Groupe de travail sur la lutte contre l'extrémisme violent
Initiative pour la communication stratégique

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

Introduction

Dès sa naissance, l'internet a ouvert d'innombrables possibilités à la société, en facilitant le développement économique, la communication, la participation et l'accès à l'information. 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, l'internet est souvent utilisé à mauvais escient par les extrémistes violents et les terroristes. En effet, les groupes extrémistes violents et terroristes recourent de plus en plus aux technologies de la communication en vue 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. Il convient que les gouvernements adoptent les mesures appropriées pour prévenir et lutter contre l'utilisation de l'internet à des fins d'extrémisme violent et de terrorisme (y compris sur les médias sociaux), tout en respectant la vie privée et les libertés d'expression, d'association, de réunion pacifique, de croyance ou de religion, ainsi qu'en respectant les impératifs d'une connectivité mondiale préservée et de la libre circulation de l'information en toute sécurité. Ces mesures sont regroupées dans deux catégories principales :

1. **Mesures fondées sur les contenus :** Il s'agit des efforts déployés 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, le retrait et le filtrage de contenus, au moyen de réglementations et d'une législation appropriées.
2. **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 ou terroriste par le biais de la communication stratégique, notamment en soutenant les organisations de la société civile qui diffusent des contre-discours et des récits alternatifs, tant en ligne qu'hors ligne.

Dans son cinquième examen de la *Stratégie Antiterroriste Mondiale des Nations Unies*, l'Assemblée générale des Nation Unies a affirmé l'importance de la coopération entre parties prenantes dans la mise en œuvre de la Stratégie, y compris parmi les États membres, les organisations internationales, régionales et sous-régionales, 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), tout en se conformant aux obligations qu'impose le respect des droits de l'homme, des libertés fondamentales et du droit international, notamment des buts et principes énoncés dans la Charte. L'Assemblée générale a souligné qu'il est essentiel de mettre en place des moyens aussi efficaces que possible pour lutter contre les activités de propagande, d'incitation au terrorisme et de recrutement déployées par les terroristes, en particulier sur l'internet, en conformité avec le droit international, y compris le droit international des droits de l'homme. En outre,

[1] Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et de la télématique dans le contexte de la sécurité internationale (A/70/174), 22 juillet 2015, § 2.

l'Assemblée générale recommande que les États membres envisagent la mise en œuvre des recommandations pertinentes et applicables dans le contexte national du *Plan d'action du Secrétaire général des Nations Unies pour la prévention de l'extrémisme violent*, lequel définit les communications stratégiques, l'internet et les médias sociaux comme des champs d'action prioritaires dans la prévention et la lutte contre l'extrémisme violent et le terrorisme[2].

La déclaration du Président du Conseil de sécurité des Nations Unies publiée en mai 2016 (S/PRST/2016/6) réaffirme que la communauté internationale doit concevoir des moyens efficaces de combattre la propagande terroriste, l'incitation au terrorisme et le recrutement à ces fins, notamment en utilisant l'internet, tout en se conformant aux principes du droit international, dont le droit international des droits de l'homme[3]. À la demande du Conseil de sécurité des Nations Unies, le Comité contre le terrorisme a présenté le 28 avril 2017 au Conseil une proposition visant à mettre en place un cadre international exhaustif pour lutter contre les discours terroristes[4]. Sur la base de ces propositions, le Conseil de sécurité a adopté la résolution 2354 (2017), soulignant la nécessité pressante de lutter à l'échelle mondiale contre les activités menées par certains groupes extrémistes violents et terroristes pour inciter à commettre des actes de terrorisme et pour recruter à cette fin et notant que les terroristes exploitent les secteurs des TIC, en particulier l'internet et les médias sociaux, pour élaborer un discours fallacieux ainsi que pour mobiliser des ressources et obtenir l'appui de sympathisants.

Lors de la septième réunion plénière ministérielle célébrée à New York le 21 septembre 2016, les ministres des 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 acquises en matière de prévention en ligne et de contre-mesures destinées à lutter contre l'extrémisme violent en ligne, dans le cadre de *l'Initiative du GCTF visant à interrompre le processus de radicalisation menant à la violence* (en abrégé, « Initiative sur le processus de radicalisation »).

En conséquence, les recommandations non contraignantes présentées ci-après constituent une liste non exhaustive de bonnes pratiques gouvernementales sur les aspects relatifs aux communications stratégiques et aux médias sociaux de la prévention et de la lutte contre l'extrémisme violent et le terrorisme en ligne, destinée aux membres du GCTF ainsi qu'à tout gouvernement intéressé. Les bonnes pratiques énoncées dans ce document ont été identifiées lors des réunions et discussions tenues par la suite avec les membres du GCTF et reflètent leur expérience en la matière. De plus, à travers ces recommandations, le GCTF vise à soutenir et à compléter les travaux et les initiatives existantes menées par d'autres organisations internationales et régionales, à savoir l'ONU et d'autres parties prenantes pertinentes œuvrant dans ce domaine[5].

---

[2] Examen de la Stratégie antiterroriste mondiale des Nations Unies (A/RES/70/291), 19 juillet 2016, § 42f et 40 du dispositif. Concernant le Plan d'action du Secrétaire général des Nations Unies pour la prévention de l'extrémisme violent, cf. A/70/674, 24 décembre 2015, § 55.

[3] Conseil de sécurité des Nations Unies, Déclaration du Président du Conseil de sécurité (S/PRST/2016/6), 11 mai 2016.

[4] Cadre international global de lutte contre la propagande terroriste (S/2017/375), 28 avril 2017.

[5] Il s'agit notamment de l'initiative de la Direction exécutive du Comité contre le terrorisme (DECT) de l'ONU et de la fondation ICT4Peace visant à approfondir la perception des entreprises du secteur privé dans leur réponse à l'utilisation terroriste de leurs produits et services et à d'autres problématiques connexes, et à promouvoir l'autoréglementation et le partage de bonnes pratiques au sein du secteur des TIC, www.techagainstterrorism.org ; du Forum de l'UE sur l'internet pour la détection des contenus terroristes en ligne ; du Programme d'autonomisation de la société civile du Forum de l'UE sur l'internet (lancé en 2016 lors du deuxième Forum de l'UE afin de soutenir les efforts de la société civile pour élaborer des contre-discours efficaces en ligne, en partenariat avec le secteur privé) ; du Code de conduite de la Commission européenne, qui

Les bonnes pratiques se répartissent en trois catégories :

- La section I regroupe les bonnes pratiques transversales de prévention et de lutte contre le terrorisme et l'extrémisme violent en ligne ;
- La section II regroupe les bonnes pratiques relatives aux mesures fondées sur les contenus ;
- La section III regroupe les bonnes pratiques relatives aux mesures fondées sur la communication.

Il convient de considérer les sections I, II et III comme se complétant pour définir une approche globale de prévention et de lutte contre l'extrémisme violent et le terrorisme sur l'internet et sur les plateformes des médias sociaux.

