UNODC
United Nations Office on Drugs and Crime

Utilisation de l'Internet
à des fins terroristes

En collaboration avec
L'ÉQUIPE SPÉCIALE DE LUTTE CONTRE LE TERRORISME
DE L'ORGANISATION DES NATION UNIES

OFFICE DES NATIONS UNIES CONTRE LA DROGUE ET LE CRIME
Vienne

UTILISATION D'INTERNET À DES FINS TERRORISTES

NATIONS UNIES
New York, 2014

Les appellations employées dans la présente publication et la présentation des données qui y figurent n'impliquent de la part du Secrétariat de l'Organisation des Nations Unies aucune prise de position quant au statut juridique des pays, territoires, villes ou zones ou de leurs autorités, ni quant au tracé de leurs frontières ou limites.

Les adresses et les liens vers des sites Internet mentionnés dans le présent document visent à faciliter la tâche du lecteur et sont exacts à la date de publication. L'Organisation des Nations Unies ne peut garantir qu'ils resteront valables dans l'avenir et décline toute responsabilité pour le contenu de sites Web externes.

Production éditoriale: Section des publications, de la bibliothèque et des services en anglais, Office des Nations Unies à Vienne.

"Le recours à l'Internet illustre bien la manière dont les terroristes peuvent adopter un mode opératoire réellement transnational. Pour y faire face, les États doivent eux aussi inscrire leur réflexion et leurs interventions dans un cadre transnational."

Ban Ki-moon
Secrétaire général de l'Organisation des Nations Unies

Avant-propos

Directeur exécutif
Office des Nations Unies contre la drogue et le crime

L'utilisation d'Internet à des fins terroristes est un phénomène en plein essor, qui exige des États Membres une réponse proactive et coordonnée.

L'Office des Nations Unies contre la drogue et le crime (ONUDC) joue un rôle majeur en matière d'assistance aux États Membres, dans le cadre de son mandat visant à renforcer la capacité des systèmes nationaux de justice pénale à appliquer les dispositions des instruments juridiques internationaux contre le terrorisme, et ce dans le respect des principes de l'état de droit et des normes internationales relatives aux droits de l'homme. En particulier, dans sa résolution 66/178 adoptée en 2011, l'Assemblée générale a prié l'ONUDC de continuer à développer des connaissances juridiques spécialisées sur les questions de lutte contre le terrorisme et les thèmes relevant de son mandat, notamment l'utilisation d'Internet à des fins terroristes.

Malgré une prise de conscience croissante à l'échelle internationale de la menace que constitue depuis quelques années l'utilisation d'Internet par des terroristes, il n'existe aucun instrument universel portant expressément sur cet aspect très répandu de leur activité. De surcroît, le nombre de formations spécialisées sur les aspects juridiques et pratiques des enquêtes et des poursuites relatives aux affaires de terrorisme impliquant l'utilisation d'Internet est limité. La présente publication vient compléter les documents déjà élaborés par l'ONUDC en matière de lutte contre le terrorisme, de cybercriminalité et d'état de droit. Elle traite également de l'importance de développer des connaissances intégrées et spécialisées pour répondre aux besoins d'assistance technique des États Membres dans leur lutte contre cette menace en constante évolution. L'ONUDC remercie vivement le Gouvernement du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, dont le généreux soutien a permis la publication de ce document.

La présente publication, destinée à la fois à être utilisée comme source d'information autonome et à soutenir les initiatives de renforcement des capacités de l'ONUDC, offre des conseils concernant les cadres juridiques et les pratiques en vigueur à l'échelle nationale et internationale en matière d'incrimination, d'enquêtes et de poursuites relatives aux affaires de terrorisme impliquant l'Internet.

Le terrorisme, dans toutes ses manifestations, nous concerne tous. L'utilisation d'Internet à des fins terroristes fait fi des frontières nationales, ce qui amplifie ses effets potentiels sur les victimes. En mettant en relief les exemples et les meilleures pratiques qui répondent à ce défi inédit, la présente publication poursuit deux objectifs: premièrement, mieux faire comprendre la façon dont les technologies de communication

peuvent être détournées dans le cadre d'actes de terrorisme et, deuxièmement, renforcer la collaboration entre les États Membres, pour qu'il soit possible d'élaborer des réponses de justice pénale efficaces à ce défi transnational.

Yury Fedotov
Directeur exécutif
Office des Nations Unies contre la drogue et le crime

Équipe spéciale de lutte contre le terrorisme du Secrétaire général

Le Groupe de travail sur la lutte contre l'utilisation d'Internet à des fins terroristes de l'Équipe spéciale de lutte contre le terrorisme a pour but d'assurer la coordination des activités du système des Nations Unies visant à soutenir la Stratégie antiterroriste mondiale, adoptée par l'Assemblée générale dans sa résolution 60/288. Dans cette résolution, les États Membres ont décidé "de coordonner les efforts aux échelles internationale et régionale afin de contrer le terrorisme sous toutes ses formes et dans toutes ses manifestations sur l'Internet" et "d'utiliser l'Internet comme un outil pour faire échec au terrorisme, tout en reconnaissant que les États pourront avoir besoin d'une assistance à cet égard". Le Groupe de travail a défini trois thèmes de discussion majeurs: les questions juridiques, les questions techniques et la manière dont la communauté internationale pourrait utiliser l'Internet avec davantage d'efficacité pour contrer le terrorisme en dénonçant le caractère fallacieux du message terroriste, qui prétend que la violence est un moyen légitime de parvenir à un changement politique.

La présente étude, produite par l'Office des Nations Unies contre la drogue et le crime et menée dans le cadre du Groupe de travail, doit beaucoup à la contribution et au soutien des États Membres. Elle fait progresser la discussion sur les défis juridiques rencontrés, et renforce de manière significative les connaissances et l'expertise accumulées par le Groupe de travail en la matière, et partagées avec les États Membres. En particulier, elle fournit des exemples importants de législations portant sur l'utilisation d'Internet par des terroristes et illustre, au travers d'affaires judiciaires réelles, les difficultés rencontrées par les États Membres pour incriminer et poursuivre de tels actes.

Le Groupe de travail est convaincu que le présent rapport contribuera à définir les domaines législatifs dans lesquels l'Organisation des Nations Unies peut aider les États Membres à appliquer la Stratégie antiterroriste mondiale pour combattre l'utilisation d'Internet à des fins terroristes.

Richard Barrett
Coordinateur de l'Équipe d'appui analytique et de surveillance des sanctions
Coprésident du Groupe de travail sur la lutte contre l'utilisation d'Internet à des fins terroristes de l'Équipe spéciale de lutte contre le terrorisme

Gouvernement du Royaume-Uni

Depuis 10 ans, le Royaume-Uni fait œuvre de pionnier en matière de législation contre l'utilisation d'Internet à des fins terroristes. Nous avons obtenu des succès considérables en la matière sur notre territoire, tout en nous efforçant de défendre les libertés et les avantages que l'Internet offre à nos citoyens.

Toutefois, nous reconnaissons que la menace est, de par sa nature même, transnationale. C'est seulement en agissant à l'unisson que la communauté internationale peut espérer lutter avec efficacité contre l'utilisation d'Internet par des terroristes.

Par conséquent, le Gouvernement britannique se réjouit de l'occasion qui lui est donnée d'apporter son soutien à la production par l'ONUDC de la publication que vous êtes sur le point de lire. Nous espérons qu'elle deviendra rapidement un outil qui permettra aux législateurs, aux agents des services de détection et de répression, et aux praticiens de la justice pénale d'élaborer et d'appliquer des cadres juridiques qui déstabiliseront efficacement les activités terroristes en ligne. Si tel est le cas, ce document contribuera à faire de nos communautés, réelles et virtuelles, des endroits plus sûrs.

Simon Shercliff
Chef du Département de lutte contre le terrorisme (opérations)
Ministère des affaires étrangères et du Commonwealth

Sue Hemming, Ordre de l'Empire britannique
Chef de la Division des infractions spéciales et de la lutte contre le terrorisme
Service des poursuites pénales du Royaume-Uni

Table des matières

Genèse de la présente publication

La technologie est l'un des facteurs stratégiques qui induit l'utilisation accrue d'Internet par des organisations terroristes et leurs sympathisants à de multiples fins, dont le recrutement, le financement, la propagande, l'entraînement, l'incitation à commettre des actes de terrorisme, la collecte et la diffusion d'informations. Internet présente évidemment de nombreux avantages, mais peut être utilisé pour faciliter la communication au sein d'organisations terroristes, pour transmettre des informations sur des actes de terrorisme planifiés et pour apporter un soutien matériel à ces actes. Des connaissances techniques spécifiques sont donc nécessaires pour enquêter avec efficacité sur ces infractions.

Il est généralement admis que, malgré l'atrocité de leurs actes, les terroristes présumés doivent bénéficier des mêmes garanties procédurales définies par le droit pénal que tout autre suspect. La défense des droits de l'homme est une valeur essentielle de l'Organisation des Nations Unies et un pilier fondamental de l'approche fondée sur l'état de droit de la lutte contre le terrorisme. Le présent document montre donc l'importance que revêt le respect des principes des droits de l'homme et des libertés fondamentales en toutes circonstances et, en particulier, dans le contexte de l'élaboration et de l'application d'instruments juridiques relatifs à la lutte contre le terrorisme.

L'Office des Nations Unies contre la drogue et le crime (ONUDC), entité clef des Nations Unies en matière d'assistance juridique et technique connexe dans la lutte contre le terrorisme, participe activement à l'Équipe spéciale de lutte contre le terrorisme, et veille ainsi à ce que ses activités de lutte antiterroriste soient menées dans le cadre plus large des efforts déployés à l'échelle du système des Nations Unies et en coordination avec ceux-ci. En janvier 2010, le Groupe de travail sur la lutte contre l'utilisation d'Internet à des fins terroristes de l'Équipe spéciale de lutte contre le terrorisme a organisé une série de conférences réunissant des représentants de gouvernements, d'organisations internationales et régionales, de groupes de réflexion, du monde universitaire et du secteur privé pour évaluer l'ampleur de cette utilisation et définir les moyens de s'y opposer. L'initiative du Groupe de travail visait à donner aux États Membres un aperçu de la nature actuelle du défi rencontré, et à proposer des lignes directrices en matière de politique à mener, des projets et des conseils pratiques concernant les aspects juridiques, techniques et de contre-communication de ce défi. Les conférences du Groupe de travail se sont tenues à Berlin (Allemagne) en janvier 2010, à Seattle (États-Unis d'Amérique) en février 2010 et à Riyad (Arabie saoudite) en janvier 2011.

Dans le cadre de sa mission consistant à "développer […] des connaissances juridiques spécialisées sur les questions de lutte contre le terrorisme […] afin de fournir aux États Membres qui en font la demande une assistance en ce qui concerne les mesures de

justice pénale contre le terrorisme, y compris […] l'utilisation d'Internet à des fins terroristes"[1], le Service de la prévention du terrorisme de l'ONUDC, en collaboration avec le Service de la criminalité organisée et du trafic illicite de l'ONUDC et avec le soutien du Gouvernement du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, s'est engagé à contribuer au projet du Groupe de travail en élaborant le présent outil d'assistance technique sur l'utilisation d'Internet à des fins terroristes. La présente publication de l'ONUDC s'appuie sur les conclusions des conférences du Groupe de travail, et en particulier de celle qui s'est tenue à Berlin en janvier 2010, se rapportant aux aspects juridiques du terrorisme spécifiques à Internet.

En relation avec l'élaboration de la présente publication, l'ONUDC a organisé en octobre 2011 et en février 2012 deux réunions de groupes d'experts à Vienne, qui visaient à offrir à des praticiens de la lutte contre le terrorisme issus d'États Membres géographiquement diversifiés un lieu où partager leurs expériences en matière d'utilisation d'Internet à des fins terroristes. Des experts de 25 États Membres y ont participé, notamment des procureurs, des agents des services de détection et de répression et des universitaires, ainsi que des représentants de plusieurs organisations intergouvernementales. La présente publication s'inspire fortement des discussions et de l'expertise partagées au cours de ces réunions, et a pour objet de fournir aux États Membres des conseils pratiques leur permettant d'accroître l'efficacité des enquêtes et des poursuites dans les affaires de terrorisme impliquant l'utilisation d'Internet.

[1] Résolution 66/178 de l'Assemblée générale.

I. Utilisation d'Internet à des fins terroristes

A. Introduction

1. Depuis la fin des années 80, l'Internet est devenu un moyen de communication extrêmement dynamique, qui touche un public de plus en plus large dans le monde entier. Le développement de technologies toujours plus sophistiquées a permis la création d'un réseau de portée réellement mondiale, dont l'accès est relativement aisé. La technologie d'Internet permet de communiquer au-delà des frontières dans un certain anonymat, avec rapidité et efficacité, à destination d'un public pratiquement illimité. Elle présente de nombreux avantages, à commencer par le fait qu'elle se prête tout particulièrement à la diffusion d'informations et d'idées, cet élément étant considéré comme un droit de l'homme fondamental[2]. Toutefois, il faut admettre que cette technologie, si elle facilite la communication, peut aussi être exploitée à des fins terroristes. Ce type d'utilisation crée à la fois des difficultés et des occasions à saisir dans la lutte contre le terrorisme.

B. Façons d'utiliser Internet à des fins terroristes

2. Dans le cadre de la présente publication, nous avons adopté une méthode fonctionnelle de classification des façons dont Internet est souvent utilisé pour promouvoir et soutenir les actes de terrorisme. Cette méthode nous a permis d'identifier six catégories qui se recoupent parfois: propagande (notamment recrutement, radicalisation et incitation au terrorisme), financement, entraînement, planification (notamment par le biais de communications secrètes et d'informations provenant de sources librement accessibles), exécution et cyberattaques. Nous aborderons chacune de ces catégories de manière plus détaillée ci-dessous.

1. Propagande

3. La diffusion de propagande représente l'une des principales utilisations d'Internet par les terroristes. Cette propagande se présente généralement sous forme de communications multimédias qui fournissent des instructions idéologiques ou pratiques pour la commission d'activités terroristes, ou encore expliquent, justifient ou promeuvent de telles activités. Ces éléments peuvent comprendre des messages virtuels, des présentations, des revues, des traités, des fichiers audio et vidéo, ainsi que des jeux vidéo élaborés

[2]Voir, par exemple, Pacte international relatif aux droits civils et politiques [résolution 2200 A (XXI) de l'Assemblée générale, annexe], art. 19, par. 2.

par les organisations terroristes ou leurs sympathisants. Néanmoins, la distinction entre la propagande terroriste et un plaidoyer légitime en faveur d'un point de vue repose souvent sur une évaluation subjective. En outre, la diffusion de propagande n'est généralement pas interdite en soi. L'un des principes de base du droit international est la protection des droits de l'homme fondamentaux, dont le droit à la liberté d'expression (voir discussion dans la section I.D ci-dessous). Ce principe garantit le droit d'une personne de partager une opinion ou de diffuser un contenu qui peut être considéré par autrui comme contestable, sous réserve d'exceptions limitées. Parmi les exclusions couramment acceptées figure l'interdiction de diffuser certaines catégories de contenus sexuellement explicites, cette interdiction étant réputée prise dans l'intérêt public afin de protéger certains groupes vulnérables. Parmi les autres exclusions, qui doivent être définies par la loi et dont la nécessité doit être prouvée, on peut citer les communications qui portent manifestement atteinte à la protection de la sécurité nationale ou qui ont pour objet et sont susceptibles d'inciter à commettre des actes de violence contre des personnes ou des groupes spécifiques[3].

4. La promotion de la violence est un thème courant de la propagande terroriste. Le rayonnement considérable des contenus diffusés sur Internet augmente de manière exponentielle le nombre de personnes affectées. En outre, la capacité de diffusion directe de contenus sur Internet rend leurs auteurs moins dépendants des canaux traditionnels de communication, tels les services de presse, qui pourraient prendre des mesures pour évaluer en toute indépendance la crédibilité des informations fournies ou pour modifier ou omettre les aspects jugés trop provocants. La propagande sur Internet comprend également des contenus tels que des séquences vidéo d'actes violents ou des jeux vidéo élaborés par des organisations terroristes, qui simulent des actes de terrorisme et encouragent l'utilisateur à endosser le rôle d'un terroriste virtuel.

5. La promotion de la rhétorique extrémiste encourageant les actes violents constitue également une tendance courante au sein de la gamme croissante de plates-formes Internet qui hébergent des contenus générés par les utilisateurs. Des contenus qui auraient été auparavant diffusés à un public relativement limité, personnellement ou par le biais de supports physiques tels que les disques compacts (CD) ou les disques vidéo numériques (DVD), migrent de plus en plus sur Internet. Ces contenus peuvent être diffusés à l'aide de toute une gamme d'outils, tels les sites Web dédiés, les forums de discussion virtuelle ciblés, les revues en ligne, les plates-formes de réseau social comme Twitter et Facebook, et les sites Web grand public de partage de vidéos et de fichiers, comme YouTube et Rapidshare. L'utilisation de services d'indexation tels que les moteurs de recherche Internet facilite également l'identification et l'extraction des contenus relatifs au terrorisme.

