le terrorisme en ligne. Un nombre immense de jeunes passe par les systèmes éducatifs, jeunes qui sont souvent le cœur de cible des groupes extrémistes violents et terroristes. Ces systèmes constituent également une source inépuisable de compétences, d'approches, de réseaux et d'infrastructures. L'éducation est essentielle pour inculquer les valeurs positives et transmettre les aptitudes dont les jeunes ont besoin pour réussir à l'ère du numérique, et elle peut accélérer des changements sociétaux positifs en encourageant les jeunes à se comporter en ligne en citoyens actifs et responsables. En outre, même si les adultes sont majoritairement absents du système éducatif formel, celui-ci peut néanmoins passer par des voies indirectes pour atteindre à la fois les adultes et les jeunes, notamment grâce aux interactions des écoles avec les parents d'élèves.

Ce chapitre est centré essentiellement sur l'adoption et la mise en œuvre de politiques et de programmes de prévention et de lutte contre l'extrémisme violent dans l'éducation primaire et secondaire. Il présente aussi des études de cas issus du contexte éducatif informel et inclut des approches qui ne cherchent pas explicitement à s'attaquer à l'extrémisme violent ou au terrorisme en ligne mais qui promeuvent de manière générale la sécurité en ligne et la citoyenneté numérique. Comme pour toutes les autres formes de réponses fondées sur la communication, il convient d'examiner les approches éducatives en prenant en considération le contexte pour lequel elles ont été conçues, et, en tant que de besoin, de les adapter pour cibler les facteurs spécifiques à l'échelle locale pouvant alimenter les discours de radicalisation et de recrutement extrémistes violents ou terroristes en ligne. De même, il convient de tenir compte des contextes ou systèmes éducatifs spécifiques ayant adopté ces approches à l'origine, puisque ces conditions peuvent considérablement varier d'un pays à l'autre ou même au sein d'un pays donné.

A : Conception des politiques pour les réponses éducatives

Approches sociétales de l'éducation

Comme recommandé pour les réponses fondées sur la communication de manière générale, dans les réponses éducatives les gouvernements devaient promouvoir une approche sociétale qui englobe toutes les parties prenantes compétentes, et veiller à la complémentarité des efforts avec la stratégie nationale globale de prévention et de lutte contre l'extrémisme violent et le terrorisme en ligne. Les pouvoirs publics, le secteur éducatif, la société civile, les communautés, les familles ainsi que le secteur privé devraient coopérer dans le but de déterminer en quoi l'éducation peut se transformer en outil efficace pour renforcer la résilience et diminuer l'impact du recrutement et de la radicalisation menant à l'extrémisme violent et au terrorisme. Lors de la conception de politiques et de programmes éducatifs, sachant que les jeunes femmes et les jeunes hommes peuvent avoir des besoins différents, il faudrait également réfléchir aux questions sexospécifiques. Pour formuler des réponses éducatives efficaces et

durables, les gouvernements ont un rôle important à jouer pour susciter et apporter un appui à la collaboration entre les institutions éducatives et une ample gamme d'acteurs, dès les premières rencontres et les premiers échanges relatifs à l'évaluation des besoins, puis lors de la conception, la mise en œuvre et l'évaluation des programmes.

Étant donné que le fait d'aborder des sujets sensibles dans un contexte pédagogique peut avoir des conséquences non intentionnelles, il convient également de veiller soigneusement à ne pas sur-sécuriser le secteur éducatif pour que les réponses éducatives restent efficaces. Les pouvoirs publics devraient en outre faire en sorte qu'une terminologie adéquate soit utilisée et que les initiatives éducatives de prévention et de lutte contre l'extrémisme violent et le terrorisme en ligne se déroulent dans un cadre clair et précis, ce qui facilitera l'adhésion de toutes les parties prenantes et des jeunes. Par voie de conséquence, la transparence est essentielle dans toutes les réponses et approches éducatives, au sujet de leur origine, de leur financement et de leur finalité ; ce n'est qu'ainsi que les jeunes s'y rallieront et que l'on évitera d'exacerber tout grief susceptible d'être exploité par les groupes extrémistes violents et terroristes.

Éducation primaire, secondaire et supérieure

Tous les niveaux du système éducatif ont un rôle à jouer, qu'il s'agisse d'instiller des valeurs positives, de développer les compétences et la résilience, ou en dernière instance de prévenir et de lutter contre les effets de l'extrémisme violent et du terrorisme en ligne. De nombreuses capacités cognitives relatives à la formation des valeurs et au développement de la pensée critiques sont acquises dès la prime enfance. En conséquence, il conviendrait, dans les établissements d'enseignement primaire, de se centrer davantage sur des approches implicites, notamment l'édification des valeurs positives telles que la diversité et la tolérance face aux attitudes d'autrui, tout en développant au plus vite les notions de sécurité en ligne et les capacités de pensée critique. Au niveau de l'éducation primaire il est particulièrement important de consulter et d'impliquer les parents et les membres de la famille, compte tenu du caractère sensible de certains sujets abordés dans cette approche.