Les bonnes pratiques faisant l'objet des présentes recommandations sont destinées à combattre l'extrémisme violent pouvant mener au terrorisme, sous toutes ses formes et dans toutes ses manifestations. Il convient de souligner que l'extrémisme violent et le terrorisme n'appartiennent en propre à aucune région, nationalité ou croyance particulières. Tant les membres du GCTF que tout autre gouvernement intéressé sont invités à envisager la mise en œuvre de ces bonnes pratiques dans leur contexte national respectif, en les adaptant à la situation et à la culture locales, afin de s'assurer de la conformité des mesures prises pour lutter contre le terrorisme et l'extrémisme violent – en particulier celles visant à contrecarrer les discours qui les sous-tendent – avec les obligations des États membres au titre du droit international, dont le droit international des droits de l'homme, et du respect de l'état de droit.

Ces recommandations soulignent l'importance d'inscrire fermement les mesures, qu'elles soient fondées sur les contenus ou sur la communication, dans une approche globale de prévention et de lutte contre l'extrémisme violent et le terrorisme aussi bien en ligne qu'hors ligne, en s'assurant de la participation et de la collaboration active des États et organisations internationales et régionales, tout en veillant au respect de la vie privée et du droit aux libertés d'expression, d'association, de réunion pacifique, de religion et de croyance , mais aussi, comme le souligne le rapport du 22 juillet 2015 du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et de la télécommunication dans le contexte de la sécurité internationale, en veillant à préserver la connectivité mondiale et la libre circulation de l'information en toute sécurité[6]. Cette approche globale intégrera des mesures tant préventives que de sécurité et de justice pénale, en conformité avec le droit international, tout en garantissant une appropriation nationale afin d'aborder de manière équilibrée[7], l'ensemble des moteurs tant internes qu'externes de l'extrémisme violent menant au terrorisme ainsi que les manifestations du terrorisme et de l'extrémisme violent sur l'internet et sur les plateformes des médias sociaux. Afin d'intervenir efficacement sur la disponibilité, l'accessibilité

---

contient une série d'engagements visant à lutter contre la propagation des discours de haine illégaux en Europe ; du projet Clean IT de l'UE, un dispositif public-privé qui examine les utilisations terroristes de l'internet ; du Groupe de travail du Réseau de sensibilisation à la radicalisation (RAN) de l'UE sur les communications et les discours (RAN C&N), qui s'intéresse aux meilleures pratiques et enseignements tirés de la communication de contre-discours entre praticiens de la société civile ; du Réseau européen des communications stratégiques (ESCN) chargé de mettre en place et d'organiser un réseau des États membres de l'UE, dans une approche basée sur la communication, afin de mieux comprendre et de faire face aux défis des nouvelles communications, y compris les discours de division diffusés par l'EEIL/*Da'esh* et l'extrémisme violent d'extrême droite ; de la Cellule de communication de la Coalition mondiale, qui anime des campagnes et renforce les capacités de lutte contre le discours de l'EEIL/*Da'esh*.

[6] Voir le Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et de la télématique dans le contexte de la sécurité internationale (A/70/174), 22 juillet 2015, § 30. Dans son avant-propos, le Secrétaire général des Nations Unies mentionne la nécessité de « soutenir l'engagement mondial à promouvoir un internet ouvert, sûr et pacifique ».

[7] Examen de la Stratégie antiterroriste mondiale des Nations Unies (A/RES/70/291), §39.

et l'influence en ligne des contenus relevant de l'extrémisme violent et du terrorisme, il est essentiel de faire en sorte que les autorités nationales compétentes exercent correctement leur capacité d'enquête et de poursuites à l'égard des personnes perpétrant des actions extrémistes violentes et terroristes , y compris sous forme de facilitation délictueuse de l'extrémisme violent et du terrorisme en ligne, notamment par le recrutement, le financement des terroristes, la planification et la coordination d'attentats, la diffusion de menaces et autres délits. En outre, cette approche globale suppose de prendre en compte le rôle essentiel joué par les médias pour « améliorer le dialogue et l'esprit d'ouverture, promouvoir la tolérance et le vivre ensemble, et encourager la mise en place d'un environnement qui ne soit pas propice à l'incitation au terrorisme, ainsi que pour lutter contre les discours terroristes »[8]. Dans sa « Déclaration sur la liberté d'expression et d'information dans les médias dans le contexte de la lutte contre le terrorisme », le Conseil de l'Europe a invité les médias et les journalistes à garder à l'esprit leurs responsabilités particulières afin de ne pas contribuer aux objectifs poursuivis par les terroristes, en particulier en prenant garde à ne pas accroître le sentiment de peur que peuvent susciter les actes terroristes et à ne pas offrir de tribune aux terroristes en leur donnant une place démesurée, et à adopter des mesures d'autorégulation, lorsqu'elles n'existent pas, ou adapter les mesures existantes afin qu'elles répondent efficacement aux questions déontologiques soulevées par la couverture médiatique de l'extrémisme violent et du terrorisme , et les mettre en œuvre[9].

Les bonnes pratiques présentées dans ce document n'entérinent aucune méthode particulière, mais prennent acte des diverses approches adoptées par les États pour faire face à l'extrémisme violent et au terrorisme et au déploiement de leurs discours sur l'internet et sur les plateformes des médias sociaux. 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.

Bonnes pratiques

I. Bonnes pratiques transversales de prévention et de lutte contre l'extrémisme violent et le terrorisme en ligne

Bonne pratique n° 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.

Les gouvernements sont encouragés à adopter et à mettre en œuvre des mesures visant à prévenir et à lutter contre le terrorisme et l'extrémisme violent en ligne, en conformité avec les obligations des États en vertu du droit international et dans le respect des principes de l'état de droit. Un large éventail de mesures est envisageable : conception et application de stratégies nationales de communication visant à réfuter les récits de l'extrémisme violent[10], mise en cause des tentatives de justification ou de glorification (apologie) des actes terroristes, législation interdisant (si nécessaire et en conformité avec les obligations relevant du droit international) l'incitation à commettre des actes terroristes[11].
Aux termes des résolutions 2354 (2017), 2178 (2014) et 1624 (2005) du Conseil de sécurité des Nations

[8] Résolution du Conseil de sécurité des Nations Unies, § 13 du préambule.

[9] 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, lors de la 917e réunion des Délégués des Ministres (https://wcd.coe.int/ViewDoc.jsp?p=&Ref=Decl-02.03.2005&Language=lanFrench&Ver=original&Site=COE&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75&direct=true).

[10] Assemblée générale des Nations Unies, Plan d'action du Secrétaire général des Nations Unies pour la prévention de l'extrémisme violent, (A/70/674), 24 décembre 2015, § 55 (a).

[11] Résolution 2354 (2017) du Conseil de sécurité des Nations Unies, § 12 du préambule, et Résolution 1624 (2005) du Conseil de sécurité des Nations Unies, § 1 (a) du dispositif.

Unies, les mesures législatives et politiques prises par les États à l'échelle nationale pour lutter contre le terrorisme, notamment en ligne, doivent respecter les obligations incombant aux États en vertu du droit international, notamment le droit international des droits de l'homme, le droit des réfugiés et le droit humanitaire. Sont incluses parmi ces obligations celles relevant des accords, conventions et pactes internationaux précédemment souscrits par l'État, tels le Pacte international relatif aux droits civils et politiques (PIDCP), le Pacte international relatif aux droits économiques, sociaux et culturels (PIDESC) et la Convention internationale sur l'élimination de toutes les formes de discrimination raciale (CIEDR). Il est important de noter que dans le contexte de la prévention et de la lutte contre l'extrémisme violent, l'adoption de mesures efficaces et la protection des droits de l'homme ne constituent pas des objectifs contradictoires, étant au contraire complémentaires et se renforçant mutuellement.