6. La menace fondamentale constituée par la propagande terroriste concerne la manière dont elle est utilisée et l'intention dans laquelle elle est diffusée. La propagande diffusée sur Internet vise tout un éventail d'objectifs et de publics. Elle peut être adaptée, entre autres, aux sympathisants ou opposants potentiels ou effectifs d'une organisation ou

[3] Ibid., art. 19, par. 3.

d'un courant extrémiste, aux victimes directes ou indirectes d'actes de terrorisme, à la communauté internationale ou à une partie de celle-ci. La propagande visant les sympathisants potentiels ou effectifs peut être axée sur le recrutement, la radicalisation et l'incitation au terrorisme, par le biais de messages véhiculant les notions de fierté, de réalisation et de dévouement à un objectif extrémiste. Elle peut aussi être utilisée pour prouver l'exécution d'attaques terroristes aux personnes qui les ont financées. Parmi les autres objectifs de la propagande terroriste, on peut citer le recours à la manipulation psychologique pour fragiliser la croyance d'une personne dans certaines valeurs sociales collectives, ou pour accroître le sentiment d'anxiété, de peur ou de panique au sein d'une population ou d'une partie de celle-ci. La diffusion de désinformation, de rumeurs, de menaces de violence ou d'images d'actes de violence provocants permet d'atteindre ces objectifs. Le public visé comprend les spectateurs directs de ces contenus, ainsi que les personnes touchées par la publicité potentielle en découlant. En ce qui concerne la communauté internationale au sens plus large, l'objectif est souvent de véhiculer un désir d'atteindre des objectifs politiques nobles[4].

a) Recrutement

7. Internet peut être utilisé non seulement pour publier de la rhétorique et des vidéos extrémistes, mais également pour créer des relations avec les personnes les plus réceptives à la propagande, et solliciter leur soutien. Les organisations terroristes ont de plus en plus recours à la propagande diffusée sur des plates-formes comme les sites Web protégés par mot de passe ou les groupes de discussion à accès restreint pour recruter clandestinement[5]. La portée d'Internet offre aux organisations terroristes et à leurs sympathisants un vivier mondial de recrues potentielles. Les cyberforums à accès restreint offrent à ces recrues un lieu où s'informer sur les organisations terroristes, leur apporter leur soutien et participer directement à des actions en vue d'objectifs terroristes[6]. L'utilisation de verrous technologiques à l'entrée des plates-formes de recrutement complique également la tâche du personnel des services de renseignement, de détection et de répression en matière de surveillance de l'activité terroriste.

8. La propagande terroriste est souvent conçue de façon à séduire les groupes vulnérables et marginalisés de la société. Le processus de recrutement et de radicalisation exploite généralement les sentiments d'injustice, d'exclusion ou d'humiliation[7]. La propagande est parfois adaptée pour tenir compte de facteurs démographiques, comme l'âge ou le sexe d'une personne, ainsi que de sa situation sociale ou économique.

[4]Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington, D.C., United States Institute of Peace Press, 2006), p. 37 et 38.

[5]Scott Gerwehr et Sarah Daly, "Al-Qaida: terrorist selection and recruitment", in *The McGraw-Hill Homeland Security Handbook*, David Kamien, éd. (New York, McGraw-Hill, 2006), p. 83.

[6]Dorothy E. Denning, "Terror's web: how the Internet is transforming terrorism", in *Handbook of Internet Crime*, Yvonne Jewkes et Majid Yar, éd. [Cullompton, Royaume-Uni, Willan Publishing (2010)], p. 194 à 213.

[7]Commission européenne, Groupe d'experts sur la radicalisation violente, "Radicalisation processes leading to acts of terrorism" (2008). Disponible à l'adresse: www.clingendael.nl/publications/2008/20080500_cscp_report_vries.pdf.

9. Internet peut être un outil particulièrement efficace de recrutement des mineurs, qui représentent une forte proportion de ses utilisateurs. La propagande diffusée sur Internet dans ce but prend parfois la forme de dessins animés, de vidéoclips ou de jeux électroniques attrayants. Les sites Web gérés par les organisations terroristes ou leurs partenaires ont recours à des tactiques qui combinent des dessins animés ou des contes pour enfants avec des messages qui soutiennent les actes de terrorisme, tels les attentats-suicides, et en font l'apologie. De même, certaines organisations terroristes ont conçu des jeux vidéo en ligne destinés à servir d'outils de recrutement et d'entraînement. Ces jeux prônent l'utilisation de la violence contre un État ou une personnalité politique en vue, en récompensant les succès virtuels, et sont parfois proposés en plusieurs langues pour attirer un large public[8].

b) Incitation

10. La propagande n'est généralement pas interdite en soi, mais de nombreux États Membres considèrent comme illégale son utilisation par des terroristes pour inciter autrui à commettre des actes de terrorisme. Internet offre une abondance de documents et de possibilités de télécharger, de modifier et de diffuser des contenus qui peuvent être considérés comme constituant une apologie illégale des actes de terrorisme ou une provocation à les commettre. Toutefois, il convient de noter que certains mécanismes intergouvernementaux et relatifs aux droits de l'homme ont exprimé des doutes quant au fait que le concept d'"apologie" du terrorisme était suffisamment étroit et précis pour servir de fondement à des sanctions pénales conformes aux exigences du principe de légalité et des limitations autorisées du droit à la liberté d'expression, tel que garanti par les articles 15 et 19 du Pacte international relatif aux droits civils et politiques[9,10].

11. Il importe de souligner la différence entre la simple propagande et les matériels destinés à inciter autrui à commettre des actes de terrorisme. Dans plusieurs États Membres, il est nécessaire, pour accuser quelqu'un d'incitation au terrorisme, de démontrer l'intention requise ainsi qu'un lien de causalité direct entre la propagande alléguée et un complot effectif ou l'exécution d'un acte terroriste. À titre d'exemple, dans une contribution présentée lors des réunions du groupe d'experts, un spécialiste français a indiqué que la diffusion de matériel didactique sur les explosifs ne constituait pas une violation du droit de son pays sauf si cette communication contenait des informations précisant que ce matériel était partagé dans un but terroriste.

12. La prévention et la dissuasion de l'incitation au terrorisme dans l'intérêt de la sauvegarde de la sécurité nationale et de l'ordre public constituent des motifs légitimes de limitation de la liberté d'expression, tels que visés au paragraphe 3 de l'article 19

[8] Gabriel Weimann, "Online terrorists prey on the vulnerable", *YaleGlobal Online*, 5 mars 2008. Disponible à l'adresse: http://yaleglobal.yale.edu/content/online-terrorists-prey-vulnerable.

[9] Résolution 2200 A (XXI) de l'Assemblée générale, annexe.

[10] Voir les rapports A/65/258 (par. 46) et A/61/267 (par. 7) du Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste; voir également le rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, additif, Déclaration commune marquant 10 années de collaboration: les 10 principaux obstacles à la liberté d'expression à surmonter au cours de la prochaine décennie (A/HRC/14/23/Add.2).

du Pacte international relatif aux droits civils et politiques. Ces motifs s'inscrivent également dans la logique du paragraphe 2 de l'article 20 de ce Pacte, qui impose aux États d'interdire tout appel à la haine nationale, raciale ou religieuse qui constitue une incitation à la discrimination, à l'hostilité ou à la violence. Toutefois, compte tenu du caractère fondamental du droit à la liberté d'expression, toute restriction à son exercice doit être à la fois nécessaire et proportionnelle à la menace. Le droit à la liberté d'expression est également lié à d'autres droits importants, dont les droits à la liberté de pensée, de conscience et de religion, de croyance et d'opinion[11].

c) Radicalisation

13. On peut considérer le recrutement, la radicalisation et l'incitation au terrorisme comme les éléments d'un processus. La radicalisation fait essentiellement référence à l'endoctrinement qui accompagne généralement la transformation de recrues en individus déterminés à commettre des actes de violence au nom d'idéologies extrémistes. Le processus de radicalisation implique souvent l'utilisation de propagande, personnellement ou sur Internet, pendant un certain temps. La durée et l'efficacité de la propagande et des autres moyens de persuasion employés varient en fonction de la situation et des relations individuelles.

2. Financement

14. Les organisations terroristes et leurs sympathisants ont parfois recours à Internet pour financer des actes de terrorisme. On peut classer les façons dont les terroristes utilisent Internet pour lever et collecter des fonds et des ressources en quatre catégories générales: sollicitation directe, commerce électronique, exploitation d'outils de paiement en ligne et organisations caritatives. La sollicitation directe désigne l'utilisation de sites Web ou de groupes de discussion et l'envoi massif de messages et de communications ciblées pour demander aux sympathisants de faire des dons. Les sites Web peuvent aussi faire office de magasins en ligne, et proposer des livres, des enregistrements audio ou vidéo et d'autres objets. Les moyens de paiement en ligne offerts par les sites Web ou les plates-formes de communication dédiés facilitent le transfert électronique de fonds entre les parties. Ces transferts interviennent souvent par virement électronique, carte de crédit ou autres moyens de paiement disponibles via des services comme PayPal ou Skype.

15. Les terroristes tirent également parti des moyens de paiement en ligne à la faveur de procédés frauduleux, tels que vol d'identité, vol de carte de crédit, fraude électronique, fraude en valeurs mobilières, infractions en matière de propriété intellectuelle et enchères frauduleuses. L'affaire *Royaume-Uni* c. *Younis Tsouli* (voir par. 114 ci-dessous) offre un exemple d'utilisation de gains illicites pour financer des actes de terrorisme. Les bénéfices issus de vols de cartes de crédit étaient blanchis par divers moyens, notamment le transfert via des comptes de paiement en ligne e-gold, qui permettait aux fonds de transiter par plusieurs pays avant d'atteindre leur destination. L'argent blanchi était utilisé à la fois pour financer l'enregistrement par M. Tsouli de 180 sites

[11] Haut-Commissariat des Nations Unies aux droits de l'homme, "Droits de l'homme, terrorisme et lutte antiterroriste", Fiche d'information n° 32 (Genève, 2008), chap. III, sect. H.

Web hébergeant des vidéos de propagande d'Al-Qaida et pour fournir des équipements destinés à des activités terroristes dans plusieurs pays. Environ 1 400 cartes de crédit ont ainsi été utilisées et ont généré près de 1,6 million de livres sterling de fonds illicites pour financer l'activité terroriste[12].

16. Le soutien financier apporté à des organisations apparemment légitimes, telles que les œuvres caritatives, peut aussi être détourné à des fins illicites. On sait que certaines organisations terroristes créent des sociétés écrans, camouflées en entreprises philanthropiques, pour solliciter des dons en ligne. Ces organisations prétendent soutenir des objectifs humanitaires alors qu'en fait elles utilisent les dons pour financer des actes de terrorisme. À titre d'exemple, on peut citer certaines entités aux noms inoffensifs telles que Benevolence International Foundation, Global Relief Foundation ou the Holy Land Foundation for Relief and Development, qui ont toutes utilisé des moyens frauduleux pour financer des organisations terroristes au Moyen-Orient. Il arrive également que les terroristes infiltrent certaines antennes d'organisations caritatives, qu'ils utilisent comme couverture pour promouvoir leur idéologie ou fournir un soutien matériel aux groupes militants[13].

3. Entraînement

17. Depuis quelques années, les organisations terroristes utilisent de plus en plus l'Internet comme terrain d'entraînement. Une gamme croissante de médias propose des plates-formes de diffusion de guides pratiques, présentés sous forme de manuels en ligne, de clips audio et vidéo, d'informations et de conseils. On trouve également sur ces plates-formes Internet des instructions détaillées, souvent en format multimédia facile d'accès et en plusieurs langues, sur des sujets tels que la manière de rejoindre des organisations terroristes, de fabriquer des explosifs, des armes à feu ou d'autres armes ou matières dangereuses, et de planifier et d'exécuter des attentats. Ces plates-formes servent de camp d'entraînement virtuel. Elles sont également utilisées pour partager, entre autres, certaines méthodes, techniques ou connaissances opérationnelles aux fins de commettre des actes de terrorisme.

18. Par exemple, *Inspire* est une revue en ligne prétendument publiée par Al-Qaida dans la péninsule arabique dans l'objectif déclaré de permettre aux musulmans de s'entraîner chez eux au djihad. Elle contient de nombreux documents idéologiques visant à encourager le terrorisme, notamment des déclarations attribuées à Oussama ben Laden, à Sheikh Ayman al-Zawahiri et à d'autres membres connus d'Al-Qaida. L'édition de l'automne 2010 comprenait du matériel didactique sur la manière d'adapter un véhicule à quatre roues motrices pour perpétrer un attentat contre des particuliers et sur la façon dont un individu isolé peut lancer une attaque au hasard en tirant des coups de feu à partir d'une tour. La publication suggérait même une ville cible, afin d'accroître les chances de tuer un membre du Gouvernement[14].

[12] Soumission écrite de l'expert du Royaume-Uni.

[13] Maura Conway, "Terrorist 'use' of the Internet and fighting back", *Information & Security*, vol. 19 (2006), p. 12 à 14.

[14] Soumission écrite de l'expert du Royaume-Uni.

19. Le matériel didactique disponible en ligne inclut des outils visant à faciliter les activités de contre-espionnage et de piratage, et à améliorer la sécurité des communications et de l'activité en ligne illicites à l'aide de dispositifs de cryptage et de techniques d'anonymisation. Le caractère interactif des plates-formes Internet contribue à créer un sentiment de communauté entre des personnes situées dans des lieux différents et issues de milieux divers, et encourage la création de réseaux d'échange de matériel didactique et tactique.

4. Planification

20. De nombreux praticiens de la justice pénale ont indiqué que quasiment toutes les affaires de terrorisme qui donnaient lieu à des poursuites judiciaires impliquaient l'utilisation de la technologie Internet. En particulier, la planification d'un acte de terrorisme requiert généralement des communications à distance entre plusieurs parties. Une affaire récemment jugée en France, *Ministère public* c. *Hicheur*[15], illustre la manière dont différentes formes de technologies Internet peuvent être utilisées pour faciliter la préparation d'actes de terrorisme, notamment via des communications détaillées au sein et entre des organisations prônant un extrémisme violent, ainsi qu'à travers les frontières.

Ministère public* c. *Hicheur

En mai 2012, un tribunal français a condamné Adlène Hicheur, ressortissant français né en Algérie, à une peine de cinq ans d'emprisonnement pour participation à une association de malfaiteurs en vue de la préparation d'un acte de terrorisme (en vertu des articles 421-1 et suivants du Code pénal français), relativement à des actes survenus en France en 2008 et 2009.

L'enquête visant Hicheur, un physicien nucléaire, a été ouverte début 2008 à propos d'un courrier électronique à contenu djihadiste, qui avait été envoyé sur le site Web du Président de la République française et provenait d'un membre d'Al-Qaida au Maghreb islamique (AQMI).

Une ordonnance conservatoire rendue en janvier 2009 a permis aux autorités d'identifier des courriers électroniques échangés entre le membre d'AQMI et, entre autres, le Global Islamic Media Front (GIMF) et le Rafidayin Center, un site Web ayant pour vocation déclarée d'héberger et de diffuser des documents, vidéos et enregistrements d'Al-Qaida, des déclarations de chefs de guerre et de kamikazes, ainsi que des documents d'autres groupes islamiques extrémistes. Ces courriers électroniques étaient cryptés à l'aide d'un logiciel dédié Asrar el Mojahedeen ou "Secrets des moudjahidin", qui inclut un cryptage 256 bits, divers algorithmes aléatoires que le programme peut modifier à chaque cryptage, des clés de chiffrement RSA 2 048 bits et un système de messagerie instantanée pris en charge par un forum de discussion crypté.

Des dizaines de courriers électroniques décryptés ont été produites au procès. L'accusation a soutenu que le contenu de ces messages indiquait que Hicheur avait, entre autres, commis les actes suivants au profit du réseau djihadiste, et notamment pour le compte du Rafidayin Center:

[15] Jugement du 4 mai 2012, affaire n° 0926639036 du tribunal de grande instance de Paris (14e chambre/2), Paris.

- Il avait traduit, crypté, compressé et protégé par mot de passe des documents prodjihadistes, notamment des textes et des vidéos, qu'il téléchargeait ensuite et faisait circuler sur Internet;
- Il avait diffusé le logiciel de cryptage Secrets des moudjahidin, pour faciliter les communications clandestines sur Internet;
- Il s'était associé à un membre d'AQMI pour organiser et coordonner des activités prodjihadistes, notamment en fournissant un soutien financier à la cause djihadiste, en diffusant des informations prodjihadistes et en appuyant la création d'une cellule opérationnelle en Europe, et en particulier en France, pour préparer d'éventuels attentats terroristes;
- Il avait agi comme modérateur du site Web prodjihadiste Ribaat;
- Il avait pris des mesures concrètes pour fournir un soutien financier à AQMI, y compris en tentant d'utiliser PayPal et d'autres systèmes de paiement virtuel.

Lors du procès, l'accusation a soutenu que ces communications prouvaient que Hicheur était parfaitement conscient du fait qu'il entamait un dialogue avec un membre d'AQMI, et qu'il avait agi sciemment et volontairement comme intermédiaire entre les combattants djihadistes et le GIMF. À la fin du procès, le tribunal a jugé qu'"Hicheur était devenu […] un soutien logistique et médiatique de cette structure terroriste pour laquelle le 'djihad médiatique' avait une grande importance".

Par ailleurs, le tribunal a jugé qu'"Adlène Hicheur, en donnant un tel accord pour l'élaboration d'une cellule opérationnelle rattachée à AQMI en Europe, voire en France, […] et en déterminant les cibles ou catégories de cibles à viser, a participé à un groupe [AQMI] formé en vue de la préparation d'actes de terrorisme".

Par conséquent, le tribunal a estimé que les preuves étaient suffisantes pour démontrer, comme l'exige le Code pénal français, que Hicheur avait fourni non seulement un soutien intellectuel mais aussi un soutien logistique direct à un plan terroriste clairement identifié. La décision du tribunal est susceptible d'appel.

Sources: jugement du 4 mai 2012 du tribunal de grande instance de Paris, et Tung, Liam, "Jihadists get world-class cryptage kit" (29 janvier 2008), disponible à l'adresse: www.zdnet.com.au/jihadists-get-world-class-cryptage-kit-339285480.htm.