Au niveau secondaire, les approches explicites seront tout aussi efficaces que les approches implicites, qu'il s'agisse de consolider les notions de sécurité en ligne et l'approche fondée sur les valeurs abordées en primaire, de cibler davantage les comportements en ligne et les approches de citoyenneté active en ligne, voire de traiter directement de sujets sensibles tels que la haine, la violence, l'extrémisme violent et le terrorisme en ligne. Enfin, l'éducation supérieure peut aller plus loin dans ces approches, donnant aux jeunes de nouvelles occasions de s'impliquer dans un militantisme actif et de se responsabiliser face aux changements positifs à mettre en œuvre dans leurs communautés en ligne.

Éducation informelle

Parallèlement au secteur éducatif formel, des espaces et approches informels peuvent contribuer à prévenir et combattre les effets de l'extrémisme violent et du terrorisme en ligne au niveau de la communauté locale. L'éducation informelle peut aider à renforcer les savoirs, compétences, attitudes et comportements que les jeunes auront acquis dans un contexte éducatif formel. Souvent, les contextes éducatifs informels peuvent se prévaloir d'approches

éducatives plus variées et plus souples, devenant alors un vecteur essentiel de soutien pour les jeunes rencontrant plus de difficultés à apprendre dans des contextes plus rigides ; en outre ils allouent plus de temps et d'espace aux activités qui ne rentrent pas strictement dans le programme scolaire.

Participation des jeunes

Les jeunes ne devraient pas être vus uniquement comme des êtres vulnérables à l'extrémisme violent et au terrorisme en ligne, mais aussi comme des parties prenantes essentielles dans la conception et la mise en œuvre des réponses fondées sur la communication. Nombre de jeunes font preuve d'un réel désir de promouvoir la justice, d'avoir un effet positif dans le monde et d'apporter une contribution à leur communauté et dans la société ; il est possible de canaliser leur énergie, créativité et enthousiasme de manière positive pour s'attaquer aux discours en ligne néfastes propagés par les groupes extrémistes violents et terroristes. Les jeunes sont souvent tout à fait conscients des circonstances et des facteurs qui poussent leurs congénères vers la radicalisation et les amène à être recrutés par ces groupes, mais ils sont aussi les mieux placés pour communiquer efficacement et exercer une influence sur leurs pairs et sur leurs cadets.

Les gouvernements et les institutions éducatives devraient par conséquent encourager les jeunes à devenir des partenaires actifs, autant que possible, dans les efforts visant à prévenir et combattre l'extrémisme violent et le terrorisme en ligne, et à assumer le rôle de mentors pour d'autres jeunes. Pour ce faire, on peut envisager de faciliter les interactions entre les jeunes et des personnalités faisant figure de modèle, ou de mettre sur pied des démarches permettant aux jeunes d'attirer l'attention de leurs parents, leur famille, leur communauté sur la sécurité en ligne, l'extrémisme violent ou le terrorisme.

Participation des parents et des adultes

Des approches éducatives holistiques devraient également prévoir des interactions avec les parents, la famille et d'autres adultes pour les sensibiliser aux dangers de l'extrémisme violent et du terrorisme en ligne et renforcer leurs défenses. Les gouvernements, les institutions éducatives, les organisations de la société civile et le secteur privé peuvent collaborer pour fournir des ressources et des possibilités de formation sur les garanties à mettre en place, sur la sécurité en ligne et sur la prévention et la lutte contre l'extrémisme violent et le terrorisme en ligne, ainsi que pour apprendre à reconnaître les signes annonciateurs d'une radicalisation en ligne.

Les écoles, qui sont des institutions de confiance bénéficiant de relations profondément ancrées dans les communautés locales, peuvent servir de lieu où de telles initiatives seront proposées. Ces initiatives peuvent par ailleurs être intégrées aux programmes existants de mobilisation des parents et des membres de la famille. Lorsque les ressources nécessaires sont mises à leur disposition et que des formations leur sont dispensées, les parents et les membres de la famille peuvent renforcer à la maison les apprentissages que les jeunes reçoivent dans des contextes éducatifs formels ou informels.

Participation du secteur privé

Les gouvernements peuvent encourager le secteur privé à mettre sur pied des programmes relevant de la responsabilité sociale des entreprises (RSE) pour apporter son appui aux réponses éducatives. Celui-ci peut prendre la forme d'un partage d'expertise, de ressources allouées et de formations dispensées à des jeunes et à d'autres parties prenantes, de soutien à la diffusion de messages clé concernant la sécurité en ligne et de promotion de la disponibilité de programmes dans ce domaine. L'appui du secteur privé pourrait passer aussi par la création de nouveaux programmes ou bien par l'adaptation d'initiatives existantes sur la sécurité en ligne en vue d'y intégrer des contenus et des concepts relatifs à la prévention et la lutte contre l'extrémisme violent. Le secteur privé peut également jouer un rôle primordial pour atteindre un public plus âgé en ligne, et pour promouvoir la pensée critique, les débats civilisés et la sécurité en ligne auprès de publics de tous âges.