En outre, il est recommandé aux législateurs et autorités chargées de concevoir les politiques de faire en sorte que les termes tels que « extrémisme violent », « lutte contre l'extrémisme violent » et « terrorisme » soient bien définis et/ou compris dans les textes de loi nationaux ainsi que dans les plans d'action[12]. L'existence de ces définitions est garante de la justesse avec laquelle les États perçoivent cette problématique et cernent leurs réponses, en établissant une distinction entre les réponses légales et celles qui ne le sont pas. Elle permet également d'éviter toute interprétation ou application arbitraires des dispositions légales, susceptibles de compromettre la certitude légale ou d'enfreindre les principes de l'état de droit.

Bonne pratique n° 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.

L'une des caractéristiques intrinsèques de l'internet est sa complexité technique. Cette technologie en permanente évolution ouvre d'immenses perspectives nouvelles, tout en présentant des faiblesses susceptibles d'être exploitées par les extrémistes violents et les terroristes. Par conséquent, il est recommandé aux gouvernements de se donner les moyens de bien comprendre l'évolution des tendances technologiques ainsi que les problèmes que celles-ci peuvent engendrer. Cette connaissance passe par l'analyse des audiences pertinentes en ligne, des plateformes les plus courantes et des contenus nouveaux et populaires. Le cas échéant, elle permet aussi de mesurer l'impact des « chambres d'écho » et des « bulles filtrantes » algorithmiques qui opèrent sur l'internet[13].
Les gouvernements sont également encouragés à investir dans des outils de recherche et analytiques

---

[12] Sans exclure d'autres définitions ou termes utilisés par ailleurs, y compris dans la législation nationale, une référence pouvant être prise en compte pour déterminer ce qui est généralement entendu par « actes terroristes » est celle qui figure au § 3 de la Résolution 1566 (2004) du Conseil de sécurité des Nations Unies : « […] 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, [et] ne sauraient en aucune circonstance être justifiés par des motifs de nature politique, philosophique, idéologique, raciale, ethnique, religieuse ou similaire […] ».

[13] 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'autres opinions alternatives ou dissidentes. Les « bulles filtrantes » se réfèrent aux effets probable de la personnalisation par les moteurs de recherche ou les réseaux sociaux des résultats ou flux d'actualités grâce à des modèles informatiques apprenants 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.

afin de mieux connaître les impacts en ligne et hors ligne de la communication des extrémistes violents cherchant à radicaliser et à recruter des individus à des fins violentes et à polariser les communautés. Ces outils permettent aussi de faire ressortir les tendances générales des conversations virtuelles ainsi que des audiences et influences s'exerçant en ligne, au-delà des seules communications à caractère terroriste.

Bonne pratique n° 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.

Afin que l'approche adoptée soit exhaustive et graduée, il est impératif de veiller à ce que les efforts déployés pour lutter contre l'extrémisme violent en ligne s'inscrivent dans une stratégie en ligne claire et globale dotée d'objectifs spécifiques, mesurables et réalistes.

La stratégie menée par les gouvernements doit intégrer 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 et buts assignés à la stratégie globale, tout en mettant en place des garanties visant à s'assurer que ces réponses sont proportionnées ou qu'elles produisent les effets escomptés. Les gouvernements sont invités à veiller à ce qu'un contrôle soit exercé sur ces réponses tout au long de leur déploiement, parallèlement aux évaluations conduites au regard de leurs buts et objectifs stratégiques globaux, en recourant à des indicateurs et à des méthodologies cohérentes et comparables.

Cette stratégie gouvernementale en ligne doit promouvoir une approche sociétale favorisant les synergies entre parties prenantes pertinentes et s'inscrire dans des stratégies nationales plus larges de prévention et de lutte contre l'extrémisme violent et le terrorisme ainsi que dans des cadres politiques garantissant la bonne coordination des efforts déployés tant en ligne qu'hors ligne pour faire face aux menaces. Il peut s'agir d'initiatives visant à favoriser la pensée critique, les compétences numériques et la résilience par l'éducation, mais aussi d'activités de mobilisation des communautés locales et d'autres mesures destinées à influer sur les facteurs sociaux et personnels pouvant amener les individus à soutenir l'extrémisme violent et le terrorisme.

Une telle stratégie globale pourra voir son efficacité renforcée grâce à l'établissement d'une unité spéciale nationale inter-agences chargée de synchroniser et d'intégrer les activités et les programmes pangouvernementaux de prévention et de lutte contre l'extrémisme violent et le terrorisme, d'effectuer la planification stratégique et d'évaluer les initiatives en cours dans ce domaine aussi bien en ligne qu'hors ligne.

Bonne pratique n° 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.

Le suivi et l'évaluation des programmes et des politiques relatifs à l'extrémisme violent sont des éléments déterminants de la conception d'objectifs et d'indicateurs de réussite réalistes et permettent de garantir l'efficacité et la durabilité des mesures adoptées. En même temps, ces cadres renforcent la transparence et permettent de mieux appréhender les programmes et les politiques. La mise en place d'un cadre commun et exhaustif de suivi et d'évaluation assorti d'indicateurs clairs est une condition indispensable pour mesurer les succès enregistrés.
En outre, l'existence de ce cadre est considérée essentielle pour assurer la légitimité et l'efficacité des actions engagées en vue de prévenir et de lutter contre l'extrémisme violent et le terrorisme en ligne.

Le suivi et l'évaluation continus des politiques et des programmes collaboratifs fondés tant sur les contenus que sur la communication permettent également d'améliorer ces mesures en permanence, ce qui à terme accroît leur impact.

Néanmoins, des travaux de recherche ont fait ressortir la complexité des opérations de suivi et d'évaluation de ce type de programmes et politiques. Les gouvernements sont donc invités à établir des analogies avec les cadres de suivi et d'évaluation utilisés dans d'autres secteurs, chaque fois que cela est possible et pertinent, par exemple dans les domaines de la prévention des gangs, de la mobilisation des communautés locales ou de lutte contre l'exploitation sexuelle des enfants en ligne.

En général, 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 et concrets permettant de mesurer le succès d'une politique ou d'un programme donné en matière de prévention et de lutte contre l'extrémisme violent, tout en préservant les droits de l'homme, notamment le droit à la liberté d'expression, tels que garantis par la Déclaration universelle des droits de l'homme et par le PIDCP[14]. Ces indicateurs doivent servir à évaluer les objectifs et les buts fixés dans le cadre de la stratégie concernée. Les gouvernements sont également encouragés à partager les meilleures pratiques et l'information relatives aux politiques et programmes nationaux d'évaluation afin de pérenniser les coopérations.

Bonne pratique n° 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.

L'internet étant transnational par essence, la coopération internationale est indispensable pour prévenir et lutter contre l'extrémisme violent et le terrorisme en ligne. Les efforts concertés et coordonnés entre gouvernements améliorent la connaissance et la perception des défis posés par l'extrémisme violent et le terrorisme sur l'internet et sur les plateformes des médias sociaux [15].