21. Les terroristes peuvent également utiliser Internet pour identifier une cible potentielle d'attentat et les moyens les plus efficaces d'atteindre leurs objectifs. Ces mesures préparatoires vont de l'obtention d'instructions sur les méthodes d'attentat recommandées à la collecte d'informations provenant de sources librement accessibles et autres concernant une cible proposée. La capacité d'Internet à abolir les distances et les frontières, et la grande quantité d'informations accessibles au public dans le cyberespace, en fait un outil essentiel pour planifier les actes terroristes.

a) Communication secrète préparatoire

22. Internet a pour fonction première de faciliter la communication. Les terroristes sont de plus en plus rompus à l'utilisation des technologies pour communiquer anonymement à propos de la planification d'actes terroristes. Ils utilisent parfois un simple

compte de messagerie électronique pour créer une "boîte à lettres morte" électronique (ou virtuelle). Cette notion fait référence à la création d'un brouillon de message, qui n'est pas envoyé et qui laisse donc des traces minimes, mais auquel de nombreux individus en possession du mot de passe pertinent peuvent accéder à partir de n'importe quel terminal Internet dans le monde.

23. Il existe également une profusion de technologies sophistiquées qui rendent plus difficile l'identification de l'expéditeur, du destinataire ou du contenu des communications Internet. Des outils de cryptage et des logiciels d'anonymisation sont téléchargeables en ligne. Ces outils permettent, entre autres, de masquer l'adresse unique de protocole Internet (IP) qui identifie chaque ordinateur utilisé pour accéder à Internet ainsi que sa situation géographique, de réacheminer au moyen d'un ou de plusieurs serveurs les communications vers des pays qui répriment moins durement les activités terroristes ou de crypter les données relatives au trafic concernant les sites Web consultés. La stéganographie, qui consiste à dissimuler des messages dans des images, peut aussi être utilisée.

b) Informations accessibles au public

24. Les organisations et les particuliers publient des quantités d'informations considérables sur Internet. Dans le cas des organisations, cette tendance peut en partie résulter d'une volonté de promouvoir leurs activités et de simplifier leurs interactions avec le public. Certaines informations sensibles susceptibles d'être utilisées par des terroristes à des fins illicites sont également accessibles au moyen des moteurs de recherche Internet, qui sont capables de cataloguer et d'extraire les informations insuffisamment protégées de millions de sites Web. En outre, des informations logistiques détaillées accessibles en ligne, par exemple, des séquences en temps réel de télévision en circuit fermé, et des applications telles que Google Earth, qui sont destinées et principalement utilisées à des fins légitimes, peuvent être détournées par des personnes qui ont l'intention de tirer parti de l'accès gratuit aux images satellitaires à haute résolution, aux cartes et aux informations sur le relief et les bâtiments afin de reconnaître des cibles potentielles à partir d'un terminal à distance.

25. À l'ère des médias de réseau social grand public, tels que Facebook, Twitter, YouTube, Flickr ou les plates-formes de blogage, les particuliers publient également, volontairement ou par mégarde, une quantité sans précédent d'informations sensibles sur Internet. Ceux qui diffusent ces informations ont l'intention de fournir à leur public des nouvelles ou d'autres mises à jour dans un but informatif ou social, mais certaines de ces informations peuvent être détournées et utilisées au profit d'activités criminelles.

5. Exécution

26. Certains éléments des catégories décrites ci-dessus peuvent être employés pour exécuter des actes terroristes. À titre d'exemple, des menaces explicites de violence, relatives notamment à l'utilisation d'armes, sont parfois diffusées sur Internet pour provoquer de l'anxiété, de la peur ou de la panique au sein d'une population ou d'une

partie de celle-ci. Dans de nombreux États Membres, l'acte consistant à proférer des menaces, même si elles ne sont pas mises à exécution, peut être considéré comme une infraction. En Chine, par exemple, le fait d'inventer et/ou de diffuser une menace que l'on sait inventée relativement à l'utilisation de bombes ou de matières ou autres armes biologiques, chimiques ou radioactives, lorsqu'il a pour but de "porter gravement atteinte à l'ordre public", est érigé en infraction pénale par la législation interne[16]. Les communications Internet peuvent aussi être utilisées pour communiquer avec des victimes potentielles ou pour coordonner l'exécution d'actes physiques de terrorisme. À titre d'exemple, les auteurs des attentats du 11 septembre 2001 contre les États-Unis ont abondamment utilisé Internet à des fins de coordination.

27. L'utilisation d'Internet aux fins d'exécution d'actes de terrorisme offre des avantages logistiques, et permet de réduire la probabilité de détection ou de masquer l'identité des parties responsables. L'activité sur Internet peut aussi faciliter l'acquisition d'objets nécessaires à l'exécution de l'attentat. Les terroristes achètent parfois en ligne les articles ou services requis pour perpétrer des actes violents. Ils utilisent des cartes de crédit détournées ou d'autres formes de paiement électronique compromis pour financer ces achats.

6. Cyberattaques

28. Une cyberattaque désigne généralement l'exploitation délibérée de réseaux informatiques pour lancer une attaque. Elle vise généralement à perturber le fonctionnement des cibles, telles que les systèmes informatiques, les serveurs ou les infrastructures sous-jacentes, par le biais d'opérations de piratage, de techniques pointues de menace constante, de virus informatiques, de logiciels malveillants[17], de *phlooding*[18] ou d'autres moyens d'accès non autorisé ou malveillant. Les cyberattaques présentent parfois les caractéristiques d'un acte de terrorisme, notamment la volonté fondamentale de faire naître la peur à des fins politiques ou sociales. En janvier 2012, on a observé un exemple de cyberattaque en Israël: il consistait à cibler de multiples sites Web symboliques, par exemple ceux de la Bourse de Tel Aviv et de la compagnie aérienne nationale, et à divulguer de manière non autorisée les coordonnées de cartes de crédit et de comptes bancaires de milliers d'Israéliens[19]. Bien que la menace de cyberattaque par des terroristes fasse l'objet d'une attention considérable depuis quelques années, ce sujet sortirait du cadre de la présente publication et ne sera donc pas analysé.

[16] Soumission écrite de l'expert de la Chine.

[17] Conformément à la section 1 *n* du référentiel de législation contre la cybercriminalité de l'Union internationale des télécommunications, on peut définir un logiciel malveillant comme un programme qui est inséré dans un programme ou système informatique, généralement en secret, dans l'intention de compromettre la confidentialité, l'intégrité ou la disponibilité du programme, des données ou du système informatique.

[18] Le terme "*phlooding*" désigne le fait de cibler les serveurs centraux d'authentification d'une organisation par de multiples requêtes simultanées, dans le but de les surcharger, ce qui provoque un déni de service distribué.

[19] Voir Isabel Kershner, "Cyberattack exposes 20,000 Israeli credit card numbers and details about users", *New York Times*, 6 janvier 2012, et "2 Israeli web sites crippled as cyberwar escalates", *New York Times*, 16 janvier 2012.

C. Utilisations d'Internet pour contrer l'activité terroriste

29. Les terroristes ont élaboré de nombreuses façons d'utiliser l'Internet à des fins illicites, mais cette tendance offre également des possibilités de collecter des renseignements et de mener d'autres activités pour prévenir et contrer les actes de terrorisme, ainsi que de recueillir des preuves pour les poursuivre. De multiples connaissances concernant le fonctionnement, les activités et parfois les cibles des organisations terroristes proviennent de sites Web, de forums de discussion et d'autres communications sur Internet. Parallèlement, l'utilisation accrue d'Internet à des fins terroristes engendre une augmentation du nombre de données électroniques susceptibles d'être réunies et analysées à des fins antiterroristes. Les services de détection, de répression, de renseignement et autres élaborent des outils de plus en plus sophistiqués pour prévenir, détecter et décourager de manière proactive l'activité terroriste impliquant l'utilisation d'Internet. Le recours aux moyens d'enquête traditionnels, par exemple à des ressources de traduction spécialisées pour identifier d'éventuelles menaces en temps utile, se développe également.

30. Les discussions en ligne permettent de présenter des points de vue opposés ou d'engager un débat constructif, qui peut avoir pour effet de décourager d'éventuels sympathisants. Il est possible de transmettre des contre-communications reposant sur des faits avérés via des forums de discussion, des images et des vidéos en ligne. Pour être efficaces, les messages peuvent également faire preuve d'empathie à l'égard des problèmes sous-jacents qui contribuent à la radicalisation, telle la situation politique et sociale, et mettre en valeur d'autres options que les moyens violents pour atteindre les résultats souhaités[20]. On peut aussi opposer des communications stratégiques en plusieurs langues à la propagande terroriste sur Internet, pour atteindre un public géographiquement diversifié.

31. Le Center for Strategic Counterterrorism Communications, établi aux États-Unis, offre un exemple d'initiative interinstitutions récente visant à réduire la radicalisation et la violence extrémiste en identifiant en temps utile la propagande extrémiste, entre autres sur Internet, et en réagissant rapidement par des contre-communications ciblées à l'aide de tout un ensemble de technologies de communication, et notamment d'outils numériques[21]. Par exemple, il a été indiqué qu'en mai 2012 le Centre avait répondu dans les 48 heures à des bandeaux publicitaires promouvant la violence extrémiste diffusés par Al-Qaida dans la péninsule arabique sur divers sites Web, par des contre-publicités mises en ligne sur les mêmes sites et présentant une version modifiée du message, qui indiquait que les victimes des activités de l'organisation terroriste étaient des Yéménites. Cette campagne de contre-communication a nécessité une coopération entre le Département d'État américain, les services de renseignement et l'armée. Le

[20] Groupe de travail sur la lutte contre l'utilisation d'Internet à des fins terroristes de l'Équipe spéciale de lutte contre le terrorisme, document intitulé "Conference summary and follow-up/recommendations" de la Conférence sur l'utilisation d'Internet pour conjurer l'appel à la violence extrémiste, tenue à Riyad du 24 au 26 janvier 2011. Disponible à l'adresse: www.un.org/en/terrorism/ctitf/pdfs/ctitf_riyadh_conference_summary_recommendations.pdf.

[21] Décret 13584 du 9 septembre 2011, "Developing an Integrated Strategic Counterterrorism Communications Initiative and Establishing a Temporary Organization to Support Certain Government-wide Communications Activities Directed Abroad", *Federal Register*, vol. 76, n° 179, 15 septembre 2011.

Centre utilise également des plates-formes médias comme Facebook et YouTube pour diffuser des contre-communications[22,23].

D. Considérations concernant l'état de droit

32. Le respect des droits de l'homme et de l'état de droit fait partie intégrante de la lutte contre le terrorisme. Il convient de prendre toutes les précautions voulues pour respecter les normes internationales relatives aux droits de l'homme à toutes les étapes des initiatives de lutte contre le terrorisme, de la collecte préventive de renseignements à la garantie d'une procédure régulière lorsque des poursuites sont exercées contre un suspect. Cela nécessite l'élaboration d'une législation nationale et de pratiques qui défendent et protègent les droits fondamentaux de l'homme et l'état de droit[24].

33. Les États ont à la fois le droit et le devoir de mener une action efficace pour contrer les effets destructeurs du terrorisme sur les droits de l'homme, et en particulier sur les droits à la vie, à la liberté et à l'intégrité physique des personnes physiques et sur l'intégrité territoriale et la sécurité des États. Une action antiterroriste efficace et la protection des droits de l'homme sont des objectifs complémentaires et synergiques qui doivent être poursuivis ensemble[25]. Les initiatives antiterroristes relatives à l'utilisation d'Internet peuvent avoir des effets sur la jouissance de tout un éventail de droits de l'homme, notamment, le droit à la liberté d'expression, le droit à la liberté d'association, le droit à la vie privée et le droit à un procès équitable. Une analyse détaillée des questions relatives aux droits de l'homme sortirait du cadre de la présente publication, mais il est important de souligner les principaux domaines à prendre en compte.

34. Comme nous l'avons indiqué dans la sous-section B.1 *b* ci-dessus, l'interdiction de l'incitation au terrorisme peut engendrer des restrictions à la liberté d'expression. La liberté d'expression n'est pas un droit absolu. Elle peut être restreinte, sous réserve de respect de critères de légalité, de nécessité, de proportionnalité et de non-discrimination strictement interprétés, lorsque cette liberté est utilisée pour inciter à la discrimination, à l'hostilité ou à la violence. L'une des difficultés majeures dans les affaires d'apologie du terrorisme ou d'incitation au terrorisme concerne la détermination de la limite d'acceptabilité, celle-ci variant considérablement d'un pays à l'autre en fonction des différences d'histoires culturelles et juridiques[26]. De la même façon, le droit à la liberté d'association n'est pas un droit absolu, et il peut faire l'objet de limitations et de dérogations étroitement interprétées.

[22] Camille Elhassani, "United States State Department fights al-Qaeda in cyberspace", *Al Jazeera* (25 mai 2012). Disponible à l'adresse: http://blogs.aljazeera.com/americas/2012/05/25/us-state-department-fights-al-qaeda-cyberspace.

[23] Karen De Young et Ellen Nakoshima, "U.S. uses Yemeni web sites to counter al-Qaeda propaganda", *The Washington Post* (23 mai 2012). Disponible à l'adresse: www.washingtonpost.com/world/national-security/us-hacks-web-sites-of-al-qaeda-affiliate-in-yemen/2012/05/23/gJQAGnOxlU_story.html.

[24] Haut-Commissariat des Nations Unies aux droits de l'homme, Fiche d'information n° 32, chap. III, sect. H.

[25] Ibid., chap. I, sect. C.

[26] Organisation pour la sécurité et la coopération en Europe, Bureau des institutions démocratiques et des droits de l'homme, "Human rights considerations in combating incitement to terrorism and related offences", note d'information rédigée pour la réunion d'experts sur le thème "La prévention du terrorisme: la lutte contre l'incitation au terrorisme et contre les activités terroristes connexes", qui s'est tenue à Vienne les 19 et 20 octobre 2006, sect. 3 et 4.

35. La lutte contre l'utilisation d'Internet par des terroristes nécessite parfois des opérations de surveillance et de collecte d'informations sur les suspects. Il convient de veiller à protéger toute personne contre toute immixtion arbitraire ou illégale dans son droit à la vie privée[27], ce qui comprend le droit à la confidentialité des informations relatives à son identité ainsi qu'à sa vie privée. Les lois nationales doivent être suffisamment détaillées concernant, entre autres, les circonstances spécifiques dans lesquelles cette immixtion est autorisée. Des garanties appropriées doivent être également mises en place pour prévenir l'abus d'outils de surveillance secrète. En outre, les données à caractère personnel collectées doivent être protégées de manière adéquate pour empêcher tout accès ou toute divulgation ou utilisation illicite ou arbitraire[28].

36. Il est essentiel de garantir le droit à un procès équitable pour que les mesures de lutte contre le terrorisme soient efficaces et respectent l'état de droit. Les mesures de protection en matière de droits de l'homme accordées à toutes les personnes accusées d'infractions pénales, y compris en relation avec des actes de terrorisme, incluent le droit d'être présumé innocent, le droit de faire entendre sa cause conformément aux garanties d'une procédure régulière et dans un délai raisonnable par un tribunal compétent, indépendant et impartial ainsi que le droit de faire réexaminer la déclaration de culpabilité et la condamnation par une juridiction supérieure qui répond aux mêmes critères[29].

37. Pour une analyse plus détaillée des questions évoquées dans la présente section et d'autres considérations pertinentes, on peut consulter par exemple la Fiche d'information n° 32 du Haut-Commissariat des Nations Unies aux droits de l'homme intitulée "Droits de l'homme, terrorisme et lutte antiterroriste", le rapport de la Haut-Commissaire des Nations Unies aux droits de l'homme sur la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste (A/HRC/16/50), ainsi que les rapports intitulés "Dix pratiques optimales en matière de lutte antiterroriste" (A/HRC/16/51) et "Compilation de bonnes pratiques en matière de cadres et de mesures juridiques et institutionnels, notamment de contrôle, visant à garantir le respect des droits de l'homme par les services de renseignement dans la lutte antiterroriste" (A/HRC/14/46) du Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste.

[27]Voir Pacte international relatif aux droits civils et politiques, art. 17.

[28]"Droits de l'homme, terrorisme et lutte antiterroriste", chap. III, sect. J.

[29]Ibid., chap. III, sect. F.

II. Contexte international

A. Introduction

38. L'utilisation d'Internet par des terroristes est un problème transnational, qui nécessite une réponse intégrée entre les différents pays et systèmes nationaux de justice pénale. L'Organisation des Nations Unies joue un rôle central à cet égard, en facilitant la discussion et le partage des meilleures pratiques entre les États Membres, et en créant un consensus sur les méthodes communes de lutte contre l'utilisation d'Internet à des fins terroristes.

39. Diverses sources forment le cadre juridique international applicable en matière de lutte contre le terrorisme, dont des résolutions de l'Assemblée générale et du Conseil de sécurité, des traités, de la jurisprudence et du droit international coutumier. Les résolutions du Conseil de sécurité imposent des obligations juridiquement contraignantes aux États Membres ou fournissent des éléments de "droit souple" à l'origine d'engagements politiques ou de nouvelles normes de droit international. Les résolutions du Conseil de sécurité adoptées en vertu du Chapitre VII de la Charte des Nations Unies lient tous les États Membres. L'Assemblée générale a aussi adopté un certain nombre de résolutions concernant le terrorisme, qui sont des sources utiles de règles de "droit souple" et ont une haute importance politique bien qu'elles ne soient pas juridiquement contraignantes[30].

40. Des obligations juridiques s'imposent également aux États en vertu d'instruments bilatéraux et multilatéraux portant sur le terrorisme. Les instruments juridiques "universels" sont des accords qui sont ouverts à la ratification ou à l'adhésion de tout État Membre de l'Organisation des Nations Unies. En revanche, les accords promulgués par des groupes inter-États régionaux ou autres ne sont ouverts qu'à un nombre limité de signataires potentiels; les obligations fondées sur des traités ne lient que les États qui décident de devenir parties à ces accords.