B : La panoplie des réponses éducatives

Les tentatives de radicalisation et de recrutement menées par les extrémistes violents et les terroristes réussissent d'autant mieux que la pensée critique, la culture numérique et la perception des dynamiques du cyberespace font défaut. Des approches éducatives diversifiées peuvent contribuer à édifier la résilience et à réduire la vulnérabilité à l'extrémisme violent et au terrorisme en ligne, tout en enrichissant les connaissances des jeunes, en étoffant leurs compétences et en consolidant leurs attitudes et comportements. S'il est vrai que les différentes approches éducatives peuvent avoir des buts premiers très variés, et qu'elles sont toujours très liées au contexte particulier dans lequel elles s'inscrivent, elles partagent souvent nombre d'objectifs ou de résultats d'apprentissage.

Indépendamment du type d'approche utilisée, ces modalités éducatives rencontrent toujours plus de succès lorsqu'elles font appel à des pédagogies actives et expérientielles plutôt qu'aux méthodes et pédagogies plus traditionnelles. Il peut s'agir de simulations, de jeux, d'exercices de groupe et d'activités pratiques, voire même d'un assortiment de différents types de médias pour capter et retenir l'attention des jeunes.

Aux fins de la présente Boîte à outils, les démarches éducatives sont globalement réparties entre approches « explicites » et « implicites » de la prévention et la lutte contre l'extrémisme violent (sigle anglais : P/CVE) et le terrorisme en ligne :

- **Les approches explicites (spécifiques à la prévention et la lutte contre l'extrémisme violent)** abordent directement les thèmes de l'extrémisme violent et du terrorisme, et sont généralement plus adaptées aux élèves de l'enseignement secondaire (ou plus).
- **Les approches implicites (applicables à la prévention et la lutte contre l'extrémisme violent)** abordent de manière indirecte les facteurs sous-jacents susceptibles de contribuer à la résilience et de réduire la vulnérabilité des jeunes aux messages à caractère extrémiste violent ou terroriste et à d'autres menaces en ligne. Ces approches peuvent s'adapter aux jeunes de tous âges et de tous les niveaux d'éducation.

Le tableau ci-dessous (Figure 2) décrit la panoplie des réponses éducatives, en précisant le niveau d'éducation adéquat pour chacune d'entre elles, leurs buts et objectifs, et les résultats d'apprentissage prévus pour chaque type de réponse.

Figure 2 : Approches explicites et implicites des réponses éducatives

	Explicite (Spécifique à la P/CVE)	**Implicite (Applicable à la P/CVE)**	
Type de réponse	Éducation à la P/CVE	Culture numérique et éducation à la citoyenneté	Éducation à la sécurité en ligne
Niveau d'éducation	Secondaire, supérieur	Primaire, secondaire, supérieur	Primaire, secondaire
Buts	Édifier la résilience à l'extrémisme violent et au terrorisme	Encourager un usage positif d'Internet et des médias sociaux et édifier la résilience à l'extrémisme violent et au terrorisme en ligne ainsi qu'à d'autres menaces en ligne	Encourager un usage positif d'Internet et des médias sociaux
Objectifs et résultats d'apprentissage (indicatifs)	Comprendre et être conscients des dangers de l'extrémisme violent et du terrorisme en ligne Acquérir les compétences de pensée critique Maîtriser les médias et de la propagande en ligne Discerner les tactiques de manipulation et de recrutement Discerner des points de vue différents	Acquérir les compétences de pensée critique Maîtriser la culture des médias et de l'image1* Connaître l'architecture d'Internet et des communications en ligne (par ex. les chambres d'écho et les bulles filtrantes) Cerner la responsabilité collective et protéger autrui en ligne Discerner des points de vue différents Maîtriser la citoyenneté numérique et le militantisme numérique	Préserver la vie privée et la réputation en ligne (« hygiène numérique ») Gérer les informations et la sécurité en ligne Détecter la manipulation en ligne Maîtriser les relations en ligne et détecter le harcèlement en ligne Maîtriser l'image de soi et protéger son bien-être en ligne

* « L'éducation à l'image doit enseigner aux étudiants le pouvoir du visuel et leur faire comprendre que les images transmettent une émotion et non une thèse. Il faudrait donc souligner que contrairement aux mots qui peuvent prouver une thèse, une image ne saurait rien prouver. L'influence des différents caractères typographiques, polices, couleurs et styles visuels, ainsi que l'effet de la musique qui accompagne une image, devraient être débattus afin que les étudiants apprennent à les reconnaître. Il convient que les écoles enseignent aux étudiants que les différents médias se sont dotés de normes relatives à l'utilisation d'images modifiées, ce qui leur permettra de mieux juger de la véracité d'une image. » R. Hornik, *A strategy to counter propaganda in the digital era*, Yearbook of the Institute of East-Central Europe, 2016, Volume 14, Numéro 2, pp. 61–74.