La coopération internationale facilite le renforcement des capacités grâce au partage de bonnes pratiques garantissant le caractère complémentaire et durable des mesures nationales visant à lutter contre la propagande extrémiste violente et terroriste et à en limiter l'impact – tant en ligne qu'hors ligne. Les forums internationaux peuvent faciliter les discussions approfondies sur la création de synergies au sein de la communauté internationale afin de maximiser les efforts collectifs et d'agréger l'expertise sur la prévention et la lutte contre l'extrémisme violent et le terrorisme sur l'internet et sur les plateformes des médias sociaux. En outre, ces forums sont à même de créer un environnement de confiance mutuelle, de même qu'ils contribuent à mettre en place des plateformes de communication plus riches et à garantir une utilisation plus efficace et efficiente des ressources.
Enfin, les gouvernements sont encouragés à renforcer l'entraide judiciaire, à participer à des plateformes régionales de coopération et à élaborer et améliorer les dispositifs permettant une

[14] Comme rappelé 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 PIDCP adopté par l'Assemblée générale en 1966, et 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.

[15] On peut citer comme exemples témoignant de l'élargissement et de l'approfondissement de la prise de conscience collective des défis posés par l'extrémisme violent sur l'internet, la tenue de la Réunion spéciale du Comité contre le terrorisme des Nations Unies à New York en 2016, où les États membres et les organisations internationales et régionales compétentes, les organisations de la société civile et le secteur privé ont abordé le thème des « moyens d'empêcher les terroristes d'exploiter l'Internet et les médias sociaux à des fins terroristes, tout en respectant les droits de l'homme et les libertés fondamentales », ainsi que du deuxième Symposium du GCTF sur la prévention et la lutte contre l'utilisation de l'internet par les terroristes à Beijing en 2016.

coopération transrégionale accélérée[16]. En particulier, les organisations internationales et régionales peuvent jouer un rôle important dans le domaine du renforcement des capacités destinées à exploiter les preuves numériques afin d'améliorer les enquêtes[17]. Par exemple, le système mondial de communication policière INTERPOL I-24/7 permet la transmission d'informations opérationnelles en soutien des enquêtes criminelles.

Bonne pratique n° 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.

Compte tenu de la nature transnationale de l'internet, la prévention et la lutte contre l'extrémisme violent et le terrorisme en ligne ne peuvent réussir qu'en mettant en place une collaboration efficace entre les gouvernements, le secteur des TIC et les organisations pertinentes de la société civile. Cette approche pluri-acteurs associant des expertises politiques, techniques et contextuelles est fructueuse aussi bien pour les réponses fondées sur les contenus que pour celles fondées sur la communication[18]. Un dialogue ouvert entre les principaux acteurs compétents est indispensable à la mise en place d'une coopération efficace et durable fondée sur le partage des responsabilités entre les États, le secteur des TIC et les organisations de la société civile afin de prévenir et de lutter contre l'extrémisme violent et le terrorisme.

Une approche pluri-acteurs gagne en efficacité dès lors que les parties prenantes pertinentes ont une perception commune de leurs responsabilités et rôles respectifs, ainsi que de leurs limitations et atouts particuliers en matière de réponse à l'extrémisme violent en ligne. À cet égard, les gouvernements peuvent jouer un rôle important en nouant un dialogue avec le secteur des TIC en vue de lutter contre l'extrémisme violent et le terrorisme en ligne, basé sur une participation et collaboration volontaires, et en apportant une aide aux parties prenantes pertinentes, en particulier par la mise en place de plateformes de collaboration en ligne et hors ligne. Ces plateformes favorisent un processus plus inclusif, ouvrent de nouveaux canaux de communication, renforcent les capacités, désamorcent les conflits d'intérêts et font apparaître les lacunes critiques. Ce type d'efforts concertés permet de prévenir d'éventuels chevauchements d'activités tout en facilitant la complémentarité des actions et la rationalisation des initiatives pluri-acteurs, par exemple sous forme de partenariat public-privé. Les gouvernements sont également encouragés à soutenir et à participer aux initiatives émanant du secteur privé[19].

---

[16] Résolution 2322 (2016) du Conseil de sécurité des Nations Unies, § 13 (h).

[17] 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, (S/2017/375), § 5. [18] On peut citer l'exemple de l'initiative de la DECT de l'ONU et de la fondation ICT4Peace qui vise à approfondir la perception des entreprises du secteur privé dans leur réponse à l'utilisation terroriste de leurs produits et services et à d'autres problématiques connexes, et à promouvoir l'autoréglementation et le partage de bonnes pratiques au sein du secteur des TIC, www.techagainstterrorism.org.

[18] On peut citer l'exemple de l'initiative de la DECT de l'ONU et de la fondation ICT4Peace qui vise à approfondir la perception des entreprises du secteur privé dans leur réponse à l'utilisation terroriste de leurs produits et services et à d'autres problématiques connexes, et à promouvoir l'autoréglementation et le partage de bonnes pratiques au sein du secteur des TIC, www.techagainstterrorism.org.

[19] Un exemple pertinent de ces efforts est la création du *Forum mondial de l'internet contre le terrorisme*, annoncée en juin 2017 par ses concepteurs (Microsoft, Twitter, Facebook et Google), qui vise à accélérer et à renforcer la collaboration autour des mesures fondées sur les contenus et sur la communication et à travailler avec les organisations de la société civile, les gouvernements et les organisations régionales et internationales (https://newsroom.fb.com/news/2017/06/global-internet-forum-to-counter-terrorism).

Le secteur des TIC possède des compétences techniques, des capacités d'accès et des ressources qui pourraient être exploitées pour assurer la réussite des mesures mises en œuvre pour prévenir et lutter contre l'extrémisme violent en ligne. Par exemple, les sociétés du secteur des TIC détiennent l'expertise technique nécessaire pour développer des outils et des mécanismes (tant humains qu'automatisés) afin de contrer les discours des extrémistes violents et des groupes terroristes et d'élaborer des solutions permettant d'identifier et de retirer rapidement tout contenu extrémiste violent et terroriste diffusé sur l'internet. Les organisations de la société civile ont souvent un fort enracinement au sein des communautés locales et bénéficient donc d'une meilleure crédibilité auprès des principaux publics visés, ce qui les met en meilleure position pour soutenir l'élaboration de réponses efficaces et durables à l'échelle de ces communautés.

II. Bonnes pratiques relatives aux mesures fondées sur les contenus

Bonne pratique n° 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.

Le droit à la liberté d'expression est l'un des piliers du cadre du droit international des droits de l'homme. En même temps, il peut faire l'objet de certaines restrictions, dans des circonstances spécifiques précisées à l'article 19 (3) du PIDCP[20]. Le cas de l'incitation à commettre un ou plusieurs actes terroristes peut faire partie de ces exceptions[21]. Il est important de noter que toute restriction légale à la liberté d'expression doit se conformer aux obligations incombant aux États en vertu du droit international, y compris les droits de l'homme et de la législation nationale en la matière.