41. L'obligation de traduire en justice les auteurs d'actes de terrorisme incombe principalement aux autorités nationales, car les tribunaux internationaux n'ont généralement pas compétence pour connaître de tels actes[31]. Les résolutions des Nations Unies, les instruments juridiques universels, les accords régionaux et les lois types contre le

[30]Voir Office des Nations Unies contre la drogue et le crime, *Questions les plus fréquemment posées sur les aspects du droit international touchant la lutte contre le terrorisme* (2009). Disponible à l'adresse: www.unodc.org/documents/terrorism/Publications/FAQ/French.pdf.

[31]Le Tribunal spécial pour le Liban, créé conformément à la résolution 1757 (2007) du Conseil de sécurité, est actuellement le seul tribunal international doté d'une compétence limitée concernant l'infraction de terrorisme.

terrorisme jouent un rôle déterminant dans l'établissement de normes communes acceptées dans plusieurs pays.

B. Résolutions des Nations Unies visant à lutter contre le terrorisme

42. La Stratégie antiterroriste mondiale des Nations Unies[32] a été adoptée à l'unanimité par l'Assemblée générale en 2006, et a marqué une étape importante en matière d'initiatives multilatérales de lutte contre le terrorisme. Conformément à cette Stratégie, les États Membres ont décidé, entre autres:

> *a*) De condamner systématiquement, sans équivoque et vigoureusement le terrorisme sous toutes ses formes et dans toutes ses manifestations, quels qu'en soient les auteurs, les lieux et les buts, car il constitue une des menaces les plus graves contre la paix et la sécurité internationales;
>
> *b*) D'agir d'urgence pour prévenir et combattre le terrorisme sous toutes ses formes et dans toutes ses manifestations;
>
> *c*) De reconnaître que la coopération internationale et toutes les mesures qu['ils] [prennent] pour prévenir et combattre le terrorisme doivent être conformes aux obligations que [leur] impose le droit international, notamment la Charte des Nations Unies et les conventions et protocoles internationaux pertinents, en particulier les instruments relatifs aux droits de l'homme, le droit des réfugiés et le droit international humanitaire;
>
> *d*) S'employer avec l'Organisation des Nations Unies, sans nuire à la confidentialité, dans le respect des droits de l'homme et conformément aux autres obligations prévues par le droit international, à explorer les moyens "*a) De coordonner les efforts aux échelles internationale et régionale afin de contrer le terrorisme sous toutes ses formes et dans toutes ses manifestations sur l'Internet; b) D'utiliser l'Internet comme un outil pour faire échec au terrorisme, tout en reconnaissant que les États pourront avoir besoin d'une assistance à cet égard*" [non souligné dans le texte].

43. Plusieurs résolutions du Conseil de sécurité adoptées ces dernières années exigent des États qu'ils coopèrent pleinement dans la lutte contre le terrorisme, sous toutes ses formes. En particulier, les résolutions 1373 (2001) et 1566 (2004), adoptées en vertu du Chapitre VII de la Charte des Nations Unies, requièrent que des mesures législatives et autres soient prises par tous les États Membres pour combattre le terrorisme, au moyen notamment d'une coopération accrue avec les autres gouvernements en matière de recherche, de détection, d'arrestation, d'extradition et de poursuite des personnes impliquées dans des actes terroristes, et exhortent les États à appliquer les conventions et protocoles internationaux relatifs au terrorisme.

44. La résolution 1624 (2005), qui porte sur l'incitation à commettre des actes terroristes et l'apologie de tels actes, constitue une autre résolution essentielle du Conseil

[32] Résolution 60/288 de l'Assemblée générale.

de sécurité relativement à l'activité terroriste susceptible d'être menée à l'aide d'Internet. Dans le quatrième paragraphe du préambule, le Conseil condamne "avec la plus grande fermeté l'incitation à commettre des actes terroristes" et récuse "toute tentative de justifier les actes terroristes ou d'en faire l'apologie, susceptible d'inciter à commettre de nouveaux actes de terrorisme". Dans le premier paragraphe, le Conseil 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 et prévenir une telle incitation.

45. De récents rapports et résolutions des Nations Unies ont expressément reconnu que le fait de contrer l'utilisation terroriste d'Internet constituait un élément essentiel d'une stratégie globale de lutte contre le terrorisme. Dans son rapport présenté en 2006 à l'Assemblée générale et intitulé "S'unir contre le terrorisme: recommandations pour une stratégie antiterroriste mondiale"[33], le Secrétaire général indiquait expressément ceci: "il est donc essentiel pour [les terroristes] de pouvoir générer et transférer des fonds, acquérir des armes, recruter et former des cadres et communiquer, en particulier via l'Internet"[34]. Le Secrétaire général affirmait ensuite que les terroristes se servaient de plus en plus de l'Internet pour recruter et pour diffuser des informations et de la propagande, et qu'il fallait contrer cette tendance par une action coordonnée entre les États Membres, tout en respectant les droits de l'homme et les autres obligations au regard du droit international[35].

46. Dans sa résolution 1963 (2010), le Conseil de sécurité s'est dit "préoccupé par le fait que les terroristes utilisent de plus en plus souvent, dans une société mondialisée, les nouvelles technologies de l'information et de la communication, en particulier Internet, pour recruter et convaincre, ainsi que pour financer, planifier et préparer leurs actes". Le Conseil a également reconnu l'importance de la coopération entre les États Membres pour empêcher les terroristes d'exploiter la technologie, les moyens de communication et les autres ressources.

C. Instruments juridiques universels de lutte contre le terrorisme

47. Depuis 1963, la communauté internationale élabore des instruments juridiques universels visant à prévenir les actes terroristes sous les auspices de l'Organisation des Nations Unies et de ses institutions spécialisées, en particulier l'Organisation de l'aviation civile internationale, l'Organisation maritime internationale et l'Agence internationale de l'énergie atomique. Ces instruments universels constituent un élément essentiel du régime antiterroriste mondial et un cadre important pour la coopération internationale en matière de lutte contre le terrorisme. Ils recouvrent des actes allant du détournement d'aéronefs aux actes de terrorisme nucléaire commis par des individus

[33] A/60/825.

[34] Ibid., par. 38.

[35] Ibid., par. 58 et 60.

ou des groupes[36], et font obligation aux États qui les adoptent de réprimer la plupart des actes de terrorisme prévisibles dans les domaines couverts par les conventions. Néanmoins, ces instruments juridiques universels ne lient juridiquement que leurs signataires[37], qui sont également tenus d'appliquer leurs dispositions via leur système national de justice pénale.

48. Grâce à l'attention portée à la lutte contre le terrorisme après la résolution 1373 (2001) du Conseil de sécurité, dans laquelle le Conseil appelait les États Membres à devenir parties aux instruments juridiques universels s'y rapportant, le taux d'adhésion a considérablement augmenté. En juin 2011, les deux tiers des États Membres avaient ratifié au moins 10 des 16 instruments juridiques universels de lutte contre le terrorisme ou y avaient adhéré[38].

49. Actuellement, il n'existe pas de traité global des Nations Unies qui soit applicable à une liste exhaustive de manifestations de terrorisme. De même, la communauté internationale ne s'est pas encore mise d'accord sur une définition internationalement contraignante du terme "terrorisme"[39], en raison principalement de la difficulté de concevoir une classification juridique universellement acceptable des actes de violence commis par des États, par des groupes armés tels que les mouvements de libération ou d'autodétermination ou par des particuliers.

50. Les États Membres mènent depuis 2000 des négociations relatives à une convention générale de lutte contre le terrorisme, qui engloberait enfin une définition du terrorisme. Cependant, face à la difficulté de parvenir à un consensus sur une définition unique et mondialement acceptée, l'avancée est intervenue par le biais d'instruments juridiques universels en vigueur, qui se sont développés dans certains secteurs. Ces instruments portent sur l'incrimination d'"actes terroristes" spécifiques sans définir le concept plus large de terrorisme.

51. Les instruments mondiaux ne définissent pas les infractions terroristes comme crimes relevant du droit international. En revanche, ils font obligation aux États parties de criminaliser les actes illégaux spécifiés conformément à leur législation nationale, d'exercer leur compétence à l'égard des délinquants dans certaines conditions prescrites et de promouvoir la coopération internationale afin de pouvoir poursuivre ou extrader les délinquants présumés. Jusqu'à l'aboutissement des négociations concernant une

[36] Les autres actes de terrorisme couverts sont notamment les suivants: sabotage d'aéronefs, actes de violence dans les aéroports, actes contre la sécurité de la navigation maritime, actes contre la sécurité des plates-formes fixes situées sur le plateau continental, infractions contre des personnes jouissant d'une protection internationale (par exemple enlèvement de diplomates), obtention et possession illicites de matières nucléaires, prise d'otages, attentats terroristes à l'explosif et financement d'actes de terrorisme ou d'organisations terroristes.

[37] Pour obtenir un état du statut de ratification de ces instruments juridiques universels, veuillez consulter: www.unodc.org/tldb/universal_instruments_NEW.html.

[38] Voir www.un.org/fr/sc/ctc/laws.html.

[39] Cependant, il importe de noter que dans une décision récente, le Tribunal spécial pour le Liban a jugé qu'il existait suffisamment de preuves pour soutenir l'existence d'une définition du crime de terrorisme en vertu du droit international coutumier. Voir Décision préjudicielle sur le droit applicable: terrorisme, complot, homicide, commission, concours de qualifications, affaire n° STL-11-01/I, Tribunal spécial pour le Liban (16 février 2011); disponible à l'adresse: www.stl-tsl.org/en/the-cases/stl-11-01/rule-176bis/filings/orders-and-decisions/appeals-chamber/interlocutory-decision-on-the-applicable-law-terrorism-conspiracy-homicide-perpetration-cumulative-charging.

définition universelle ou une convention générale relative au terrorisme, les accords bilatéraux et multilatéraux devraient fournir la base d'élaboration de normes communes pour contrer l'utilisation d'Internet à des fins terroristes, en vue de promouvoir la coopération internationale.

52. Aucune convention universelle n'a été adoptée concernant expressément la prévention et la répression de l'utilisation d'Internet par des terroristes. En décembre 2010, l'Assemblée générale a adopté la résolution 65/230, dans laquelle elle a, entre autres, approuvé la Déclaration de Salvador sur des stratégies globales pour faire face aux défis mondiaux: les systèmes de prévention du crime et de justice pénale et leur évolution dans un monde en mutation[40], et prié la Commission pour la prévention du crime et la justice pénale de créer, conformément à la Déclaration de Salvador, un groupe intergouvernemental d'experts à composition non limitée chargé de faire une étude exhaustive du phénomène de la cybercriminalité et des mesures prises par les États Membres, la communauté internationale et le secteur privé pour y faire face, et notamment l'échange d'informations sur les législations nationales, les meilleures pratiques, l'assistance technique et la coopération internationale. Les résultats de cette étude, qui a été lancée par l'ONUDC en février 2012, faciliteront l'évaluation des effets de l'utilisation des nouvelles technologies de l'information aux fins d'activités criminelles, et notamment de l'Internet, dans le domaine par exemple des infractions d'incitation au terrorisme et de financement du terrorisme liées à l'informatique.

D. Droit international des droits de l'homme

53. Les obligations en matière de droits de l'homme font partie intégrante du cadre juridique international de lutte contre le terrorisme, tant par l'obligation qu'ont les États de prévenir les attaques terroristes, lesquelles peuvent fragiliser considérablement les droits de l'homme, que par l'obligation qu'ils ont de veiller à ce que cette lutte ne porte pas atteinte aux droits de l'homme. Dans la Stratégie antiterroriste mondiale des Nations Unies, les États Membres ont réaffirmé ces obligations, en reconnaissant en particulier "qu'une action efficace contre le terrorisme et la protection des droits de l'homme sont des objectifs non pas contradictoires mais complémentaires et synergiques".

54. Les principaux instruments universels relatifs aux droits de l'homme et adoptés sous les auspices de l'Organisation des Nations Unies sont notamment la Déclaration universelle des droits de l'homme[41], le Pacte international relatif aux droits civils et politiques, le Pacte international relatif aux droits économiques, sociaux et culturels[42], et les protocoles applicables.

[40] Adoptée par le douzième Congrès des Nations Unies pour la prévention du crime et la justice pénale, tenu du 12 au 19 avril 2010 à Salvador (Brésil), qui portait, entre autres, sur la nécessité pour les États Membres d'examiner les manières de lutter contre les nouvelles formes de criminalité, notamment la cybercriminalité.

[41] Résolution 217 A (III) de l'Assemblée générale.

[42] Résolution 2200 A (XXI) de l'Assemblée générale, annexe.

55. Plusieurs organisations régionales ont également élaboré des conventions garantissant les droits de l'homme. On peut notamment citer la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales[43] (1950), la Convention américaine relative aux droits de l'homme[44] (1969), la Charte africaine des droits de l'homme et des peuples[45] (1981) et la Charte des droits fondamentaux de l'Union européenne[46] (2000).

56. Une analyse globale des questions relatives au droit des droits de l'homme sortirait du cadre de la présente publication; néanmoins, les considérations concernant l'état de droit et les instruments juridiques applicables seront abordées à propos des mesures spécifiques de lutte contre le terrorisme lorsque le contexte l'exigera[47].

E. Instruments juridiques régionaux et sous-régionaux de lutte contre le terrorisme

57. Outre les instruments universels de lutte contre le terrorisme, plusieurs instruments régionaux et sous-régionaux offrent des normes de fond et de procédure extrêmement utiles pour ériger en infractions pénales les actes de terrorisme perpétrés au moyen de l'Internet. Ces instruments, qui complètent les instruments universels de lutte contre le terrorisme, ont une portée et un degré d'applicabilité variables.

1. Conseil de l'Europe

58. En 2001, le Conseil de l'Europe a élaboré la Convention du Conseil de l'Europe sur la cybercriminalité[48], qui est actuellement le seul instrument multilatéral juridiquement contraignant portant sur l'activité criminelle menée via l'Internet. Cette convention tente d'harmoniser les lois nationales relatives à la cybercriminalité, d'améliorer les procédures nationales de détection, d'enquête et de poursuite concernant ces infractions et de prévoir des arrangements permettant une coopération internationale rapide et fiable sur ces questions[49]. La Convention établit une norme commune minimale applicable aux infractions nationales liées à l'informatique[50] et prévoit l'incrimination de neuf de ces infractions, notamment celles qui se rapportent à l'accès non autorisé aux systèmes, programmes ou données et à leur altération illicite, à la fraude et à la falsification informatiques, ainsi qu'à la tentative de commettre ces actes et à la complicité en vue de leur perpétration[51].

[43] Conseil de l'Europe, *Série des traités européens*, n° 5.

[44] Organisation des Nations Unies, *Recueil des Traités*, vol. 1144, n° 17955.

[45] Ibid., vol. 1520, n° 26363.

[46] *Journal officiel des Communautés européennes*, C 364, 18 décembre 2000.

[47] Voir aussi Office des Nations Unies contre la drogue et le crime, *Questions les plus fréquemment posées sur les aspects du droit international touchant la lutte contre le terrorisme*, sect. V.

[48] Conseil de l'Europe, *Série des traités européens*, n° 185 (également disponible à l'adresse: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/default_FR.asp).

[49] Ibid., préambule.

[50] Rapport explicatif sur la Convention du Conseil de l'Europe sur la cybercriminalité, par. 33. Disponible à l'adresse: http://conventions.coe.int/Treaty/FR/Reports/Html/185.htm.

[51] Ibid., art. 2 à 8 et 11.

59. La Convention du Conseil de l'Europe sur la cybercriminalité comprend également d'importantes dispositions de procédure, susceptibles de faciliter les enquêtes et la collecte de preuves relativement aux actes de terrorisme impliquant l'utilisation d'Internet. Ces dispositions s'appliquent à toute infraction pénale commise au moyen d'un ordinateur et au recueil de preuves se présentant sous forme électronique, et sont soumises aux garanties prévues par le droit interne[52].

60. À titre d'exemple, la Convention du Conseil de l'Europe sur la cybercriminalité exige des parties qu'elles adoptent une législation contraignant les fournisseurs d'accès à l'Internet (FAI) à conserver les données spécifiées stockées sur leurs serveurs durant une période pouvant atteindre 90 jours[53] (renouvelable), si les agents des services de détection et de répression en font la demande dans le cadre d'une enquête criminelle ou d'une procédure pénale, jusqu'à ce que les mesures appropriées puissent être prises pour imposer la divulgation de ces données[54]. Cette procédure accélérée de conservation des données stockées est essentielle compte tenu de la nature éphémère des données électroniques et du délai nécessaire à l'aboutissement des procédures traditionnelles d'entraide judiciaire dans les affaires transnationales[55]. Le prononcé d'une injonction ordonnant de conserver des données, ou toute mesure similaire, présente également plusieurs avantages par rapport aux procédures traditionnelles de perquisition et de saisie, puisque le FAI est parfois mieux placé pour sécuriser rapidement les preuves en question. En outre, une mesure de conservation est moins susceptible de perturber son activité légitime et de porter atteinte à sa réputation[56], ce qui peut faciliter une coopération suivie. La procédure de recherche et de saisie des données stockées, établie conformément à l'article 19 de la Convention du Conseil de l'Europe sur la cybercriminalité, prévoit des mesures de protection de ces données qui sont similaires à celles généralement accordées aux preuves matérielles[57] en vertu de la législation nationale pertinente[58].

61. La Convention du Conseil de l'Europe sur la cybercriminalité impose également aux parties d'appliquer la législation portant sur la production de données relatives aux abonnés stockées[59]. Ces informations peuvent être essentielles pendant la phase d'enquête pour établir l'identité de l'auteur d'un acte terroriste impliquant l'utilisation d'Internet, et peuvent comprendre l'endroit où se trouve cette personne, ainsi que

[52] Ibid., art. 14, par. 2 *b* et *c*, et art. 15. Ces conditions comprendront la protection adéquate des droits de l'homme et des libertés, en particulier des droits établis conformément aux obligations souscrites en application de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et du Pacte international relatif aux droits civils et politiques, ou d'autres instruments internationaux applicables en matière de droits de l'homme, à toute supervision judiciaire ou autre forme de supervision indépendante.