Comme pour les autres catégories de réponses fondées sur la communication, les gouvernements devraient s'assurer que les approches éducatives sont conçues sur la base de données empiriques afin de garantir l'efficacité des nouveaux programmes pédagogiques ou des nouvelles initiatives de prévention et de lutte contre les impacts de l'extrémisme violent et du terrorisme en ligne. Ces données peuvent inclure des recherches de base, telles qu'évaluations des besoins, études de perception, analyses des publications sur l'éducation et des statistiques en ligne, mais aussi passer par la conception et l'évaluation de programmes pilotes.

Bounce, programme éducatif financé par la Commission européenne et coordonné par le Service Public Fédéral Intérieur de la Belgique, est un exemple de programme éducatif explicite de prévention et de lutte contre l'extrémisme violent qui dispense aux jeunes une formation en résilience[153]. Un deuxième exemple est Extreme Dialogue, initiative financée par Sécurité Publique Canada à travers le Projet Kanishka[154], puis par le programme ISEC de l'Union européenne[155]. Extreme Dialogue est une ressource didactique interactive destinée aux parents, aux enseignants et aux intervenants auprès de la jeunesse, centrée sur des courts métrages éloquents, mettant notamment en scène d'anciens extrémistes violents ainsi que des survivants d'actes à caractère extrémiste violent du Royaume-Uni, du Canada, d'Allemagne et de Hongrie[156].

Enfin, la Russie a lancé en 2016 son *Centre national d'information en vue de contrer le terrorisme et l'extrémisme dans le contexte éducatif et sur Internet*, une ressource en ligne donnant des informations sur les activités de promotion de la citoyenneté active chez les enfants et les jeunes organisées dans l'ensemble du territoire national. En outre, le programme Zero Discrimination a été lancé durant la période précédant la Coupe du monde 2018 de la FIFA, visant à améliorer les connaissances et réduire les risques que des jeunes de 14 à 21 ans entreprennent des actions à caractère extrémiste et discriminatoires, en renforçant les valeurs humanistes grâce à des exemples tirés du monde du sport et du football en particulier. Ce programme s'appuyait sur une approche interactive, il était axé sur une série de vidéos d'actualité et un ensemble d'activités participatives telles qu'exercices et discussions de groupe.

C : Mise en œuvre des réponses éducatives

Les approches éducatives à la prévention et la lutte contre l'extrémisme violent et le terrorisme en ligne étant encore relativement nouvelles, les gouvernements peuvent s'attendre à devoir relever des défis avant de réussir à les élargir et les généraliser au sein du système éducatif. Il sera impératif, pour que ces approches gagnent en ampleur et en portée, d'établir des partenariats avec les établissements scolaires et les institutions chargées de la jeunesse ainsi qu'avec la société civile et le secteur privé. Lors de l'élaboration de leur approche, les gouvernements devraient soigneusement passer en revue les compétences existantes, répertorier les besoins ainsi que les exigences des praticiens travaillant avec la jeunesse.

153 Voir https://www.bounce-resilience-tools.eu/fr.
154 Voir https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/r-nd-flght-182/knshk/index-en.aspx.
155 Voir https://ec.europa.eu/home-affairs/financing/fundings/security-and-safeguarding-liberties/prevention-of-and-fight-against-crime_en.
156 Voir https://extremedialogue.org/.

Lieux sûrs

Pour que les approches éducatives soient efficaces, il convient de faire en sorte que les écoles et autres institutions et contextes éducatifs demeurent des « lieux sûrs », où les idées peuvent être librement exprimées, discutées et débattues sans qu'un jugement ne s'y oppose, des lieux exempts de toute discrimination, de harcèlement, de menaces ou de violences émotionnelles ou physiques réelles. Les approches de ce type devraient être établies et normalisées en tant que philosophie institutionnelle, permettant d'explorer une diversité de points de vue et de faire état de tout grief librement, sachant qu'il sera traité dans un contexte d'ouverture et de sécurité.

Les institutions éducatives et travaillant avec la jeunesse devraient envisager de proposer à leurs enseignants et personnels de suivre une formation leur précisant de quelle façon entamer la discussion avec les jeunes de manière sûre et efficace sur des sujets sensibles, et comment éviter d'accroître le sentiment d'aliénation d'une personne ou sa vulnérabilité. De même, dans des contextes où les jeunes sont susceptibles d'avoir subi un traumatisme ou d'avoir été exposés à de la violence (par exemple des réfugiés ou des populations ayant vécu un conflit ou une période post-conflit), les enseignants et le personnel doivent réfléchir aux conséquences éventuelles de cette exposition et en tenir compte dans leurs méthodes pédagogiques et dans leurs approches.

S'appuyer sur les compétences et les ressources existantes

Au moment d'aborder les sujets sensibles, les formations portant sur la prévention et la lutte contre l'extrémisme violent pourraient établir des liens et faire des comparaisons avec d'autres problématiques sociales rencontrées en ligne ou avec des menaces que les enseignants et les praticiens travaillant avec la jeunesse connaissent déjà. En fonction du contexte, on pourrait par exemple faire le lien entre les problèmes de l'extrémisme violent et du terrorisme en ligne et d'autres phénomènes déjà couverts, tels que la violence et la criminalité des gangs, la drogue et l'alcool, le traumatisme, la manipulation psychologique et le harcèlement en ligne. Cette approche contribue à faire comprendre aux praticiens que s'il est vrai que la prévention et la lutte contre l'extrémisme violent et le terrorisme en ligne exigent de leur part des savoirs et des perceptions distincts, ils possèdent quand même déjà bon nombre des compétences nécessaires.