Les gouvernements peuvent légitimement restreindre le droit à la liberté d'expression dans les situations spécifiques où une telle restriction est prévue par la loi en vertu du respect des droits ou de la réputation de tiers ou de la nécessité de protéger la sécurité nationale ou l'ordre public, dès lors que la restriction est proportionnée[22]. Les manifestations en ligne de l'extrémisme violent et du terrorisme pouvant représenter une menace pour la sécurité nationale et/ou l'ordre public, elles peuvent, dans certains cas, être restreintes, sous réserve de l'existence d'une prohibition légale et justifiée en vertu des dispositions de l'article 19 (3) du PIDCP. À cet égard, les gouvernements sont encouragés à définir clairement cette typologie de délits dans leurs législations nationales respectives, de sorte que les individus puissent connaître et anticiper les conséquences de leurs actes.

---

[20] L'article 20 du PIDCP, qui prohibe toute propagande en faveur de la guerre, tout appel à la haine nationale, raciale ou religieuse qui constitue une incitation à la discrimination, à l'hostilité ou à la violence est également pertinent dans ce contexte. À cet égard, l'Observation générale n° 34 du Comité des droits de l'homme considère que les articles 19 et 20 du PIDCP sont compatibles et se complètent l'un l'autre. Les actes visés à l'article 20 tombent tous sous le coup des restrictions énoncées au paragraphe 3 de l'article 19. Dans tous les cas où l'État restreint la liberté d'expression, il est nécessaire de justifier les interdictions et les dispositions qui les définissent, dans le strict respect de l'article 19 (CCPR/HRC/GC/34, 12 septembre 2011, § 50 f).

[21] Voir aussi les Résolutions 2354 (2017) et 1624 (2005) du Conseil de sécurité des Nations Unies, qui condamnent l'incitation à commettre des actes de terrorisme et réprouvent toute tentative de justifier ces actes ou d'en faire l'apologie, qui serait de nature à inciter à en commettre de nouveaux. La Résolution 1624 (2005) du Conseil de sécurité des Nations Unies, au § 1 (a) du dispositif, appelle tous les États à adopter des mesures qui peuvent être nécessaires et appropriées et sont conformes aux obligations qui leur incombent en vertu du droit international, pour Interdire par la loi l'incitation à commettre un ou des actes terroristes.

[22] Article 19 (3) du PIDCP ; Article 19 de la Déclaration universelle des droits de l'homme ; voir l'Observation générale n° 34 du Comité des droits de l'homme sur la liberté d'opinion et la liberté d'expression, CCPR/C/GC/34, 12 septembre 2011, § 21-36.

En même temps, les communications moralement répugnantes, choquantes, dérangeantes ou vexatoires ne relèvent généralement pas d'une qualification pénale. L'un des moyens les plus efficaces de contrer ce type de communication consiste à mettre en place un débat ouvert et pluraliste pour examiner ces idées et opinions de manière respectueuse afin de promouvoir la compréhension interculturelle. La récusation de ces idées lors de débats plus nombreux, en donnant la parole aux membres de toutes les communautés contribue à mettre en lumière le caractère fallacieux et mensonger qui leur est associé.

Un autre droit qui doit être pris en considération lors du traitement des contenus extrémistes violents et terroristes sur l'internet est le droit à ne pas être l'objet d'immixtion arbitraire ou illégale dans sa vie privée, comme le prévoient l'article 12 de la Déclaration universelle des droits de l'homme et l'article 17 du PIDCP. Il est rappelé que toute personne a droit à la protection de la loi contre de telles immixtions arbitraires ou illégales[23].

Bonne pratique n° 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

Divers documents recommandent aux gouvernements – mais aussi au secteur des TIC – de prendre en compte l'existence de normes et/ou principes internationaux afin de se conformer aux obligations du droit international lors du traitement des contenus extrémistes violents et terroristes sur l'internet. Parmi ces documents, figurent notamment (mais non exclusivement), la Résolution 16/18 du Conseil des droits de l'homme des Nations Unies (Lutte contre l'intolérance, les stéréotypes négatifs, la stigmatisation, la discrimination, l'incitation à la violence et la violence visant certaines personnes en raison de leur religion ou de leur conviction)[24], le Plan d'action de Rabat sur l'interdiction de l'appel à la haine nationale, raciale ou religieuse qui constitue une incitation à la discrimination, à l'hostilité ou à la violence[25], l'article 19 des Principes de Camden sur la liberté d'expression et l'égalité[26] ou la Note de politique de la Global Network Initiative sur les contenus à caractère extrémiste et le secteur des TIC[27] ; tous ces documents peuvent fournir des orientations pratiques, si besoin et le cas échéant. Les principes de Camden contiennent des orientations générales sur la manière de préserver le droit à la liberté d'expression en conformité avec les obligations des États relevant du droit international des droits de l'homme ; de son côté, la note de politique de la Global Network Initiative contient un ensemble de recommandations pratiques pour les gouvernements et le secteur des TIC concernant la prévention de l'extrémisme violent et du terrorisme sur l'internet.

---

[23] Assemblée générale des Nations Unies, Rapport du Haut-Commissaire des Nations Unies aux droits de l'homme sur les pratiques optimales et les enseignements tirés concernant la façon dont la protection et la promotion des droits de l'homme contribuent à prévenir et à combattre l'extrémisme violent (A/HRC/33/29), 21 juillet 2016, p. 15f, disponible en ligne : https://daccess-ods.un.org/TMP/4224119.18640137.html.

[24] Conseil des droits de l'homme des Nations Unies, Lutte contre l'intolérance, les stéréotypes négatifs, la stigmatisation, la discrimination, l'incitation à la violence et la violence visant certaines personnes en raison de leur religion ou de leur conviction (A/HRC/RES/16/18), 12 avril 2011. Disponible en ligne : http://www2.ohchr.org/english/bodies/hrcouncil/docs/16session/A.HRC.RES.16.18_en.pdf.

[25] Assemblée générale des Nations Unies, Additif au Rapport annuel du Haut-Commissaire des Nations Unies aux droits de l'homme 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, disponible en ligne : http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session22/A-HRC-22-17_Add4_fr.pdf.

[26] Article 19, Principes de Camden sur la liberté d'expression et l'égalité, avril 2009, disponible en ligne : http://www.refworld.org/docid/4b5826fd2.html

[27] Global Network Initiative Policy Brief, Extremist Content and the ICT Sector, novembre 2016, disponible en ligne : https://www.globalnetworkinitiative.org/sites/default/files/Extremist-Content-and-ICT-Sector.pdf.

Bonne pratique n° 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.

Compte tenu de l'importance du rôle du secteur des TIC dans la mise à disposition des outils, services et infrastructures nécessaires aux communications en ligne, il est vital de poursuivre la collaboration entre les gouvernements et ce secteur afin de traiter efficacement et de manière efficiente le problème 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. Cette collaboration peut prendre plusieurs formes et sa mise en place dépend du contexte national. Certains États ont introduit des mécanismes faisant intervenir de manière concertée les acteurs du secteur public et privé dans le but de réduire l'accessibilité des contenus à caractère extrémiste violent et terroriste en ligne, notamment en bloquant, filtrant ou retirant ces contenus. Dans certains pays, les autorités compétentes identifient les contenus à caractère terroriste et informent les fournisseurs de service de l'utilisation potentiellement illicite qui est faite de leurs plateformes. Dans d'autres, le retrait de ces contenus ne peut être imposé par les autorités nationales, dans la mesure où une telle interdiction constituerait une violation de leurs obligations en vertu du droit international, en particulier le droit international des droits de l'homme, et du droit national.