[53] Un minimum de 60 jours est imposé concernant la conservation de données en réponse à une demande d'entraide judiciaire (Convention du Conseil de l'Europe sur la cybercriminalité, art. 29).

[54] Convention du Conseil de l'Europe sur la cybercriminalité, art. 16.

[55] Rapport explicatif sur la Convention du Conseil de l'Europe sur la cybercriminalité, par. 157.

[56] Ibid., par. 155.

[57] Par exemple, le support sur lequel les données sont conservées.

[58] Rapport explicatif sur la Convention du Conseil de l'Europe sur la cybercriminalité, par. 184.

[59] Voir Convention du Conseil de l'Europe sur la cybercriminalité, art. 18. L'expression "données relatives aux abonnés" désigne toute information, autre que des données relatives au trafic ou au contenu, se rapportant à l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, ou toute autre information relative à l'endroit où se trouvent les équipements de communication disponibles sur la base d'un contrat conclu avec le prestataire de services.

d'autres services connexes à la communication employés pour commettre cet acte. La Convention exige également des États signataires qu'ils établissent des normes minimales pour permettre la collecte en temps réel de données relatives au trafic[60] associées à des communications spécifiées, ainsi que l'interception de données relatives au contenu concernant certaines infractions graves spécifiées en vertu du droit national[61].

62. Il est possible d'appliquer la Convention du Conseil de l'Europe sur la cybercriminalité de manière conjointe avec les instruments de lutte contre le terrorisme, telle la Convention du Conseil de l'Europe pour la prévention du terrorisme[62], pour fournir un fondement juridique à la coopération contre l'utilisation d'Internet à des fins terroristes. La Convention du Conseil de l'Europe pour la prévention du terrorisme impose aux parties d'incriminer certains actes en vertu du droit national qui pourraient conduire à la commission d'infractions terroristes, tels que la provocation publique, le recrutement et l'entraînement, tous ces actes pouvant être commis au moyen d'Internet. La Convention rend également obligatoire l'adoption de mesures de coopération nationale et internationale visant à prévenir le terrorisme, notamment des mesures d'enquête. À titre d'exemple, l'article 22 de la Convention prévoit le partage avec une autre partie d'informations non sollicitées relatives à l'enquête ou à la procédure, dans les limites imposées par le droit national, dans le but commun de réagir aux actes criminels (informations spontanées).

63. La Convention du Conseil de l'Europe sur la cybercriminalité et la Convention du Conseil de l'Europe pour la prévention du terrorisme sont ouvertes à la ratification ou à l'adhésion de tous les États membres du Conseil de l'Europe[63], des États non membres ayant participé à leur élaboration et d'autres États non membres par invitation, avec l'accord de tous les États alors parties à la Convention pertinente[64]. Il convient de noter que plusieurs pays qui n'ont pas officiellement adhéré à la Convention du Conseil de l'Europe sur la cybercriminalité ont néanmoins utilisé ses dispositions comme lignes directrices lors de la rédaction de leur législation interne sur la cybercriminalité. (Voir également la section F ci-dessous sur la loi type.)

64. Le Conseil de l'Europe a également élaboré le Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et

[60] Conformément à l'article 1 *d* de la Convention du Conseil de l'Europe sur la cybercriminalité, les "données relatives au trafic" incluent les informations qui indiquent l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée d'une communication ou le type de service sous-jacent.

[61] Conformément aux articles 20 et 21, respectivement, de la Convention du Conseil de l'Europe sur la cybercriminalité.

[62] Conseil de l'Europe, *Série des traités européens*, n° 196. Également disponible à l'adresse: http://conventions.coe.int/Treaty/fr/treaties/html/196.htm.

[63] À la date de la présente publication, les 47 États membres du Conseil de l'Europe sont les suivants: Albanie, Allemagne, Andorre, Arménie, Autriche, Azerbaïdjan, Belgique, Bosnie-Herzégovine, Bulgarie, Chypre, Croatie, Danemark, Espagne, Estonie, ex-République de Macédoine, Fédération de Russie, Finlande, France, Géorgie, Grèce, Hongrie, Irlande, Islande, Italie, Lettonie, Liechtenstein, Lituanie, Luxembourg, Malte, Monaco, Monténégro, Norvège, Pays-Bas, Pologne, Portugal, République de Moldova, République tchèque, Roumanie, Royaume-Uni, Saint-Marin, Serbie, Slovaquie, Slovénie, Suède, Suisse, Turquie, Ukraine.

[64] Voir Convention du Conseil de l'Europe sur la cybercriminalité, art. 36, et Convention du Conseil de l'Europe pour la prévention du terrorisme, art. 23 et 24.

xénophobe commis par le biais de systèmes informatiques[65]. Ce Protocole additionnel peut également faciliter la poursuite d'actes terroristes commis via l'Internet avec l'intention d'inciter à la violence en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique, ou de la religion[66]. Il est ouvert à tous les États contractants de la Convention du Conseil de l'Europe sur la cybercriminalité[67].

2. Union européenne

65. Le Conseil de l'Union européenne a adopté la décision-cadre 2002/475/JAI du 13 juin 2002 relative à la lutte contre le terrorisme, qui harmonise la définition des infractions terroristes dans tous les États membres de l'Union européenne[68] en adoptant une définition spécifique et commune du concept de "terrorisme", en énonçant des règles de compétence juridictionnelle visant à garantir que les infractions terroristes soient poursuivies avec efficacité et en présentant des mesures concernant les victimes d'infractions terroristes. En réaction à la menace terroriste croissante, et notamment à l'utilisation de nouvelles technologies telles que l'Internet, la décision-cadre 2002/475/JAI a été modifiée en 2008[69] pour inclure expressément des dispositions relatives à l'incitation publique à commettre une infraction terroriste, au recrutement et à l'entraînement pour le terrorisme. Dans cette décision, le Conseil de l'Union européenne a également pris acte de la résolution 1624 (2005) du Conseil de sécurité, dans laquelle ce dernier appelait les États à prendre des mesures visant à interdire par la loi l'incitation à commettre des actes terroristes et à prévenir de tels comportements.

66. La décision-cadre 2008/919/JAI permet de poursuivre la diffusion de propagande terroriste et l'expertise en matière de fabrication d'explosifs par le biais d'Internet, dans la mesure où cette diffusion est commise intentionnellement et remplit les critères des infractions nommées. Les modifications apportées à la décision-cadre 2002/475/JAI relatives aux infractions d'incitation publique, de recrutement et d'entraînement se sont appuyées sur des dispositions similaires de la Convention du Conseil de l'Europe pour la prévention du terrorisme[70]. La décision-cadre 2008/919/JAI a créé de nouvelles infractions relatives aux conduites susceptibles de mener à des actes de terrorisme, quels que soient les moyens ou les outils technologiques utilisés pour commettre ces infractions. Comme celles de la Convention du Conseil de l'Europe pour la prévention du terrorisme, les dispositions de la décision-cadre 2008/919/JAI ne sont pas spécifiques à Internet, mais elles couvrent également les activités menées par ce biais.

[65] Conseil de l'Europe, *Série des traités européens*, n° 189.

[66] Ibid., art. 2.

[67] Ibid., art. 11.

[68] À la date de la présente publication, les 27 États membres de l'Union européenne sont les suivants: Allemagne, Autriche, Belgique, Bulgarie, Chypre, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Pays-Bas, Pologne, Portugal, République tchèque, Roumanie, Royaume-Uni, Slovaquie, Slovénie, Suède.

[69] Décision-cadre 2008/919/JAI du Conseil de l'Union européenne du 28 novembre 2008 modifiant la décision-cadre 2002/475/JAI relative à la lutte contre le terrorisme.

[70] Conseil des ministres, "Amendment of the Framework Decision on combating terrorism", communiqué de presse du 18 avril 2008.

3. Autres instruments juridiques

67. Parmi les autres instruments juridiques contraignants adoptés par les organisations régionales ou sous-régionales et contenant des dispositions applicables à la lutte contre l'utilisation d'Internet par des terroristes, on peut citer les textes suivants:

- Convention régionale sur la répression du terrorisme de l'Association sud-asiatique de coopération régionale (1987);
- Convention arabe sur la répression du terrorisme (1998);
- Traité de coopération entre les États membres de la Communauté d'États indépendants dans la lutte contre le terrorisme (1999);
- Convention de l'Organisation de la Conférence islamique pour combattre le terrorisme international (1999);
- Convention de l'Organisation de l'unité africaine sur la prévention et la lutte contre le terrorisme (1999);
- Convention interaméricaine contre le terrorisme (2002);
- Convention de l'Association des nations de l'Asie du Sud-Est sur la lutte contre le terrorisme (2007);
- Directive portant sur la lutte contre la cybercriminalité de la Communauté économique des États de l'Afrique de l'Ouest (2009).

F. Lois types

68. Si les lois types définissent des lignes directrices consultatives, et non des obligations juridiquement contraignantes, elles n'en jouent pas moins un rôle important dans l'harmonisation des normes juridiques entre les États. Contrairement aux conventions internationales, qui font parfois l'objet de longues négociations pour refléter les besoins de tout un ensemble de signataires potentiels, les lois types offrent aux États de solides dispositions juridiques, qui peuvent servir de point de départ à l'élaboration de la législation nationale. L'un des principaux avantages de l'utilisation de dispositions types comme fondement d'une législation nationale est qu'elle facilite la coopération internationale, en atténuant notamment les conflits découlant d'une mauvaise interprétation des dispositions dans les différents systèmes juridiques (par exemple, entre les pays de *common law* et ceux de droit romano-germanique) et concernant les exigences de double incrimination[71]. (Voir discussion à la section V.F.5 ci-dessous.)

1. Commonwealth

69. La loi type sur la criminalité informatique et liée à l'informatique (2002) du Commonwealth a été rédigée sur la base de la Convention du Conseil de l'Europe sur la

[71] Conformément au principe de double incrimination, l'extradition n'est possible que dans le cas où l'acte sur le fondement duquel l'extradition a été demandée est passible de sanctions à la fois dans l'État requérant et dans l'État requis.

cybercriminalité[72]. Cette loi type vise à tirer parti des similitudes de traditions juridiques entre les États membres du Commonwealth[73] pour favoriser l'harmonisation des aspects matériels et procéduraux de la lutte contre la cybercriminalité, et pour promouvoir la coopération internationale. La loi type du Commonwealth s'inscrit dans la ligne des normes définies par la Convention du Conseil de l'Europe sur la cybercriminalité.

2. Communauté d'États indépendants

70. Les États membres de la Communauté d'États indépendants (CEI) ont également adopté des actes législatifs types et des lignes directrices, visant à harmoniser les systèmes législatifs nationaux et prenant en compte les expériences internationales en matière de lutte contre le terrorisme. Ces dispositions types reflètent les normes juridiques internationales, adaptées aux besoins des États membres de la CEI[74]. Par exemple, l'article 13 de la loi type portant sur le cadre réglementaire de l'Internet[75] prévoit des dispositions types concernant la lutte contre l'utilisation d'Internet à des fins illégales.

3. Union internationale des télécommunications

71. L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies, qui joue un rôle prépondérant dans les questions de cybercriminalité. L'UIT a élaboré le référentiel de législation contre la cybercriminalité (2010) afin de promouvoir l'adoption d'une législation nationale et de règles procédurales harmonisées sur la cybercriminalité, concernant notamment les actes de terrorisme commis à l'aide d'Internet. Le référentiel a été élaboré à partir d'une analyse globale de la Convention du Conseil de l'Europe sur la cybercriminalité et de la législation des pays développés en la matière[76]. Le référentiel de l'UIT aborde principalement les questions de cybersécurité, mais il prévoit des dispositions types relatives à l'incrimination de certains actes de terrorisme impliquant l'utilisation d'Internet, tels que l'accès non autorisé à des programmes ou des données informatiques aux fins de terrorisme ou la transmission de logiciels malveillants dans l'intention de favoriser le terrorisme[77].

---

[72] Pour de plus amples informations, voir www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf.

[73] À la date de la présente publication, les 53 États membres du Commonwealth étaient les suivants: Afrique du Sud, Antigua-et-Barbuda, Australie, Bahamas, Bangladesh, Barbade, Belize, Botswana, Brunéi Darussalam, Cameroun, Canada, Chypre, Dominique, Gambie, Ghana, Grenade, Guyana, Iles Salomon, Inde, Jamaïque, Kenya, Kiribati, Lesotho, Malaisie, Malawi, Maldives, Malte, Maurice, Mozambique, Namibie, Nauru, Nigéria, Nouvelle-Zélande, Ouganda, Pakistan, Papouasie-Nouvelle-Guinée, République-Unie de Tanzanie, Royaume-Uni, Rwanda, Sainte-Lucie, Saint-Kitts-et-Nevis, Saint-Vincent-et-les Grenadines, Samoa, Seychelles, Sierra Leone, Singapour, Sri Lanka, Swaziland, Tonga, Trinité-et-Tobago, Tuvalu, Vanuatu, Zambie.

[74] À la date de la présente publication, les 11 États membres de la Communauté d'États indépendants étaient les suivants: Arménie, Azerbaïdjan, Bélarus, Fédération de Russie, Kazakhstan, Kirghizistan, Ouzbékistan, République de Moldova, Tadjikistan, Turkménistan, Ukraine.

[75] Annexe à la résolution 36-9 de l'Assemblée interparlementaire des membres de la Communauté d'États indépendants, adoptée le 16 mai 2011.

[76] Union internationale des télécommunications, référentiel de législation contre la cybercriminalité (2010), par. 2.2.

[77] Ibid., sect. 3 *f* et 6 *h*.

III. Cadres politiques et législatifs

A. Introduction

72. Les terroristes utilisent l'Internet pour planifier et financer leurs actes, mais également pour recruter et former de nouveaux membres, communiquer, rechercher ou reconnaître d'éventuelles cibles, diffuser de la propagande et inciter autrui à commettre des actes de terrorisme.

73. Dans le présent chapitre, nous aborderons les questions relatives à l'élaboration de politiques et de législations en matière de justice pénale pour contrer ces menaces, de manière à déterminer, en nous référant aux expériences et aux exemples exposés par certains États représentés aux réunions du groupe d'experts, les difficultés et les approches communes susceptibles soit de compromettre soit de renforcer l'efficacité des enquêtes et des poursuites dans les affaires de terrorisme impliquant une quelconque utilisation d'Internet.

B. Politiques

74. Pour apporter des réponses de justice pénale efficaces aux menaces présentées par les terroristes utilisant l'Internet, les États ont besoin de cadres politiques et législatifs clairs. De façon générale, ces politiques et ces lois doivent privilégier les points suivants:

a) Incrimination des actes illégaux commis par des terroristes sur Internet ou à l'aide de services connexes;

b) Octroi de pouvoirs d'investigation aux services de détection et de répression chargés de mener les enquêtes liées au terrorisme;

c) Réglementation des services connexes à Internet (par exemple, FAI) et contrôle des contenus;

d) Facilitation de la coopération internationale;

e) Mise au point de procédures spécialisées en matière judiciaire ou probatoire;

f) Respect des normes internationales relatives aux droits de l'homme.

1. Approches politiques

75. Dans sa publication de 2011, intitulée "*Countering the Use of the Internet for Terrorist Purposes: Legal and Technical Aspects*"[78], le Groupe de travail sur la lutte contre l'utilisation d'Internet à des fins terroristes de l'Équipe spéciale de lutte contre le terrorisme a défini trois approches stratégiques globales permettant aux États de contrer les activités terroristes Internet, à savoir grâce à:

a) Une législation générale sur la cybercriminalité;

b) Une législation générale (non spécifique à l'Internet) sur la lutte contre le terrorisme;

c) Une législation spécifique à l'Internet sur la lutte contre le terrorisme.

76. On note que dans la première approche *a)*, il est possible d'utiliser, en sus d'une législation générale sur la cybercriminalité, d'autres infractions pénales inchoatives comme l'incitation ou l'association de malfaiteurs, pour traiter les affaires de terrorisme impliquant une quelconque utilisation d'Internet, et en particulier les actes présumés visant à inciter autrui à commettre des actes de terrorisme.

77. Le système de classification globale du Groupe de travail fournit un cadre conceptuel utile aux dirigeants et aux législateurs lorsqu'ils examinent les approches politiques et législatives adaptées à leurs États.

78. Le document intitulé "*Countering the Use of the Internet for Terrorist Purposes*"[79] mentionne une autre ressource utile aux dirigeants et aux législateurs: le référentiel pour une législation contre la cybercriminalité (Toolkit for Cybercrime Legislation), élaboré sous les auspices de l'UIT. En sus d'autres dispositions pénales types, le référentiel prévoit plusieurs infractions spécifiques liées au terrorisme, notamment dans sa section 3 *f*, qui traite de l'accès non autorisé aux programmes informatiques, ou de l'acquisition de tels programmes, aux fins d'élaborer, de formuler, de planifier, de faciliter des actes de terrorisme, d'aider à la commission de tels actes, de s'associer pour les commettre ou de les commettre.

79. Au sein du cadre général fourni par les instruments universels de lutte contre le terrorisme et les normes internationales pertinentes en matière de droits de l'homme, les gouvernements disposent d'une grande latitude pour privilégier telle ou telle approche; inévitablement, celle-ci varie selon les États. Le présent chapitre ne fait qu'exposer des exemples de méthodes adoptées par certains États, qui pourraient être utiles aux dirigeants et aux législateurs.

80. Actuellement, peu d'États ont élaboré une législation de lutte contre le terrorisme visant expressément l'utilisation d'Internet, mais quelques-uns l'ont fait, dont le

[78] Voir Nations Unies, Équipe spéciale de lutte contre le terrorisme, Groupe de travail sur la lutte contre l'utilisation d'Internet à des fins terroristes, *Countering the Use of the Internet for Terrorist Purposes: Legal and Technical Aspects* (New York, 2011).

[79] Ibid., par. 20.