Il conviendrait également d'envisager des formations et l'octroi de ressources à l'ensemble du secteur éducatif pour s'assurer de l'adhésion généralisée de l'ensemble du système aux approches de prévention et de lutte contre l'extrémisme violent. L'on pense ici à tout une gamme de parties prenantes : les chefs d'établissement, les directeurs et l'administration scolaire, les fonctionnaires d'État ou locaux (relevant notamment des ministères de l'éducation, de la culture, de la jeunesse, des sports, de la religion), les prestataires de formation, les inspecteurs ou les régulateurs, les universitaires, les chercheurs et les organismes professionnels. Pour ces groupes, les formations peuvent proposer un aperçu plus basique de la menace en ligne, des buts et objectifs des approches spécifiques ou applicables à la prévention et la lutte contre l'extrémisme violent, mais inclure des questions de terminologie et la présentation des rôles

incombant à chacune des parties prenantes dans la réponse éducative et sociétale à apporter à l'extrémisme violent et au terrorisme en ligne.

Intégration des programmes pédagogiques

Les gouvernements (à l'échelon national, régional ou local, en fonction des systèmes éducatifs) sont les mieux placés pour modifier les programmes pédagogiques dans le but de garantir que tous les jeunes passant par l'éducation formelle bénéficient des réponses éducatives globales à l'extrémisme violent et au terrorisme en ligne. Si des domaines apparentés figurent déjà au programme, les gouvernements peuvent élargir et compléter les matières qui soulignent ou qui ont trait à l'éducation citoyenne, aux valeurs communes ou aux droits de l'homme avec des contenus relatifs à la prévention et la lutte contre l'extrémisme violent, et définir les résultats d'apprentissage correspondants. En intégrant ces contenus dans des matières existantes, la tâche des enseignants se trouvera facilitée car un sujet sensible sera rattaché à un thème qu'ils ont l'habitude d'aborder ; en outre, cela évitera de surcharger le programme pédagogique et le rythme de travail des enseignants déjà pressés par le temps.

Suivi et évaluation

Le suivi et l'évaluation sont essentiels pour démontrer les résultats et l'impact des programmes, et peuvent contribuer à l'adhésion des principales parties prenantes (*voir chapitre 4 B : Suivi et évaluation des réponses fondées sur la communication*). Là où les données empiriques sont lacunaires, il convient que les gouvernements réalisent ou commanditent de nouveaux travaux de recherche multidisciplinaires en vue d'identifier les meilleures pratiques et d'améliorer en permanence les réponses, tout en les adaptant de manière itérative au fil de l'évolution numérique et de celle de la menace. Étant donné le nombre infime de programmes déjà évalués dans ce domaine, on pourra extrapoler les meilleures pratiques d'autres domaines ou champs d'activités, y compris les théories de l'apprentissage ou la pédagogie. Les gouvernements devraient également mettre en place des mesures d'incitation appropriées pour encourager les fournisseurs de services d'éducation à évaluer et analyser de manière critique leurs programmes, et diffuser les résultats de ces évaluations à l'ensemble du secteur.

Étude de cas : Prévention et lutte contre l'extrémisme et la radicalisation – Plan d'action national (Danemark)[157]

Le Plan d'action national danois a mis en place une approche globale de la prévention et de la lutte contre l'extrémisme violent et la radicalisation qui fait intervenir conjointement les autorités nationales et locales, diverses agences, le secteur éducatif et la société civile, et se centre tout particulièrement sur les enfants et les jeunes. Les démarches de prévention visent essentiellement à promouvoir et protéger le bien-être et le développement de l'enfant par le biais d'activités favorisant la citoyenneté

157 Udlændinge- og Integrationsministeriet, *Preventing and countering extremism and radicalisation National action plan*, dernière mise à jour du 15 mars 2017.

active, renforçant les compétences démocratiques, sociales, de pensée critique et relatives à l'emploi, décourageant les « comportements à risque » et améliorant la résilience des jeunes face aux messages à caractère extrémiste.

Cette approche regroupe des parties prenantes de niveau national (ministère de l'Enfance, de l'éducation et de l'égalité hommes-femmes, et Agence nationale pour l'éducation et la qualité de l'enseignement), de niveau local (administrations municipales), des agences locales (districts de la police, services sociaux et « points d'info » qui proposent leur expertise sur l'extrémisme et la radicalisation), et le secteur éducatif (garderies, établissements scolaires du primaire et du secondaire supérieur, programmes de formation pour jeunes et pour adultes). Au niveau local, les parties prenantes sont réunies au sein des partenariats de prévention de la criminalité constitués entre la police, les services sociaux et les écoles. Le gouvernement national apporte son appui à ces efforts au travers de travaux de recherche, de partages de savoir-faire et de connaissances, d'activités de conseil et de formation, et de l'élaboration d'approches et d'initiatives spécifiques et leur évaluation indépendante dans le but de partager les meilleures pratiques.