Il est recommandé aux gouvernements de prendre en compte les initiatives pluri-acteurs existantes et de tirer les leçons de leur expérience lors de la conception d'un cadre spécifique de collaboration. L'une des méthodes possibles pour renforcer la collaboration entre les gouvernements et le secteur des TIC dans la perspective de cette bonne pratique consiste à mettre en place des « unités référentes internet » (IRU) qui serviront de points focaux dans le cadre de la coordination et collaboration volontaires entre différentes agences gouvernementales et le secteur des TIC[28]. Ces unités ont pour principale tâche d'identifier les contenus extrémistes violents et terroristes sur l'internet, en veillant à se conformer aux obligations des États en vertu du droit international et national, et d'en référer aux entreprises pertinentes du secteur afin que celles-ci procèdent à l'évaluation des contenus identifiés, comme le prévoient leurs propres conditions d'utilisation. Il est important de noter que cette activité de référencement ne constitue pas un acte exécutoire. La décision de retirer le contenu en ligne ainsi identifié revient à l'entreprise du secteur des TIC, conformément à ses propres termes et conditions d'utilisation, sauf dispositions contraires de la législation nationale. Ces unités peuvent également servir de plateforme pour faciliter l'échange d'informations au moyen de réunions périodiques entre les partenaires nationaux et les entreprises pertinentes du secteur des TIC. Cet aspect s'avère particulièrement important pour éviter de s'immiscer ou d'interférer dans les investigations en cours conduites par les services de renseignement ou dans les enquêtes ou poursuites judiciaires lancées contre des individus ou des groupes.

Il est recommandé de coopérer avec les organisations de la société civile à même de contribuer à l'identification et au signalement des contenus à caractère extrémiste violent et terroriste sur l'internet, en s'inspirant de la méthode utilisée pour lutter contre les publications à caractère pédophile sur l'internet[29]. Pourraient s'engager dans une telle collaboration les forces de l'ordre, le secteur des TIC et toute organisation de la société civile détenant des compétences dans la prévention et la lutte contre l'extrémisme violent et le terrorisme. Les organisations de la société civile intéressées pourraient procéder ainsi à la détection proactive et volontaire des contenus extrémistes violents et

[28] Des « unités référentes internet » (IRU) sont en place par exemple dans l'Union européenne, aux Pays-Bas et au Royaume-Uni.

[29] Une analogie peut être faite à cet égard avec la détection des publications à caractère pédophile sur l'internet et avec les travaux de la fondation Internet Watch Foundation.

terroristes et mettre à disposition du public une plateforme permettant de signaler ces contenus de manière anonyme. Les organisations de la société civile peuvent choisir d'intégrer en leur sein et/ou de collaborer avec des équipes ayant reçu une formation spécifique afin d'évaluer les contenus en ligne qui auront été signalés ; dans un deuxième temps, en étroite collaboration avec les parties prenantes des secteurs public et privé, selon les cas, elles signaleront les contenus problématiques aux entreprises du secteur des TIC, qui devront les examiner au regard des dispositions de leurs conditions d'utilisation et/ou engager les procédures de signalement de contenus illicites auprès des forces de l'ordre, suivant les cas. Les organisations de la société civile peuvent par la suite vérifier si les contenus signalés sont toujours en ligne ou non.

Bonne pratique n° 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.

Il est recommandé aux gouvernements d'indiquer clairement les lois et les réglementations en vertu desquelles sont notifiés aux fournisseurs de services les contenus en ligne à caractère extrémiste violent et terroriste, ou justifiant les injonctions de retrait, de filtrage ou de blocage de ces contenus. Cette franchise lors des décisions et des procédures exécutoires permet de renforcer la confiance mutuelle entre les différents intervenants, contribuant ainsi à promouvoir une plus grande transparence. En parallèle, les gouvernements sont encouragés à émettre des lois et des réglementations pertinentes qui serviront de fondement juridique au traitement des contenus à caractère extrémiste et violent publiés sur l'internet ; il leur est également recommandé de renseigner les fournisseurs de TIC sur les autorités compétentes en matière de traitement des contenus à caractère violent et extrémiste qui sont autorisées à procéder à ces signalements.

En outre, afin d'améliorer la transparence et la surveillance exercée, il est recommandé aux unités référentes internet et au secteur des TIC de continuer à publier des rapports périodiques précisant le nombre total de signalements et de retraits de contenus.

Bonne pratique n° 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.

En ce qui concerne le traitement de la disponibilité et de l'accessibilité des contenus extrémistes violents et terroristes en ligne, on peut considérer que le rôle essentiel joué par le secteur des TIC relève du contrôle que celui-ci exerce concrètement sur les plateformes de communication en ligne. Le secteur des TIC doit être attentif aux attentes légitimes de ses utilisateurs concernant le traitement des contenus en ligne. Les conditions d'utilisation des fournisseurs de services constituent un moyen approprié pour prendre en compte ces attentes.

Néanmoins, tous les fournisseurs de services de communication en ligne ne s'alignent pas sur les mêmes normes et lignes directrices pour formuler et mettre en application leurs conditions d'utilisation, même si le terrorisme, l'extrémisme violent et l'incitation à la violence sont généralement bannis de leurs plateformes[30]. Par conséquent, le secteur des TIC doit être encouragé à

[30] À cet égard, le fait que certains fournisseurs de services du secteur des TIC se réfèrent à des listes de sanctions différentes est considéré comme un problème. Par exemple, certains se réfèrent à la Liste récapitulative des sanctions du Conseil de sécurité des Nations Unies, tandis que d'autres se réfèrent uniquement à la liste des organisations et/ou groupes terroristes établies par un État. Par conséquent, les gouvernements sont encouragés à sensibiliser les parties prenantes concernées à la question des organisations et groupes considérés comme terroristes au plan international, en particulier au sein du secteur des TIC.

mettre en œuvre de manière collaborative et volontaire des lignes directrices cohérentes en matière de prévention et de lutte contre l'extrémisme violent et le terrorisme en ligne[31]. Dans ce contexte, les entreprises du secteur des TIC sont invitées à réexaminer et à adapter leurs conditions d'utilisation afin de prendre en compte la législation et les réglementations pertinentes, chaque fois que nécessaire. Il est rappelé à cet égard qu'il appartient au secteur des TIC de veiller au respect des droits de l'homme, conformément aux Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme ; il leur est donc recommandé de formuler leurs conditions d'utilisation dans une perspective respectueuse des droits de l'homme, c'est-à-dire d'éviter de formuler des lignes directrices sectorielles excessivement restrictives, qui pourraient inhiber l'entière jouissance des droits de l'homme des utilisateurs, en particulier le droit à la liberté d'expression et le droit d'exprimer une opinion sans subir d'ingérence[32].