Royaume-Uni. Après les attentats de Londres en 2005, le Gouvernement a adopté la loi de 2006 intitulée *Terrorism Act* (loi contre le terrorisme), dont la première partie comprend des dispositions traitant expressément des activités menées sur Internet qui sont susceptibles d'encourager ou de faciliter la commission d'actes de terrorisme. Cette loi complète la loi de 1990 intitulée *Computer Misuse Act* (loi contre l'utilisation abusive d'ordinateurs), qui porte sur la criminalité informatique et la cybercriminalité de manière plus générale.

81. En 2007, les Émirats arabes unis ont adopté plusieurs lois fédérales qui, outre le piratage et d'autres activités liées à Internet, incriminent la création de sites Web ou la publication d'informations destinés à des groupes terroristes sous un faux nom, dans l'intention de faciliter le contact avec les responsables de ces groupes ou de promouvoir leur idéologie, de financer leurs activités ou de publier des informations relatives à la manière de fabriquer des explosifs ou d'autres substances pour les utiliser lors d'attaques terroristes[80].

82. En 2008, le Gouvernement saoudien a mis en œuvre de nouvelles lois relatives aux technologies, et notamment un texte érigeant en infraction pénale passible d'amende et d'une peine d'emprisonnement pouvant aller jusqu'à 10 ans, le fait de posséder un site Web prônant ou soutenant le terrorisme[81].

83. La même année, le Gouvernement pakistanais a édicté une ordonnance intitulée *Prevention of Electronic Crimes Ordinance* (Ordonnance sur la prévention des infractions électroniques), qui créait une disposition spécifique relative aux infractions liées au cyberterrorisme. Toutefois, ce texte n'est plus en vigueur[82].

84. Enfin, toujours en 2008, le Gouvernement indien a modifié la loi de 2000 intitulée *Information Technology Act* (loi sur les technologies de l'information), pour prévoir l'infraction de "cyberterrorisme" (art. 66F) et traiter d'autres questions relatives à Internet.

85. Néanmoins, en l'absence d'instrument universel imposant l'obligation expresse d'adopter une législation visant expressément l'activité terroriste sur Internet, les gouvernements ont, à l'échelle internationale et à quelques exceptions près, retenu une approche mixte pour faire face à ces menaces, en faisant appel à une combinaison de lois pénales générales et de législation relative à la cybercriminalité et à la lutte contre le terrorisme. Dans certains États, par exemple, les lois pénales se concentrent sur les actes criminels matériels sans faire de distinction entre les moyens utilisés pour les commettre. Dans cette optique, l'Internet est considéré comme un simple outil à l'aide duquel les terroristes ont commis une infraction matérielle, souvent prévue par les dispositions du Code pénal national.

[80] Loi fédérale n° 2 de 2006 sur la prévention des infractions relatives aux technologies de l'information, *Official Gazette of the United Arab Emirates*, vol. 442, 36e année, Muharam 1427 H/janvier 2006 (traduction anglaise non officielle disponible à l'adresse: www.aecert.ae/pdfs/Prevention_of_Information_Technology_Crimes_English.pdf).

[81] David Westley, "Saudi tightens grip on Internet use", *Arabian Business*, 26 janvier 2008.

[82] "Pakistan lacks laws to combat cyber terrorism", *The New New Internet*, disponible à l'adresse: www.thenewnew-Internet.com/2010/09/01/pakistan-lacks-laws-to-combat-cyber-terrorism.

86. C'est l'approche retenue en Chine, où la loi pénale contient un article portant sur l'incrimination de toutes les activités illégales impliquant l'utilisation d'Internet. L'article 287 de la loi pénale confère le caractère d'infraction au fait d'utiliser un ordinateur pour commettre une infraction, qui sera poursuivie et punie conformément aux dispositions applicables de cette loi relatives à l'incrimination et à la détermination de la peine. Ainsi, en vertu de la loi pénale chinoise, l'utilisation d'Internet est considérée comme un moyen de commettre un acte criminel ou un outil permettant de le faire, et non comme un élément constitutif indépendant de l'infraction. Cette utilisation est par conséquent incriminée dans les dispositions de fond de cette loi.

87. Dans le contexte du terrorisme, la Chine a adopté des dispositions afférentes à diverses formes d'activités terroristes, dont l'article 120 de la loi pénale qui incrimine les activités relatives au fait d'organiser, de mener et de participer à des organisations terroristes. Cette disposition globale recouvre un large éventail d'activités liées au terrorisme, dont celles qui sont commises sur Internet.

88. En République de Corée, deux types de lois pénales peuvent s'appliquer aux actes terroristes impliquant l'utilisation d'Internet. L'une est le Code pénal général et l'autre est un Code pénal spécial adopté en 1986, relatif aux actes criminels concernant l'information et la communication. L'article 90 de ce Code pénal porte sur la préparation de tels actes, ainsi que sur l'entente criminelle, l'incitation ou la propagande et prévoit que quiconque prépare les infractions visées à l'article 87 du Code pénal (émeutes, révoltes ou troubles publics) ou à l'article 88 (homicides commis aux fins des actes visés par l'article 87), ou complote en vue de commettre de telles infractions, est passible d'une peine de prison d'au moins trois ans. En vertu de l'article 101 du Code pénal, quiconque prépare ou se rend complice des infractions visées aux articles 92 à 99 du Code pénal commet une infraction et est passible d'une peine de prison d'au moins deux ans. L'article 114 du Code pénal se rapporte à l'organisation d'un groupe criminel. Toujours en vertu du Code pénal spécial, le Gouvernement a établi un éventail d'infractions pénales incriminant expressément les actes illégaux visant les réseaux d'information et de communication et les informations à caractère personnel.

89. En pratique, l'expérience montre que, quelle que soit l'optique retenue, la plupart des États adoptent une approche multidimensionnelle des enquêtes et des poursuites concernant les affaires de terrorisme, notamment celles qui impliquent l'utilisation d'Internet. Les services de détection et de répression ainsi que les organismes chargés des poursuites utilisent les dispositions législatives les plus adaptées aux circonstances, quelles qu'elles soient.

90. Les pouvoirs dont les services de détection et de répression ont besoin pour enquêter avec efficacité sur les affaires de terrorisme sont à peu près semblables dans tous les pays, les différences constatées en matière de politiques et de législations nationales reflétant la diversité des systèmes juridiques, des dispositifs constitutionnels et d'autres facteurs (par exemple, culturels).

91. Dans le domaine de la réglementation de l'Internet et du contrôle des contenus, les approches nationales sont extrêmement diverses. La Déclaration universelle des

droits de l'homme et le Pacte international relatif aux droits civils et politiques offrent des normes internationales se rapportant à la réglementation de l'expression et de la communication d'idées, mais aucun instrument global internationalement contraignant ne définit de normes définitives et impératives concernant ce qui est considéré comme un contenu Internet approprié ou la manière dont chaque État devrait réglementer l'activité Internet sur son territoire. Actuellement, la pornographie enfantine est la seule activité interdite par tous les États, alors même qu'il n'existe pas de définition ou d'instrument universellement contraignant[83]. Dans le contexte du terrorisme, en revanche, l'absence de définition universellement acceptée constitue un obstacle à toute approche internationalement convenue de la réglementation appropriée de l'activité liée au terrorisme et des contenus Internet.

92. En matière de procédures judiciaires ou probatoires spécialisées, certains États ont adopté des processus judiciaires et de gestion des instances spécifiques, susceptibles de s'appliquer aux affaires impliquant l'utilisation d'Internet par des terroristes. Lorsque cette méthode est retenue, il importe que ces mécanismes spécialisés soient pleinement conformes aux obligations internationales pertinentes en matière de droits de l'homme, notamment à celles qui se rapportent au droit à la liberté et à un procès équitable.

C. Législation

1. Incrimination

93. Comme nous l'avons précédemment indiqué, aucun instrument universel contre le terrorisme ne contraint les États à adopter une législation visant expressément l'utilisation d'Internet par les terroristes. Par conséquent, s'il est très probable que la plupart des affaires de terrorisme impliquent l'utilisation d'Internet par les auteurs d'infractions, les autorités de nombreux États s'appuieront vraisemblablement sur les dispositions relatives aux actes illégaux figurant dans les instruments universels, mais également sur les dispositions concernant d'autres infractions pénales définies dans leur Code pénal, et notamment les infractions inchoatives comme l'entente criminelle, l'incitation et l'association de malfaiteurs, pour poursuivre les délinquants.

94. Dans la présente section, nous examinerons les dispositions législatives adoptées par certains États, en vue de déterminer les approches permettant d'apporter des réponses de justice pénale efficaces aux différents types d'actes.

a) Actes ou déclarations sur Internet soutenant le terrorisme

95. Indépendamment des actes associés à la commission d'actes terroristes matériels (par exemple, attentats à l'explosif), il est manifeste que les terroristes utilisent de plus en plus l'Internet pour mener des actions de soutien comme le recrutement et l'entraînement de membres, le partage d'informations utiles, la diffusion de propagande et

[83] Maura Conway, "Terrorism and Internet governance: core issues", *Disarmament Forum*, vol. 3 (2007), p. 27.

l'incitation à commettre des actes de terrorisme. En raison de la configuration et de la portée mondiale de l'Internet, il est de plus en plus probable que ces activités fassent intervenir différents acteurs, physiquement présents dans divers pays.

96. Au Royaume-Uni, la partie VI de la loi de 2000 intitulée *Terrorism Act* (loi contre le terrorisme) prévoit plusieurs infractions sur lesquelles se fonder pour mettre en accusation les individus qui ont utilisé l'Internet pour soutenir des activités terroristes.

97. L'article 54 de cette loi confère le caractère d'infraction au fait de fournir, de recevoir ou d'inviter autrui à recevoir des instructions ou un entraînement en matière de fabrication ou d'utilisation d'armes à feu, de matière radioactive ou d'armes connexes, d'explosifs ou d'armes chimiques, biologiques ou nucléaires.

98. L'article 57 érige en infraction pénale la possession d'objets dans des circonstances qui permettent raisonnablement de penser que la personne possède ces objets en relation avec la préparation d'un acte de terrorisme, l'incitation à un acte terroriste ou la commission d'un tel acte. Ces dernières années, cette infraction a été utilisée avec succès pour poursuivre plusieurs individus qui avaient été trouvés en possession d'objets aussi divers que des disques durs, des DVD et des documents didactiques sur la manière de fabriquer ou de faire fonctionner des éléments tels que des mortiers, des gilets-suicides ou du napalm[84]. Pour qu'une telle infraction soit considérée comme commise, le ministère public doit prouver l'existence d'un lien entre l'objet en question et un acte de terrorisme donné. Plusieurs délinquants ont été poursuivis avec succès au titre des infractions définies par l'article 57; cependant, les tribunaux ont adopté une approche plus restrictive dans l'interprétation du champ d'application de cet article, comme le montre l'affaire *R.* c. *Zafar, Butt, Iqbal, Raja et Malik* [2008] EWCA Crim 184.

R.* c. *Zafar, Butt, Iqbal, Raja et Malik

Survenue au Royaume-Uni en 2007, cette affaire concernait les appels interjetés avec succès par Zafar, Butt, Iqbal, Raja et Malik contre les condamnations prononcées à leur encontre pour possession d'objets dans un but lié à la commission d'un acte de terrorisme, à sa préparation ou à l'incitation à sa commission, en violation de l'article 57 de la loi britannique de 2000 contre le terrorisme.

Sur ces cinq personnes, quatre étaient étudiants à l'Université de Bradford. Le cinquième, Raja, était élève à Ilford et avait pris contact avec Iqbal par le biais du service de messagerie Internet MSN.

Raja a séjourné quelques jours à Bradford, dans la maison où vivaient Iqbal et Zafar. Il a emporté trois CD réalisés par ses soins, qui contenaient des fichiers choisis provenant de l'ordinateur et qui étaient étiquetés "disques de philosophie". Raja a été arrêté par la police lorsqu'il est rentré chez lui.

[84] Susan Hemming, "The practical application of counter-terrorism legislation in England and Wales: a prosecutor's perspective", *International Affairs*, vol. 86, n° 4 (juillet 2010), p. 963.

L'enquête a conduit les policiers à arrêter les autres accusés et à perquisitionner leurs domiciles. Les policiers ont découvert que ces personnes étaient aussi en possession de documents djihadistes radicaux et d'autres documents tels qu'un manuel militaire américain téléchargé sur Internet. Des preuves de communications par messagerie en ligne ont été découvertes, dont une discussion entre les quatre appelants de Bradford et un cousin de Malik, Imran, qui vivait au Pakistan.

Les charges initialement retenues contre les cinq personnes se fondaient sur l'article 58 de la loi de 2000; cependant, lors du renvoi en jugement, le ministère public a ajouté des charges au titre de l'article 57, qui reflétaient les mêmes éléments que ceux relevant de l'article 58. Après diverses décisions préalables au procès portant sur la question de savoir si des informations stockées électroniquement pouvaient être considérées comme un "objet" (*"article"*) aux fins de l'article 57, le ministère public a décidé d'agir au procès sur le seul fondement de l'article 57.

Lors du procès, Zafar et Iqbal ont été acquittés du chef d'accusation de possession de trois "disques de philosophie" contenant des fichiers émanant de Raja; en revanche, comme les autres accusés, ils ont été reconnus coupables de tous les autres chefs d'accusation. Malik a été condamné à trois ans d'emprisonnement, Zafar et Iqbal à trois ans de détention dans une institution pour jeunes délinquants, Butt à 27 mois de détention et Raja à deux ans de détention.

Les intéressés ont fait appel de ces condamnations. La Cour d'appel a examiné la question déterminante de savoir si, au vu des faits de l'espèce, il existait entre les objets en question et les actes de terrorisme un lien répondant aux critères de l'article 57.

Les objets qui, d'après le ministère public, étaient en possession des appelants en violation de l'article 57 se composaient, pour l'essentiel, de CD et de disques durs contenant des informations stockées électroniquement. Ces informations comprenaient de la propagande idéologique et des communications entre les appelants qui, selon l'accusation, démontraient que les intéressés projetaient de se rendre au Pakistan pour bénéficier d'un entraînement et participer aux combats en Afghanistan, ce qui, toujours selon l'accusation, équivalait à des actes de terrorisme. La Cour d'appel a jugé que le ministère public devait prouver d'abord le but auquel chaque appelant détenait le matériel stocké, et ensuite le lien entre ce but et "la commission, la préparation ou l'instigation à la commission" des actes de terrorisme potentiels sur lesquels se fondait l'accusation, à savoir la lutte contre le Gouvernement afghan.

Relevant que les faits de l'espèce soulevaient des questions complexes d'interprétation du champ d'application de l'article 57, la Cour a jugé que le lien nécessaire n'était pas présent et que les condamnations étaient donc infondées. Par conséquent, elle a fait droit à l'appel.

99. L'article 58 de la loi s'est avéré particulièrement utile dans plusieurs affaires où les autorités avaient dû intervenir alors qu'il n'était nullement prouvé que l'individu concerné se livrait à une activité associée au terrorisme. Cet article érige en infraction pénale le fait de collecter, de fabriquer ou d'avoir en sa possession, sans excuse raisonnable, toute information de nature à être utile à une personne commettant ou préparant un acte de terrorisme ou d'avoir en sa possession tout document ou enregistrement contenant une telle information.

100. Dans l'affaire *R* c. *K* [2008] 3 All E.R. 526, le tribunal a jugé qu'un document n'entrait dans le champ d'application de l'article 58 que s'il était de nature à fournir probablement une assistance pratique à une personne commettant ou s'apprêtant à commettre un acte de terrorisme. Cette approche a été réaffirmée dans l'affaire *R* c. *G et J* [2009] UKHL 13, où le tribunal a confirmé ce "critère d'utilisation pratique": la possession d'un document ou d'un enregistrement ne constitue une infraction que si ce dernier a une utilisation pratique et que la personne concernée le possède sans excuse raisonnable[85]. Il n'existe aucune restriction quant à ce qui pourrait constituer une excuse raisonnable à cette fin, dès lors que cet élément peut constituer en droit un moyen de défense.

101. En vertu de l'article 58, l'accusation n'est pas tenue de prouver que l'accusé est un terroriste ou qu'il possède les objets en question à des fins terroristes; cependant, elle ne peut avoir recours à des preuves extrinsèques pour prouver l'utilité pratique de l'objet que dans des circonstances très limitées. À titre d'exemple, elle peut invoquer des preuves de cryptage pour déchiffrer un document écrit en code, mais ne peut le faire pour expliquer la signification de lieux entourés sur une carte. L'information doit "parler d'elle-même" et ne pas être de nature à circuler de manière générale.

102. Dans l'affaire *R* c. *Sultan Mohammed* [2010] EWCA Crim 227, le tribunal a jugé que "[p]ourvu que le document contenant l'information en question ne soit pas un document utilisé quotidiennement par le grand public (par exemple, horaires et cartes publiés) et pourvu qu'un jury raisonnable puisse conclure avec justesse que le document contient une information de nature à être utile à une personne commettant ou préparant un acte de terrorisme, le jury devra se demander s'il est certain que le document contient cette information. Dans l'affirmative, et pourvu que l'accusé ait l'intention criminelle nécessaire, la seule question serait de déterminer si l'accusé avait une excuse raisonnable"[86]. Par conséquent, le jury doit décider si l'explication donnée concernant la possession du document est raisonnable au vu des faits et des circonstances de l'espèce [87].

103. La loi britannique de 2006 contre le terrorisme a créé (dans son article 5) l'infraction de "commission d'actes préparatoires au terrorisme". Cet article a été élaboré pour gérer les affaires dans lesquelles des individus planifiant activement des actes de terrorisme ont été interrompus avant de pouvoir accomplir ou tenter d'accomplir un acte terroriste matériel[88].