Éducation formelle : programmes

Le Plan d'action national met l'accent sur le renforcement de la pensée critique chez les jeunes et sur leur compréhension de la citoyenneté, en particulier, au travers du programme pédagogique national des écoles primaires et du premier cycle du secondaire (Folkeskole). Ces objectifs passent par l'inclusion des droits de l'homme dans les cours d'études sociales (matière obligatoire qui couvre la santé, les relations interpersonnelles et l'éducation familiale), et par une plus grande attention aux compétences numériques et de traitement des sources dans les cours de danois et d'histoire. Ces sujets sont mis en exergue au moyen d'une « semaine thématique » annuelle, organisée par le ministère de l'Enfance, de l'éducation et de l'égalité hommes-femmes, qui met en avant dans l'ensemble du système éducatif l'importance de la démocratie, de la communauté et de la citoyenneté.

Éducation formelle : formation et ressources

Dans le but de faciliter la nouvelle importance accordée à ces matières dans le programme, tous les niveaux du secteur éducatif et toutes les parties prenantes impliquées (telles les administrations municipales) reçoivent une formation pédagogique et professionnelle et une panoplie de matériels qui leur permettent d'assurer une mise en œuvre efficace. Ainsi, des « consultants en apprentissage » sont mis à disposition par l'Agence nationale pour l'éducation et la qualité de l'enseignement. Ils organisent une série d'événements dans tout le pays au cours desquels ils présentent les meilleures pratiques dans l'enseignement de la démocratie et de la citoyenneté. Un projet pilote sur la prévention des crimes de haine a également été lancé dans une sélection d'écoles en vue de concevoir et tester des matériels supplémentaires

pour combattre le harcèlement, les clivages, les préjugés et les stéréotypes chez les jeunes. Le projet incluait une formation en pédagogie et en facilitation de dialogue autour de sujets sensibles à l'intention des enseignants et directeurs d'école.

L'Agence nationale pour l'éducation et la qualité de l'enseignement conçoit des matériels qu'elle diffuse sur le portail national de l'apprentissage (www.emu.dk) à l'intention des enseignants, directeurs d'école et autres praticiens du secteur ; il s'agit de ressources concrètes qui visent à intégrer les approches de prévention de la marginalisation et de la radicalisation et à renforcer la résilience face aux messages à caractère extrémiste et terroriste en ligne. Ces ressources portent notamment sur la pensée critique et sur la propagande et la manipulation et incluent des programmes sur la sécurité en ligne et la culture numérique pour les établissements du primaire et du secondaire et pour les clubs d'activités extrascolaires. Enfin, des approches et des ressources sont aussi disponibles pour que les écoles favorisent l'implication des parents d'élèves.

Éducation informelle, jeunes et société civile

Le Plan d'action national inclut également une série d'approches destinées aux contextes éducatifs informels, aux organisations de la société civile tournées vers les jeunes et aux organisations confessionnelles, et prévoit des activités ciblant les jeunes. Des formations et des ressources sont également fournies aux services municipaux pour leur permettre d'acquérir les compétences nécessaires à une collaboration effective avec la société civile locale et les organisations de la jeunesse, et au codéveloppement d'occasions constructives de mobiliser les jeunes.

L'Agence danoise pour le recrutement international et l'intégration a lancé une initiative nationale de dialogue entre pairs à l'intention des jeunes (de 18 à 35 ans) dans le but de favoriser la tenue de débats sur des thèmes importants, d'encourager l'indépendance et de créer un sentiment d'appropriation au sein des communautés et d'appartenance à la société. Cette initiative couvre une ample gamme de sujets, dont : « identité, relations familiales, opportunités de s'exprimer, contrôle social, conflits liés à l'honneur, participation sociale, liberté et responsabilité, droits et obligations, groupes antisociaux et prosociaux, discrimination et non-discrimination, images d'amis et d'ennemis, intolérance, extrémisme ». En outre, un partenariat réunit le gouvernement national et diverses institutions éducatives avec pour objectif de mobiliser les jeunes, grâce à une formation en communication numérique, dans la lutte contre la radicalisation en ligne par le biais de récits positifs ou de discours alternatifs.

L'Agence danoise pour le recrutement international et l'intégration propose aussi, outre ces initiatives, des formations à l'intention de la société civile locale, des organisations de la jeunesse et des professionnels du secteur en vue de renforcer leurs compétences pour qu'ils soient mieux à même de dispenser des programmes

de prévention et de lutte contre l'extrémisme et la radicalisation, d'encourager la participation positive au sein des communautés et dans les activités locales, et de s'adresser à des groupes vulnérables ou à risque. En guise de complément à ces formations, du matériel pédagogique destiné spécifiquement aux contextes éducatifs informels, portant sur la pensée critique et la culture numérique, a été mis au point en coopération avec le Conseil des médias pour l'enfance et la jeunesse.