Le secteur des TIC et plus particulièrement les prestataires de services de communication en ligne doivent appliquer strictement les conditions d'utilisation relatives au traitement des contenus en ligne afin d'en assurer la mise en œuvre efficace. Les fournisseurs de services numériques doivent veiller à ce que leurs conditions d'utilisation couvrent l'éventualité d'une introduction de contenus terroristes et qu'elles autorisent le retrait, le blocage, le filtrage de tous contenus mis en ligne en violation de leurs conditions d'utilisation, ou toute autre opération applicable, et ce dans un délai raisonnable. À cet égard, nombre de fournisseurs de services de communication en ligne donnent aux internautes la possibilité de signaler tout contenu en ligne constituant une violation des conditions d'utilisation. De ce fait, le secteur des TIC doit également veiller aux conséquences parfois indésirables que peut entraîner l'application des conditions d'utilisation, par exemple un impact potentiel sur la jouissance des droits de l'homme des utilisateurs, le risque d'empiéter sur des enquêtes judiciaires en cours, mais aussi veiller à ne pas exacerber le sentiment perçu d'injustice ni à renforcer une vision du monde exclusive de type « eux contre nous » qui peut indirectement servir les intérêts des extrémistes violents et des terroristes.

Bonne pratique n° 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.

Les procédures automatisées constituent un moyen efficace et efficient de traiter l'ampleur de l'environnement en ligne ainsi que la rapidité de la diffusion des contenus. Nombre de procédures automatisées permettent d'apporter un renfort aux opérations d'examen effectuées par l'homme et d'accélérer l'identification des contenus en ligne ; elles sont utilisées par les entreprises, mais aussi par d'autres acteurs de la détection se rapportant à la criminalité et aux atteintes en ligne, notamment les images à caractère pédophile et les violations du droit d'auteur.

L'automatisation peut être utilisée dans plusieurs domaines pour contribuer à lutter contre la dissémination de contenus en ligne existants et/ou précédemment identifiés comme étant à caractère extrémiste violent ou terroriste, en accélérant leur retrait. Par exemple, des initiatives telles que les bases de données de partage de hashtags créées par le secteur des TIC permettent de repérer la

---

[31] La Plateforme de partage de connaissances créée par la DECT de l'ONU avec le projet ICT4Peace recueillera l'ensemble des conditions d'utilisation appliquées actuellement ou exemplaires qui pourraient être reprises par les prestataires ; cette liste est disponible sur http:///www.techagainstterrorism.org.

[32] Voir par exemple : Commission européenne, *ICT Sector Guide on Implementing the Guiding Principles on Business and Human Rights* [Guide sectoriel des TIC pour la mise en œuvre des Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme], disponible sur https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/information_and_communication_technology_0.pdf

réitération de contenus précédemment examinés et retirés suite à une intervention humaine et d'empêcher que ces contenus réapparaissent sur d'autres plateformes en ligne, contribuant ainsi à prévenir de nouvelles disséminations de contenus existants et/ou déjà identifiés comme étant à caractère extrémiste violent[33].

Les gouvernements sont encouragés à soutenir les efforts déployés spontanément par les entreprises privées pour examiner et évaluer de manière continue et rigoureuse les résultats des procédures automatisées qu'elles appliquent, afin d'en vérifier l'efficacité et la pertinence et de s'assurer qu'elles ne génèrent pas de résultats inexacts ou susceptibles d'induire en erreur. Compte tenu de la rapidité des avancées technologiques dans ce domaine, il conviendra de soumettre les nouvelles procédures automatisées à un examen rigoureux afin de s'assurer qu'elles n'entraînent pas d'effet indésirable et qu'elles ne constituent pas une violation des droits relatifs à la liberté d'expression. À cette fin, il conviendra d'encourager le dialogue entre le secteur des TIC et les gouvernements concernant les procédures automatisées de retrait de contenus et leur compatibilité avec le droit à la liberté d'expression.

III. Bonnes pratiques relatives aux mesures fondées sur la communication.

Bonne pratique n° 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.

Afin de faire face à l'ensemble des contenus à caractère extrémiste violent et terroriste disponibles en ligne, il convient de prévoir une large palette de réponses en matière de communication, y compris des campagnes de prévention à visée pédagogique ou de dissémination de discours positifs destinées à un large public, des campagnes de contre-discours ciblant des publics davantage exposés au risque, et des interventions en ligne personnalisées visant spécifiquement les individus appartenant aux communautés liées à l'extrémisme violent et au terrorisme en ligne. La sécurité des individus menant à bien ces activités doit constituer une priorité absolue de l'action gouvernementale. Il est également crucial que les gouvernements communiquent efficacement sur les aspects de leurs politiques de sécurité nationale relatifs à la prévention et à la lutte contre l'extrémisme violent et le terrorisme, et que les communications en ligne sur le sujet s'ajoutent aux activités et communiqués hors ligne.

Les gouvernements pourraient envisager de concevoir leurs propres discours positifs et proactifs, visant non seulement à combattre directement ou à réfuter les récits extrémistes violents et terroristes, mais aussi à susciter un fort sentiment d'identité et d'appartenance et à encourager le sens civique, les principes d'inclusion et la responsabilisation, créant ainsi les conditions de la résilience au sein des sociétés concernées. Ces campagnes devraient s'efforcer de fournir des alternatives crédibles et d'aborder les sujets qui préoccupent les publics sensibles et les rendent vulnérables aux discours extrémistes violents et terroristes. Des formations aux compétences numériques et des cours de citoyenneté numérique pourraient être intégrés aux cursus d'éducation afin d'apporter une solution aux faiblesses sous-jacentes ou connues dans ce domaine. Ces programmes gagnent souvent en efficacité lorsqu'ils sont conçus et mis en œuvre en partenariat avec les organisations de la société civile. Il est important de veiller à la transparence de ce type de campagnes en ce qui concerne leur origine ou leur financement ; de même, leur conception doit être réaliste afin d'éviter d'exacerber le sentiment d'injustice souvent exploité par les groupes extrémistes violents et terroristes ; enfin, les campagnes de communication en ligne et hors ligne doivent être complémentaires.

---

[33] Commission européenne, Communiqué de Presse, Forum de l'UE sur l'internet : Un grand pas en avant dans la lutte pour l'enrayement des contenus à caractère terroriste sur l'internet, 8 décembre 2016, http://europa.eu/rapid/press-release_IP-16-4328_fr.htm.

Néanmoins, pour diverses raisons, les campagnes organisées directement par les gouvernements rencontrent parfois un succès limité dans la lutte contre les contenus à caractère extrémiste violent et terroriste en ligne. Les gouvernements sont donc encouragés à se rapprocher du secteur des TIC et des organisations pertinentes de la société civile afin de soutenir et de donner une marge de manœuvre à des communicants crédibles, s'exprimant sur une base volontaire, afin que ces voix soient entendues dans l'environnement en ligne et puissent diffuser des messages positifs alternatifs et nouer un dialogue avec les individus exprimant des opinions extrémistes violentes sur l'internet. Enfin, les organisations de la société civile peuvent contribuer aux travaux de recherche et d'analyse consacrés aux menaces et à l'impact des réponses qui leur sont apportées.

Bonne pratique n° 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.