104. L'article 5 s'est révélé particulièrement utile dans les cas de "loup solitaire", où un délinquant agit seul, et où les autorités ne disposent pas de preuves suffisantes pour fonder une accusation d'entente criminelle parce qu'elles ne peuvent démontrer que plusieurs personnes étaient impliquées, ou qu'elles ne connaissent pas les détails de l'infraction planifiée. L'accusation n'est pas tenue de faire la preuve d'un ou de plusieurs

[85] Ibid., p. 962.

[86] Citation extraite de "R. v. Muhammed [2010] EWCA Crim 227: terrorism—preparing an act of terrorism", *Criminal Law and Justice Weekly* (20 mars 2010).

[87] Hemming, "The practical application of counter-terrorism legislation in England and Wales", p. 963.

[88] Ibid., p. 964.

actes de terrorisme finaux identifiables, mais elle doit démontrer l'existence d'une intention spécifique de commettre un acte terroriste ou d'aider un tiers à le faire. Au Royaume-Uni, plusieurs individus ont été condamnés au titre de cette infraction à des peines d'emprisonnement de durées diverses, notamment à la réclusion à perpétuité[89].

105. L'affaire *R* c. *Terence Roy Brown* [2011] EWCA Crim 2751 illustre l'utilité de dispositions telles que l'article 58.

R* c. *Terence Roy Brown

Terence Roy Brown, citoyen britannique, gérait une entreprise en ligne. Dans ce cadre, il faisait de la publicité pour l'édition annuelle d'un CD-ROM qu'il intitulait "Anarchist's Cookbook" (titre pratiquement identique à celui d'un ouvrage très célèbre, *The Anarchist Cookbook*) et la vendait. Ce CD ne se composait pas d'une publication unique, mais de 10 322 fichiers, dont certains constituaient des documents à part entière. Ces fichiers contenaient des manuels terroristes comme le manuel d'Al-Qaida et des instructions pour fabriquer diverses formes d'explosifs et de bombes. D'autres fichiers se composaient d'instructions concernant la fabrication de poisons, la manière d'éviter d'attirer l'attention des autorités lors des déplacements et les techniques de manipulation d'armes. Dans un effort manifeste de contourner la loi, M. Brown plaçait des dénis de responsabilité sur le site Web faisant la publicité de cette publication, indiquant que la mise en œuvre des instructions qu'elle contenait pouvait être illégale ou dangereuse et que ces instructions étaient destinées "au seul plaisir de la lecture et n'avaient qu'une valeur historique". L'enquête a clairement démontré que M. Brown était animé par des motifs purement commerciaux. Il est également apparu qu'il avait délibérément étendu sa collection juste après les attentats à l'explosif commis à Londres en juillet 2005, et qu'il avait dès lors considérablement accru ses bénéfices.

En mars 2011, M. Brown a été convaincu de sept chefs d'accusation en vertu de la loi de 2000 contre le terrorisme (article 58) relatifs à la collecte d'informations susceptibles d'être utilisées pour préparer ou commettre des actes de terrorisme, de deux chefs d'accusation en vertu de la loi de 2006 contre le terrorisme (art. 2) relatifs à la diffusion de publications terroristes et d'une infraction en vertu de la loi de 2002 intitulée *Proceeds of Crime Act* (loi sur le produit du crime) relative au transfert de biens criminels (à savoir, l'utilisation des bénéfices de son entreprise)[a].

Au procès, M. Brown a invoqué l'excuse suivante: ses activités n'allaient pas au-delà de l'exercice légal de son droit à la liberté d'expression, s'agissant de matériel qui était librement accessible sur l'Internet et dont la nature, sinon le volume, était similaire au matériel vendu par d'autres libraires en ligne. Il a invoqué les mêmes arguments lors de l'appel (rejeté) de la condamnation: la Cour d'appel a jugé que la limitation des droits de M. Brown en vertu de l'article 10 concernant du matériel susceptible d'aider les terroristes était justifiée et proportionnelle. La Cour a également affirmé le pouvoir discrétionnaire du ministère public de ne pas poursuivre chaque individu qui aurait pu commettre une infraction, mais d'examiner chaque affaire au cas par cas.

[a] "*Businessman* who published bomb-makers' handbook 'facing lengthy spell in jail'", *Daily Mail*, 9 mars 2011. Disponible à l'adresse: www.dailymail.co.uk/news/article-1364621/Businessman-published-bomb-makers-handbook-facing-lengthy-spell-jail.html#ixzz1j4gXbMLu.

[89] Ibid.

106. Cette espèce fait partie d'un ensemble d'affaires, dont *R* c. *K* [2008] QB 827 et *R* c. *G* [2010] 1 AC 43, dans lesquelles les tribunaux britanniques ont précisé la jurisprudence concernant la portée et l'application de l'article 58 de la loi, à la lumière des garanties pertinentes en matière de droits de l'homme.

107. Outre les infractions pénales définies par la législation antiterrorisme, les autorités britanniques ont, lorsque les circonstances l'exigeaient, utilisé l'infraction d'incitation pour poursuivre avec succès les personnes exerçant des activités liées au terrorisme. On peut citer à titre d'exemple l'affaire *R* c. *Bilal Zaheer Ahmad*[90], dans laquelle l'intéressé a été condamné pour incitation au meurtre.

R* c. *Bilal Zaheer Ahmad

Cette espèce jugée au Royaume-Uni est liée et consécutive à l'affaire impliquant Roshanara Choudhry, qui a été condamnée le 2 novembre 2010 à la réclusion criminelle à perpétuité pour avoir tenté d'assassiner le député Stephen Timms.

Dans sa déposition, M^me^ Choudhry a indiqué qu'elle avait décidé de commettre cette infraction environ quatre semaines avant l'attaque (survenue en mai 2010), et qu'elle avait acheté deux couteaux en préparation, dont un de rechange au cas où le premier se briserait lorsqu'elle poignarderait la victime. Elle a déclaré à la police qu'elle avait regardé des vidéos d'Anwar al-Awalaki et d'Abdullah Azzam et qu'elle avait consulté le site Web www.revolutionmuslim.com pendant sa période de radicalisation. Ce site connu, qui était hébergé aux États-Unis, contenait du matériel de promotion d'un djihad violent, notamment des vidéos et des discours encourageant le terrorisme et des liens vers des publications terroristes.

Le 1^er^ novembre 2010, l'accusé a publié sur sa page Facebook un lien vers un article concernant l'affaire Timms/Choudhry, auquel il a ajouté le commentaire suivant:

> Cette sœur nous couvre de honte, nous les hommes. NOUS DEVRIONS FAIRE CELA.

Le 4 novembre 2010, l'intéressé a publié, sous le nom de "BILAL", un article intitulé "MPs that voted for War on Iraq" ("Les députés qui ont voté pour la guerre en Iraq") sur le site Revolution Muslim. Au début de cet article figurait le symbole de l'État islamique d'Iraq (une branche d'Al-Qaida). Le texte liminaire était une citation du Coran indiquant que ceux qui mouraient sans participer au djihad étaient des hypocrites.

L'article informait les lecteurs qu'ils pouvaient "localiser" les députés britanniques grâce à un lien vers un site Web parlementaire officiel. Ils étaient ainsi en mesure de trouver des informations sur les lieux de permanences des députés, où ils pourraient les "rencontrer en personne".

Ce texte était suivi de 29 citations religieuses traduites en anglais et se rapportant à l'obligation des musulmans de participer au djihad ou au "martyre". Juste après les citations figurait un lien vers une page Web faisant la publicité d'un couteau à vendre. Une copie de cet article a été enregistrée à titre de preuve par les agents des services britanniques

[90] Nottingham Crown Court, 13 mai 2011.

de lutte contre le terrorisme. Une autre copie a été fournie par Google Inc., en réponse à une lettre de requête.

Le 10 novembre 2010, l'accusé a été arrêté par l'Unité antiterroriste de la Police du West Midlands près de son domicile à Wolverhampton. Il a été trouvé en possession d'un ordinateur portable, qu'il a déclaré aux policiers venus l'arrêter avoir utilisé pour publier l'article concernant les députés sur le site Revolution Muslim. Un examen criminalistique de l'ordinateur portable a révélé que l'intéressé avait apparemment tenté d'effacer les traces de ses activités en ligne avant son arrestation.

Le 16 novembre, Bilal Zaheer Ahmad a été mis en accusation pour incitation au meurtre relativement à l'article concerné et pour trois infractions de possession de matériel de nature à être utile à un terroriste en vertu de l'article 58 de la loi de 2000 contre le terrorisme. Par la suite, il a plaidé coupable de ces chefs d'accusation, ainsi que d'une infraction d'incitation à la haine religieuse découlant de commentaires publiés sur un forum Internet, et a été condamné à une peine de 12 ans d'emprisonnement, assortie d'une période supplémentaire de cinq ans de liberté conditionnelle.

108. Aux États-Unis, l'article 842 p) du titre 18 du Code des États-Unis, intitulé "Distribution of information relating to explosives, destructive devices, and weapons of mass destruction" ("Diffusion d'informations relatives aux explosifs, engins de destruction et armes de destruction massive") rend illégal le fait de diffuser, par quelque moyen que ce soit, des informations concernant la fabrication ou l'utilisation d'explosifs, d'engins de destruction ou d'armes de destruction massive avec l'intention que ces informations soient utilisées pour commettre un crime violent ou en sachant que la personne à laquelle ces informations sont communiquées a l'intention de les utiliser pour commettre un crime violent. Ce texte a été utilisé aux États-Unis pour poursuivre des individus qui ont diffusé de telles informations sur Internet.

b) Incitation

109. L'infraction d'incitation à commettre des actes terroristes fait l'objet de la résolution 1624 (2005) du Conseil de sécurité. Dans cette résolution, le Conseil a appelé tous les États à, entre autres, 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, et prévenir une telle incitation.

110. L'élaboration et l'application de lois incriminant l'incitation à commettre des actes de terrorisme tout en protégeant pleinement les droits de l'homme, tels que la liberté d'expression et le droit d'association, constituent des défis permanents pour les dirigeants, les législateurs, les services de détection et de répression et les procureurs. Les affaires concernant des déclarations faites sur Internet, en particulier lorsque le délinquant présumé, les services Internet utilisés et le public visé se trouvent dans des pays différents, sont régies par des lois nationales et garanties constitutionnelles diverses, et supposent donc des difficultés supplémentaires pour les enquêteurs et les procureurs du point de vue de la coopération internationale.

111. En matière de répression des infractions pénales concernant l'incitation à commettre des actes terroristes, l'expérience internationale fait ressortir deux éléments: premièrement, à quel point il est important (et parfois difficile) de faire, en pratique, la distinction entre la propagande terroriste (déclarations défendant des opinions idéologiques, religieuses ou politiques particulières), d'une part, et les documents ou les déclarations qui constituent une incitation à commettre des actes terroristes violents, d'autre part; et deuxièmement, à quel point l'application des lois relatives aux actes d'incitation présumés requiert une évaluation approfondie, dans chaque cas, des circonstances et du contexte pour déterminer si, dans une affaire donnée, il convient d'engager des poursuites au titre de l'infraction d'incitation.

112. Les spécialistes présents à la réunion du groupe d'experts qui sont intervenus dans des enquêtes et des poursuites relatives à des infractions d'incitation à commettre des actes terroristes se sont accordés à souligner l'importance pratique d'évaluer parfaitement le contexte dans lequel les déclarations présumées constitutives d'incitation ont été prononcées, et notamment les mots employés, mais également le lieu où ils l'ont été. Ils ont également mis en relief le fait que les caractéristiques des destinataires probables de ces déclarations pouvaient constituer des facteurs extrêmement pertinents pour déterminer s'il convenait d'engager des poursuites pénales au titre de l'infraction d'incitation et si ces poursuites étaient susceptibles d'aboutir dans une affaire donnée.

113. Au Royaume-Uni, l'article 59 de la loi de 2000 contre le terrorisme confère le caractère d'infraction au fait d'inciter une autre personne à commettre un acte de terrorisme totalement ou partiellement en dehors du Royaume-Uni, lorsque cet acte, s'il était commis en Angleterre ou au pays de Galles, constituerait une infraction spécifiée dans l'article (par exemple, meurtre, coups et blessures volontaires, explosion ou mise en danger de la vie d'autrui par atteinte aux biens).

114. Dans la célèbre affaire *R* c. *Tsouli* et al.[91], Younes Tsouli, Waseem Mughal et Tariq al-Daour ont plaidé coupables des chefs d'accusation d'incitation au meurtre à des fins terroristes, visés par la loi de 2000 contre le terrorisme, en créant et en gérant de nombreux sites Web et forums de discussion utilisés pour publier des documents incitant au meurtre terroriste, principalement en Iraq.

_R_ c. _Tsouli_ et al.

Cette célèbre affaire, jugée au Royaume-Uni, concernait trois individus, Younes Tsouli, Waseem Mughal et Tariq al-Daour, qui étaient initialement visés par 15 chefs d'accusation. Avant le procès, Tsouli et Mughal ont plaidé coupables de l'accusation d'entente criminelle en vue de commettre une fraude. Pendant le procès, après avoir entendu les preuves du ministère public, les trois individus ont plaidé coupables d'une accusation d'incitation au terrorisme à l'étranger, et al-Daour a plaidé coupable d'une accusation d'entente criminelle en vue de commettre une fraude.

[91] *R* c. *Tsouli* [2007] EWCA Crim 3300.

Entre juin 2005 et leur arrestation en octobre 2005, les intéressés ont été impliqués dans l'achat, la création et la gestion de nombreux sites Web et forums de discussion en ligne sur lesquels ont été publiés des matériels incitant au meurtre terroriste, principalement en Iraq. Les frais d'achat et de gestion des sites Web étaient financés par le produit d'une fraude à la carte de crédit. Les matériels publiés sur les sites Web se composaient notamment de déclarations indiquant que les musulmans avaient le devoir de se livrer au djihad armé contre les juifs, les croisés, les apostats et leurs sympathisants dans tous les pays musulmans et que chaque musulman devait les combattre et les tuer, où qu'ils se trouvent et qu'ils soient civils ou militaires.

Sur les forums de discussion en ligne, les individus disposés à rejoindre l'insurrection se voyaient fournir des itinéraires permettant de se rendre en Iraq ainsi que des manuels sur les armes et des recettes d'explosifs. Les enquêteurs ont retrouvé au domicile de chacun des accusés du matériel idéologique extrémiste montrant son adhésion aux justifications avancées concernant les meurtres que les sites Web et forums de discussion incitaient à commettre.

Al-Daour se chargeait d'obtenir des cartes de crédit volées, tant à son propre usage que pour fournir à Mughal les fonds permettant de créer et de faire fonctionner les sites Web. Al-Daour avait été impliqué dans d'autres fraudes à la carte de crédit, dont les produits n'avaient pas servi à financer les sites Web concernés. Pour les sociétés de cartes de crédit, la perte issue de cet aspect de l'activité frauduleuse des accusés s'est élevée à 1,8 million de livres sterling.

Parmi les preuves se trouvait une liste rédigée de la main de Tsouli et découverte sur son bureau, sur laquelle il avait inscrit les coordonnées d'un certain nombre de sites Web et de cartes de crédit volées. Ce document a révélé l'existence de 32 sites Web distincts, mis à disposition par plusieurs sociétés d'hébergement Web que Tsouli avait créées ou tenté de créer, principalement au cours de la dernière semaine de juin 2005, mais également en juillet et en août. La création et l'administration de ces sites Web étaient financées par l'utilisation frauduleuse des coordonnées de cartes de crédit qui avaient été volées à des titulaires de compte, soit directement par vol de documents informatiques, soit par piratage ou autre détournement frauduleux au sein d'institutions financières. Ces coordonnées de cartes de crédit avaient été communiquées à Tsouli par les deux autres accusés.

Les sites Web créés par Tsouli faisaient office de vecteurs de téléchargement de matériel djihadiste, qui incitait à commettre des actes de violence en dehors du Royaume-Uni, en Iraq. L'accès aux sites était limité aux personnes qui avaient reçu des noms d'utilisateur et des mots de passe. Au procès, le juge a considéré que les accusés avaient procédé ainsi pour que les sociétés d'hébergement Web et les services de détection et de répression aient plus de mal à savoir ce qui était publié sur les sites.

Le 5 juillet 2007, Tsouli a été condamné à 10 ans et trois ans et demi de prison (avec confusion des peines) sur deux chefs d'accusation. Mughal a été condamné à sept ans et demi et trois ans et demi de prison (avec confusion des peines) sur deux chefs d'accusation et al-Daour, à six ans et demi et trois ans et demi de prison (avec confusion des peines).

115. La première partie de la loi de 2006 contre le terrorisme a établi un certain nombre de nouvelles infractions visant à renforcer la capacité des autorités à prendre des mesures dans les affaires impliquant des déclarations incitant à commettre des actes de terrorisme, en faisant l'apologie ou autrement destinées à soutenir ces actes.

116. La première partie de cette loi érige en infraction pénale le fait de publier une déclaration destinée à encourager directement ou indirectement le public à préparer, instiguer ou commettre des actes de terrorisme, notamment (mais de manière non limitative) tout encouragement qui "fait l'apologie" des actes terroristes, ou le fait d'être imprudent quant à la possibilité que cette conduite ait un tel effet. En pratique, la manière dont une déclaration sera probablement comprise est déterminée en fonction de son contenu dans son ensemble et du contexte dans lequel elle est fournie.

117. L'article 2 de la loi confère le caractère d'infraction au fait de diffuser (intentionnellement ou par imprudence) des publications terroristes. Celles-ci se définissent comme des publications qui encourageront probablement des actes de terrorisme ou seront probablement utiles à une personne planifiant ou commettant un tel acte. Cette deuxième catégorie recouvre les mêmes types de documents ou de publications que l'article 58 de la loi de 2000 contre le terrorisme. Comme pour l'article premier de la loi de 2006 contre le terrorisme, la question de savoir si le matériel en question entre dans la définition d'une "publication terroriste" doit être déterminée par rapport à son contenu dans son ensemble et au contexte dans lequel elle est fournie[92].