Bibliographie complémentaire

Chapitre 1 : Élaboration et adoption d'une législation et de politiques relatives aux contenus

Gouvernement australien, Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act, avril 2019.

Gouvernement britannique, Online Harms White Paper, avril 2019.

Gouvernement français, Creating a French framework to make social media platforms more accountable: Acting in France with a European vision, mai 2019.

Chapitre 2 : Conception de mécanismes de transparence et de reddition de comptes

Comité d'experts sur les intermédiaires internet, Study on the human rights dimensions of automated data processing techniques and possible regulatory implications, Conseil de l'Europe, 2017.

Conway, Maura, Moign Khawaja, Suraj Lakhani, Jeremy Reffin, Andrew Robertson & David Weir, Disrupting Daesh: Measuring Takedown of Online Terrorist Material and Its Impacts, Studies in Conflict & Terrorism, octobre 2018.

Jourová, Věra, Code of Conduct on countering illegal hate speech online: Fourth evaluation confirms self-regulation works, Commission européenne, février 2019.

Pearson, Elizabeth, Online as the New Frontline: Affect, Gender, and ISIS-Take-Down on Social Media, Studies in Conflict and Terrorism, juillet 2017.

Chapitre 3 : La collaboration pluri-acteurs à l'appui des réponses fondées sur les contenus

Huang, Medea and Faris Natour, Legitimate and Meaningful: Stakeholder Engagement in Human Rights Due Diligence: Challenges and Solutions for ICT Companies, Business for Social Responsibility, septembre 2014.

Keen, Florence, Public–Private Collaboration to Counter the Use of the Internet for Terrorist Purposes: What Can be Learnt from Efforts on Terrorist Financing?' Royal United Services Institute for Defense and Security Studies, février 2019.

UNCTED, More Support Needed For Smaller Technology Platforms To Counter Terrorist Content, novembre 2018.

Tech Against Terrorism: Analysis, ISIS use of smaller platforms and the DWeb to share terrorist content, 2019.

Chapitre 4 : Élaboration, adoption et évaluation des politiques

Bhulai, Rafia, Allison Peters & Christian Nemr, From Policy to Action: Advancing an Integrated Approach to Women and Countering Violent Extremism, Global Center on Cooperative Security and Inclusive Security, juin 2016.

Cox, Kate, William Marcellino, Jacopo Bellasio, Antonia Ward, Katerina Galai, Sofia Meranto & Giacomo Persi Paoli, Social media in Africa A double-edged sword for security and development, UNDP & RAND Europe.

Direction générale des politiques internes, Département thématique C : Droits des citoyens et affaires constitutionnelles, Les politiques de l'Union européenne en matière de lutte contre le terrorisme - Pertinence, cohérence et efficacité , janvier 2017.

Feve, Sebastian & Mohammed Elshimi, Planning for Prevention: A Framework to Develop and Evaluate National Action Plans to Prevent and Counter Violent Extremism, Global Center on Cooperative Security, juin 2018.

G7, G7 Action Plan on Counter Terrorism and Violent Extremism, octobre 2016.

GCTF, Mémorandum d'Ankara sur les bonnes pratiques pour une démarche multisectorielle à l'égard de la lutte contre l'extrémisme violent, 2013.

GCTF, Bonnes pratiques relatives aux femmes et à la lutte contre l'extrémisme violent, 2014.

Hedayah, Guidelines and Good Practices for Developing National CVE Strategies.

Hedayah, Guidelines and Good Practices: Developing National P/CVE Strategies and Action Plans, septembre 2016.

Hedayah, The World of Communications Is the New Frontline in The Battle Against Violent Extremism.

Herrington, Rebecca, Emerging Practices in Design, Monitoring, and Evaluation for Education for Peacebuilding Programming, Search for Common Ground, octobre 2015.

Tuck, Henry & Louis Reynolds, The Counter-Narrative Monitoring & Evaluation Handbook, 2017.

IMPACT Europe, Innovative Methods and Procedures to Assess Counter-violent-radicalisation Techniques in Europe: Toolkit Manual.

Khalil, James & Martine Zeuthen, Countering Violent Extremism and Risk Reduction: A Guide to Programme Design and Evaluation, Royal United Services Institute, juin 2016.

RAN Centre of Excellence, Developing a local prevent framework and guiding principles - Part 2, novembre 2018.

RAN Centre of Excellence, Monitoring & Evaluating counter- and alternative narrative campaigns, février 2019.

Russell, Olivia, Meet Me At The Maskani: A Mapping of Influencers, Networks, and Communications Channels in Kenya and Tanzania, Search For Common Ground, juin 2017.

UNDP & International Alert, Improving the impact of preventing violent extremism programming: a toolkit for design, monitoring and evaluation, 2018.

Assemblée générale des Nations Unies, Plan d'action pour la prévention de l'extrémisme violent - Rapport du Secrétaire général, décembre 2015.

Bureau de lutte contre le terrorisme des Nations Unies, Developing National and Regional Action Plans to Prevent Violent Extremism.