Les gouvernements devraient encourager le secteur des TIC à être aussi proactif que possible dans la lutte contre l'extrémisme violent et le terrorisme sur ses plateformes de manière volontaire, afin de mieux protéger les internautes en soutenant les initiatives innovantes fondées sur la communication. La collaboration volontaire des grandes entreprises du secteur des TIC permet d'acquérir le rayonnement et d'avoir l'impact nécessaire pour lutter durablement et efficacement contre la menace posée par les communications en ligne à caractère extrémiste violent et terroriste.

Une approche pluri-acteurs requiert la participation de multiples intervenants du secteur des TIC, des organisations de la société civile et d'autres secteurs, agissant conformément à leurs rôles respectifs au sein de ces initiatives. Dans le secteur des TIC, les petites plateformes ont un rôle important à jouer, parallèlement aux analystes et aux spécialistes de la communication numérique, de la publicité, du marketing et de la création de contenus. Les chercheurs, les universitaires et les praticiens sont à même d'apporter un éclairage sur les communications à caractère extrémiste violent et terroriste et de réfléchir à des réponses potentielles, tandis que diverses organisations de la société civile peuvent donner la parole à des protagonistes authentiques et crédibles (dont des jeunes, des femmes, des membres des communautés ou groupes religieux, d'anciens extrémistes – éventuellement violents – ou terroristes, des survivants d'actes extrémistes et terroristes ou des figures publiques de grande notoriété) et veiller à ce que les réponses fondées sur la communication prennent en considération la dimension hommes-femmes ainsi que les préoccupations et les vulnérabilités spécifiques de chaque sexe.

Ces collaborations permettent de fédérer la créativité, l'expertise et les ressources et encouragent la mise en place de campagnes durables soutenues par des moyens de diffusion et d'évaluation efficaces. On peut citer à titre d'exemples d'initiatives innovantes la création d'ateliers d'initiation aux compétences numériques, de laboratoires de création de contenus destinés aux jeunes et de « hackathons » interactifs ainsi que la production de plateformes multimédia dédiées destinées aux collectifs de la société civile.

Bonne pratique n° 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 qu'elles proposent 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.

La réussite d'une campagne repose souvent sur la perception adéquate des meilleures plateformes et tactiques permettant d'atteindre le public cible. L'une des manières d'y parvenir est de faire appel à divers logiciels de veille sociale ou d'analyse des médias sociaux qui permettent aux équipes de communication d'identifier des porte-parole potentiels et de produire des contenus pertinents s'adressant à des publics cibles spécifiques. Ces activités doivent être conduites en tenant compte du contexte juridique de la campagne, notamment la législation sur la protection des données.

Ces outils s'avèrent particulièrement utiles lors des exercices de segmentation des publics dans la phase stratégique initiale d'une campagne. Leur utilisation apporte souvent un éclairage utile concernant les types de contenus et de discours susceptibles de trouver un écho et contribue à l'identification des porte-parole et des plateformes les plus efficaces pour relayer cette communication. Chaque fois que possible, il conviendra de consulter un échantillon représentatif du public cible pour examiner et réagir aux contenus proposés. En fonction de la portée de la campagne, il pourra s'agir, par exemple, de jeunes, de femmes, de chefs religieux ou d'anciens extrémistes – éventuellement violents – et terroristes.

Une fois la stratégie de la campagne définie et les premiers contenus diffusés, il conviendra d'assurer un suivi des performances de la campagne au moyen de logiciels d'analyse des médias sociaux. Cela peut apporter des informations sur la manière dont les contenus sont reçus en divers endroits du monde et par différentes populations. Ceci constitue le début d'un processus réitératif grâce auquel une campagne peut être optimisée et redéployée avec succès.

Bonne pratique n° 16 : S'assurer que chaque campagne a une finalité globale, qui peut être aussi simple que promouvoir le dialogue et la participation ; qu'elle vise un ensemble réaliste d'objectifs mesurables ; et qu'elle soit assortie d'une méthode d'évaluation robuste pour déterminer son impact sur les publics cibles.

Le fait de déterminer la finalité globale à long terme d'une campagne, tout en lui adjoignant un ensemble d'objectifs plus immédiats avant même la phase de conception et de dissémination, permet d'élaborer des balises permettant de mesurer son impact sur les publics cibles. Par conséquent, les objectifs doivent être formulés sous forme de mesures clairement définies et quantifiables d'un effet souhaité. Ils doivent aussi être mesurables afin que les responsables de la campagne puissent déterminer s'ils ont été atteints ou pas, en se basant sur les indicateurs et les mesures existantes, tout en étant réalistes au regard des ressources disponibles et des performances des campagnes antérieures.

Outre la poursuite d'une finalité et d'objectifs clairs, les campagnes doivent reposer sur une « théorie du changement » explicite et définir les moyens d'atteindre les objectifs fixés, d'obtenir l'impact désiré sur le public cible et d'élaborer des indicateurs pour déterminer si la finalité à long terme a été réalisée. Il conviendra, si possible, d'étayer l'élaboration des finalités et des objectifs ainsi que la théorie du changement choisie en recourant à une méthode axée sur les données.

Le suivi et l'évaluation continus des campagnes fondées sur la communication permettent de mettre en place un processus réitératif d'optimisation des contenus ou des vecteurs de communication et d'élargir la portée, la mobilisation et l'impact de ces mesures. Les gouvernements peuvent apporter leur aide en finançant des méthodes innovantes de collecte de données, d'analyse et de recherche, et en investissant dans un cadre commun de suivi et d'évaluation. Cela permettra de mieux connaître l'impact à long terme des mesures appliquées en ligne et d'adapter en conséquence les réponses ultérieures.

Bonne pratique n° 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.

Les mesures fondées sur les communications traitent inévitablement de sujets sensibles, ce qui peut entraîner un risque pour les publics cibles et les personnes faisant campagne et les rendre vulnérables, voire exposer les participants à des atteintes en ligne ou à des représailles physiques. Les risques spécifiques de sécurité à prendre en compte lors d'une campagne dépendent du type de campagne et d'autres facteurs comme le contexte dans lequel celle-ci s'inscrit. Il peut s'agir de risques de sécurité menaçant les organisations de la société civile ou les entreprises du secteur des TIC prenant part à la réalisation de la campagne. Toutefois, une planification et une mise en œuvre rigoureuses permettent d'atténuer efficacement ces risques.

Au-delà des problèmes de sécurité liés aux mesures fondées sur la communication, d'autres types de risques doivent être pris en compte. Les campagnes produisent une large palette d'impacts complexes, dont tous ne sont pas nécessairement positifs. Par exemple, diffuser involontairement au sein d'un public donné un message conçu pour un autre groupe spécifique peut se révéler attentatoire, induire un sentiment d'aliénation, voire renforcer une hostilité préalable. Les activités de suivi et d'évaluation présentent également des risques potentiels pour une campagne, par exemple lorsque des données d'utilisateur identifiables sont rendues publiques par inadvertance. Il est donc crucial de prendre en compte le contexte juridique dans lequel s'inscrit la campagne, y compris la législation sur la protection des données. Enfin, bien que nombre de mesures fondées sur la communication ne cherchent pas à entrer en contact avec les individus à haut risque de tomber dans l'extrémisme violent et le terrorisme, ni les membres actuellement actifs de groupes extrémistes violents et terroristes, toutes les campagnes devraient se doter de lignes directrices prévoyant la possibilité d'interactions avec ces individus.