Conseil de sécurité des Nations Unies, Lettre datée du 26 avril 2017, adressée à la Présidente du Conseil de sécurité par le Président du Comité du Conseil de sécurité créé par la résolution 1373 (2001) concernant la lutte antiterroriste, avril 2017.

Conseil de sécurité des Nations Unies, Résolution 2354, mai 2017.

Chapitre 5 : Collaboration avec le secteur des TIC et mobilisation des organisations de la société civile

Bhulai, Rafia, Going Local: Supporting Community-Based Initiatives to Prevent and Counter Violent Extremism in South and Central Asia, décembre 2017.

Committee on Legal Affairs and Human Rights Council of Europe Parliamentary Assembly, Counter-Narratives to Terrorism, mars 2018.

Department of Homeland Security, Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States, octobre 2016.

Elsayed Lilah, Talal Faris & Sara Zeiger, *Undermining Violent Extremist Narratives in the Middle East and North Africa: a how-to guide*, Hedayah, décembre 2017.

GCERF, A Youth Perspective on Preventing Violent Extremism.

GCTF, Mémorandum d'Ankara sur les bonnes pratiques pour une démarche multisectorielle à l'égard de la lutte contre l'extrémisme violent, 2013.

Hemmingsen, Ann-Sophie & Karin Ingrid Castro, The Trouble with Counter-Narratives, Danish Institute for International Studies, 2017.

Zeiger, Sara, Undermining Violent Extremist Narratives in East Africa: A How-To Guide, Hedayah, août 2018.

ICCT & Hedayah, Developing Effective Counter-Narrative Frameworks for Countering Violent Extremism, septembre 2014.

OSCE, The Role of Civil Society in Preventing and Countering Violent Extremism and Radicalisation that Lead to Terrorism: A Focus on South-Eastern Europe, août 2018.

RAN Centre of Excellence, A Nimble (NMBL) Approach to Youth Engagement in P/CVE.

RAN Centre of Excellence, *Developing counter- and alternative narratives together with local communities*, octobre 2018.

RAN Centre of Excellence, Directives à l'intention des jeunes activistes : comment mettre sur pied une initiative de prévention et de lutte contre l'extrémisme violent - Première partie, mars 2019.

RAN Centre of Excellence, Directives à l'intention des jeunes activistes : comment mettre sur pied une initiative de prévention et de lutte contre l'extrémisme violent - Deuxième partie : Comment développer un plan pour votre initiative de prévention et de lutte contre l'extrémisme violent, mars 2019.

Reed, Alastair, Haroro J. Ingram & Joe Whittaker, Countering Terrorist Narratives, Parlement européen, Département thématique Droits des citoyens et affaires constitutionnelles, novembre 2017.

Zeiger, Sara, Counter-Narratives For Countering Violent Extremism (CVE) In South East Asia, Hedayah, mai 2016.

Chapitre 6 : Autonomisation des jeunes et renforcement de la résilience en agissant sur la prévention et la lutte contre l'extrémisme violent, la sécurité en ligne et la citoyenneté numérique à travers l'éducation

Centre on Global Counterterrorism Cooperation, The Role of Education in Countering Violent Extremism, décembre 2013.

GCTF et Hedayah, Mémorandum d'Abou Dhabi sur les bonnes pratiques en matière d'éducation pour lutter contre l'extrémisme violent.

HabiloMédias, Utiliser, comprendre et créer : Un cadre de littératie numérique pour les écoles canadiennes, 2019.

National Society for the Prevention of Cruelty to Children (NSPCC), https://learning.nspcc.org.uk/.

RAN Centre of Excellence, Handbook on CVE/PVE training programmes: Guidance for trainers and policy makers, décembre 2017.

RAN Centre of Excellence, Éducation et prévention de la radicalisation : comment les gouvernements peuvent aider les établissements scolaires et les enseignants à prévenir/lutter contre l'extrémisme violent, mai 2019.

RAN Centre of Excellence, Transformer les écoles en laboratoires de la démocratie - Un partenaire pour prévenir la radicalisation violente par l'éducation, octobre 2018.

UNESCO, Guide du personnel enseignant pour la prévention de l'extrémisme violent, 2016.

UNESCO, Global Media and Information Literacy Assessment Framework: Country Readiness and Competencies, 2013.

UNESCO, La prévention de l'extrémisme violent par l'éducation: guide à l'intention des décideurs politiques, 2017.

UNESCO, Les jeunes et l'extrémisme violent dans les médias sociaux: inventaire des recherches, 2017.

UNESCO & Mahatma Gandhi Institute of Education for Peace and Sustainable Development, Youth Led Guide on Prevention of Violent Extremism Through Education, 2017.

United Network of Young Peacebuilders & Search for Common Ground, Translating Youth, Peace & Security Policy into Practice: Guide to kick-starting UNSCR 2250 Locally and Nationally, novembre 2016.

UK Department for Education, Educate Against Hate.

UK Home Office, E-Learning Training on Prevent.

UK Department for Education, Thomas Chisholm & Alice Coulter (Kantar Public), Safeguarding and Radicalisation Research Report, août 2017.

GCTF

GLOBAL COUNTERTERRORISM FORUM