118. Au Royaume-Uni, lorsque les procureurs décident s'ils doivent engager des poursuites pour incitation, ils exercent un large pouvoir discrétionnaire, et prennent en compte le droit à la liberté d'expression et le contexte global dans lequel les déclarations ou publications ont été effectuées ou diffusées, notamment la façon dont elles seront probablement comprises par le grand public et par leurs destinataires visés.

119. Aux États-Unis, une approche juridique différente a été adoptée concernant l'incrimination et la poursuite des actes d'incitation au terrorisme en raison des garanties constitutionnelles se rattachant au droit à la liberté d'expression prévu par le premier amendement de la Constitution. En vertu des principes définis dans l'affaire historique *Brandenburg* c. *Ohio*, 395 US. 444 (1969), le ministère public doit, afin de poursuivre avec succès un individu pour incitation à commettre des actes criminels (terrorisme inclus), prouver à la fois l'intention d'inciter à commettre ou produire une action illégale, et la probabilité que le discours incite effectivement à commettre une action illégale imminente[93].

120. Lorsqu'elles poursuivent des déclarations incitant à commettre des actes de terrorisme, les autorités américaines se fondent sur les infractions inchoatives comme l'incitation et l'entente criminelle (*conspiracy*), ainsi que sur les dispositions du Code pénal relatives au "soutien matériel" (*material support*), qui autorisent dans certaines circonstances la poursuite de conduites soutenant des actes de terrorisme violents[94].

121. Les dispositions du Code pénal des États-Unis relatives au "soutien matériel", à savoir les articles 2339A et 2339B du titre 18, interdisent de, sciemment ou

[92] Hemming, "The practical application of counter-terrorism legislation in England and Wales", p. 963.

[93] Elizabeth M. Renieris, "Combating incitement to terrorism on the Internet: comparative approaches in the United States and the United Kingdom and the need for an international solution", *Vanderbilt Journal of Entertainment and Technology Law*, vol. 11, n° 3 (2009), p. 681 et 682.

[94] Code pénal des États-Unis, titre 18, articles 2339A et 2339B.

intentionnellement, fournir, tenter de fournir ou s'associer pour fournir un soutien matériel ou des ressources à une organisation terroriste. La loi intitulée *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism* (PATRIOT) *Act* (loi pour unir et renforcer l'Amérique en fournissant les outils appropriés pour déceler et contrer le terrorisme), adoptée en 2001, a élargi la définition du soutien matériel pour inclure "tout bien, matériel ou immatériel, ou service, y compris […] formation, conseils ou assistance d'expert […] ou équipement de communication"[95].

122. L'article 373 *a* du titre 18 du Code pénal des États-Unis, relatif aux infractions pénales d'incitation ou d'entente criminelle, dispose que peut être accusé d'incitation quiconque "dans l'intention de faire commettre un acte criminel par un tiers, encourage ce tiers à commettre un acte criminel, le lui ordonne, l'y incite ou s'efforce d'une autre manière de le persuader de commettre l'acte en question".

123. Aux États-Unis, cette méthode a été utilisée avec succès dans plusieurs affaires judiciaires pour poursuivre les paroles ou les actions de terroristes communiquées via l'Internet. On peut notamment citer l'affaire *États-Unis d'Amérique* c. *Emerson Winfield Begolly*.

États-Unis d'Amérique* c. *Emerson Winfield Begolly

Emerson Winfield Begolly, un étudiant américain de 22 ans, a été mis en accusation pour son implication dans la diffusion sur Internet d'informations relatives à la fabrication de bombes et pour incitation à commettre des violences sur le territoire américain. Parmi les autres chefs d'accusation retenus à son encontre figuraient l'agression et la menace d'agents du Federal Bureau of Investigation (FBI) avec une arme chargée.

Opérant auparavant sous le pseudonyme "Asadullah Alshishani", Begolly a joué un rôle actif dans un forum djihadiste internationalement connu, l'Ansar al-Mujahideen English Forum, et en est finalement devenu modérateur. Ce forum a permis à Begolly d'exprimer son attrait pour les opinions radicales tout en encourageant ses coreligionnaires à commettre des actes terroristes aux États-Unis. Sa propagande comprenait également la diffusion de vidéos contenant des instructions pour fabriquer des engins explosifs afin d'exécuter des actes de terrorisme. Les cibles étaient notamment les synagogues, les installations militaires, les lignes ferroviaires, les postes de police, les ponts, les relais de téléphonie mobile et les stations d'épuration des eaux.

Sur une période de neuf mois, Begolly a publié plusieurs longs messages dans lesquels il évoquait abondamment la nécessité de la violence. Le tribunal de district américain du district est de Virginie a délivré le 14 juillet 2011 un acte d'accusation qui comprenait en guise de preuve déterminante une partie de la propagande publiée par Begolly sur un forum Internet:

> Les manifestations pacifiques ne servent à rien. Les Kuffar[a] considèrent la guerre comme la solution à leurs problèmes, nous devons donc la considérer comme la solution aux nôtres. Pas de paix. Mais des balles, des bombes et des opérations de martyre.

[95] Renieris, "Combating incitement to terrorism on the Internet", p. 682 et 683.

Begolly a également publié des liens vers un document téléchargeable intitulé "The explosives course" ("Le cours sur les explosifs"). Ce document de 101 pages rédigé par le "martyr Sheik Professeur Abu Khabbab al Misri" (comme l'appelait Begolly) contenait des instructions détaillées pour créer un laboratoire avec des composants chimiques de base et fabriquer des explosifs. Une note avait été ajoutée, précisant que les personnes qui téléchargeaient ce contenu devaient veiller, pour leur propre protection, à utiliser un logiciel de préservation de l'anonymat.

Pendant cette période, Begolly était sous surveillance permanente des autorités fédérales. Un agent du FBI a téléchargé le document à partir de l'un des liens proposés, ce qui a finalement conduit à l'arrestation de Begolly. Le 14 avril 2011, ce dernier a été accusé de diffusion illégale et intentionnelle d'informations sur Internet relatives à la fabrication et à la diffusion de matériels explosifs ainsi qu'à l'utilisation d'armes de destruction massive, et d'incitation à commettre des attentats à l'explosif dans les lieux publics, les bâtiments administratifs et les systèmes de transport en commun. Le 9 août 2011, Begolly a plaidé coupable d'incitation à commettre des actes terroristes. Il attend actuellement que sa peine soit prononcée.

[a]Un terme abondamment utilisé par Begolly dans ses discussions sur le forum pour désigner les "incroyants" ou infidèles.

c) Examen de l'approche juridique de l'incitation

124. En Europe, l'article 3 de la décision-cadre 2008/919/JAI du 28 novembre 2008 du Conseil de l'Union européenne modifiant la décision-cadre 2002/475/JAI relative à la lutte contre le terrorisme, ainsi que l'article 5 de la Convention du Conseil de l'Europe pour la prévention du terrorisme font obligation aux États membres respectivement parties à ces instruments d'incriminer les actes ou les déclarations constituant une incitation à commettre des actes de terrorisme. La Convention du Conseil de l'Europe pour la prévention du terrorisme impose aux États membres l'obligation d'incriminer la "provocation publique à commettre une infraction terroriste", ainsi que le recrutement et l'entraînement pour le terrorisme.

125. L'application de la Convention, qui repose en partie sur l'article 3 du Protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, contraint les États à trouver un équilibre délicat entre les exigences de détection et de répression, d'une part, et la protection des droits de l'homme et des libertés, d'autre part. Par conséquent, cette application a donné lieu à de fortes inquiétudes et fait l'objet de débats. Toutefois, l'article 5 (tout comme les articles 6 et 7 sur le recrutement et l'entraînement à des fins terroristes) doit être appliqué à la lumière de la disposition fondamentale de l'article 12, selon laquelle la mise en œuvre de cette incrimination doit intervenir d'une manière qui respecte les droits de l'homme, notamment la liberté d'expression, la liberté d'association et la liberté de religion, tels qu'établis dans les instruments relatifs aux droits de l'homme, dont le paragraphe 1 de l'article 10 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

126. La Cour européenne des droits de l'homme, dans son évaluation des garanties octroyées par le paragraphe 1 de l'article 10 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, s'est penchée sur l'article 5 de la Convention du Conseil de l'Europe pour la prévention du terrorisme. Dans la célèbre affaire *Leroy* c. *France*[96], un tribunal français a jugé qu'il n'y avait pas eu de violation de l'article 10 dans le cas d'un journaliste qui avait été déclaré coupable d'avoir publié un dessin donné dans un hebdomadaire basque et condamné à payer une amende. Le 11 septembre 2001, le dessinateur avait remis à la rédaction de la revue un dessin représentant l'attentat contre les tours jumelles du World Trade Center, avec une légende pastichant le slogan publicitaire d'une marque célèbre: "Nous en avons tous rêvé... Le Hamas l'a fait" (cf. "Sony l'a fait"). Le dessin a été publié dans la revue le 13 septembre 2001.

127. Dans son argumentation, la Cour européenne des droits de l'homme s'est référée, entre autres, à l'article 5 de la Convention du Conseil de l'Europe pour la prévention du terrorisme: c'était la première fois que la Cour prenait en considération cette Convention dans un arrêt. Elle a jugé que le dessin ne se limitait pas à une critique des États-Unis mais qu'il soutenait et glorifiait leur destruction par la violence. La Cour a pris note de la légende accompagnant le dessin, indiquant l'appui moral exprimé par le requérant aux auteurs présumés de l'attentat du 11 septembre 2001. La Cour a tenu compte d'autres facteurs, dont les termes choisis par le requérant, la date de la publication du dessin (qui, selon la Cour, accentuait la responsabilité du dessinateur) et la région politiquement sensible dans laquelle la diffusion est intervenue (le Pays basque). D'après la Cour, le dessin a entraîné des réactions pouvant attiser la violence, démontrant son impact plausible sur l'ordre public dans la région. Les principes définis dans cette espèce historique s'appliqueront aussi aux affaires dans lesquelles l'incitation présumée au terrorisme s'est produite via l'Internet.

128. Il existe plusieurs exemples de poursuites pour actes d'incitation en Europe. En Allemagne, par exemple, Ibrahim Rashid, un immigrant irako-kurde, a été déclaré coupable d'incitation en 2008 après avoir été accusé de mener un "djihad virtuel" sur Internet. Le ministère public a soutenu qu'en diffusant de la propagande d'Al-Qaida sur des forums de discussion en ligne, Rashid essayait de recruter des individus pour qu'ils rejoignent Al-Qaida et participent au djihad.

129. Le *Recueil de cas sur les affaires de terrorisme*[97] de l'ONUDC contient un résumé utile des méthodes adoptées concernant l'incrimination des actes d'incitation en Algérie, en Égypte, en Espagne et au Japon. En Algérie, l'article 87 *bis*-1 du Code pénal sanctionne les actes de terrorisme violents par la peine de mort, la réclusion criminelle à perpétuité ou d'autres peines de longue durée. L'article 87 *bis*-4 dispose que quiconque fait l'apologie, encourage ou finance les actes terroristes énumérés dans ce même article est passible de cinq à 10 ans de réclusion et d'une amende[98].

[96] Arrêt de la Cour européenne des droits de l'homme (cinquième section), affaire *Leroy* c. *France*, requête n° 36109/03 du 2 octobre 2008.

[97] Office des Nations Unies contre la drogue et le crime, *Recueil de cas sur les affaires de terrorisme* (2010).

[98] Ibid., par. 100.

130. En Égypte, l'article 86 *bis* du Code pénal érige en infractions pénales les actes constituant l'exécution et le soutien d'actes terroristes, la planification et la préparation d'actes terroristes, l'appartenance ou le soutien à une organisation illégale, le soutien financier et matériel d'organisations terroristes et l'incitation au terrorisme. De plus, cet article prévoit un alourdissement de la sanction en cas, entre autres, de promotion intentionnelle (par quelque moyen que ce soit) des objectifs des organisations terroristes ou d'obtention ou de production (directe ou indirecte) d'imprimés, de publications ou d'enregistrements de quelque nature que ce soit destinés à promouvoir ou encourager ces objectifs[99].

131. Au Japon, quiconque incite à la commission d'une infraction, directement ou par l'intermédiaire d'un tiers, est passible de sanctions pénales comme s'il était l'exécuteur matériel de l'infraction (art. 61 du Code pénal)[100]. Dans ce pays, d'autres dispositions législatives, tels les articles 38 à 40 de la loi sur la prévention des activités subversives, incriminent l'incitation à l'insurrection ou l'incendie criminel, dans l'intention de promouvoir, soutenir ou s'opposer à une doctrine ou politique.

132. En Espagne, les articles 18 et 579 du Code pénal incriminent l'incitation à commettre un acte de terrorisme en tant qu'acte préparatoire de l'infraction de provocation. L'article 578 incrimine l'apologie du terrorisme, infraction qui a été incorporée dans le Code pénal par la loi organique 7/2000 du 22 décembre 2000. Selon une traduction officieuse, cet article dispose ce qui suit: "L'apologie ou la justification par un moyen d'expression ou de diffusion public des infractions visées aux articles 571 à 577 du présent Code (crimes de terrorisme) ou de celui qui a participé à leur commission, ou la commission d'actes qui ont pour conséquence de discréditer, mépriser ou humilier les victimes d'une infraction terroriste ou les membres de leur famille, est passible d'une peine d'un à deux ans d'emprisonnement." La loi organique prévoit également, en cas de condamnation, la suspension des droits civils pour une durée déterminée[101].

133. En Indonésie, il n'existe pas de réglementation portant expressément sur les activités menées par les terroristes via l'Internet, et notamment l'incitation à commettre des actes de terrorisme. L'article 14 de la loi n° 15/2003 sur la répression des actes de terrorisme traite de l'incitation à commettre de tels actes sans faire référence au mode de communication utilisé par le délinquant. Il en va de même du Code pénal indonésien, qui traite de l'incitation à commettre d'autres actes criminels. Les autorités indonésiennes ont réussi à poursuivre des délinquants pour activité liée au terrorisme sur Internet. En 2007, Agung Prabowo, âgé de 24 ans et également connu sous le nom de Max Fiderman, a été condamné à une peine de trois ans d'emprisonnement (conformément à l'article 13 *c* de la Réglementation gouvernementale remplaçant la loi n° 1/2002 et de la loi n° 15/2003 sur la répression des actes de terrorisme) pour avoir enregistré et hébergé un site Web, www.anshar.net, à la demande de Noordin M. Top,

[99] Ibid., par. 111.

[100] Ibid., par. 100.

[101] Ibid., par. 115.

chef du groupe terroriste Jemaah Islamiyah, via un intermédiaire, Abdul Aziz. Aziz aurait conçu www.anshar.net mi-2005 à la demande de Top, dans le but de répandre la propagande djihadiste. Le site contenait des informations générales sur l'Islam et le djihad, mais également des "astuces et conseils" sur la façon de mener des attaques terroristes et sur les lieux où le faire, en préconisant les routes menant aux centres commerciaux et aux bureaux, les embouteillages et certains endroits désignés où l'on pouvait trouver du public[102]. Dans une autre espèce, Muhammad Jibril Abdul Rahman, également nommé Muhammad Ricky Ardan (le "Prince du Jihad"), a été condamné à cinq ans de prison pour complicité d'acte de terrorisme.

134. À Singapour, l'article 4 2 *g* du Code de pratiques Internet interdit les matériels qui "incitent à la haine, aux conflits ou à l'intolérance ethniques, raciaux ou religieux, les glorifient ou les approuvent".

2. Prise en compte de l'état de droit dans l'incrimination de l'incitation

135. La résolution 1624 (2005) du Conseil de sécurité, qui appelle les États à incriminer l'incitation à commettre des actes terroristes, prévoit expressément que les États doivent veiller à ce que toute mesure adoptée pour mettre en œuvre leurs obligations soit conforme à l'ensemble des obligations que leur impose le droit international, en particulier le droit des droits de l'homme, le droit des réfugiés et le droit humanitaire.

136. Ce principe, qui apparaît également dans les instruments universels de lutte contre le terrorisme, a été réaffirmé à de nombreuses reprises au niveau international (notamment dans le cadre des Nations Unies), et constitue un élément fondamental de l'approche de l'ONUDC fondée sur l'"état de droit" visant à renforcer les mesures de justice pénale en vertu du régime juridique universel de lutte contre le terrorisme. Ce principe est soutenu par de nombreux instruments régionaux de lutte contre le terrorisme et de défense des droits de l'homme, dont en premier lieu ceux qui ont été élaborés par le Conseil de l'Europe et que nous avons précédemment mentionnés (voir la section II.D ci-dessus)[103].

137. Il n'est pas possible d'analyser ici de façon détaillée, dans le contexte du respect des droits à la liberté d'expression garantis, l'ensemble des commentaires et de la jurisprudence disponibles sur la portée et l'application des dispositions adoptées par les pays pour incriminer l'incitation à commettre des actes terroristes.

[102]Voir www.indonesiamatters.com/624/wwwansharnet-chatroom-jihad.

[103]Voir les rapports présentés au Conseil des droits de l'homme et à l'Assemblée générale par le Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, dans lesquels le Rapporteur spécial a exprimé ses préoccupations quant à l'effet que la législation visant l'incitation pouvait avoir sur la liberté de parole et d'expression, en favorisant l'incrimination d'un discours libre ne constituant pas une incitation au terrorisme. Ces opinions et préoccupations ont été exposées dans une soumission écrite présentée au groupe d'experts par le Haut-Commissariat aux droits de l'homme; voir également la déclaration intitulée "Joint Declaration on Freedom of Expression and the Internet", émise le 1er juin 2011 par le Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, le Représentant de l'OSCE pour la liberté des médias, la Rapporteuse spéciale de l'Organisation des États américains chargée de la liberté d'expression, et la Rapporteuse spéciale sur la liberté d'expression et l'accès à l'information de la Commission africaine des droits de l'homme et des peuples, dans laquelle l'importance fondamentale du droit à la liberté d'expression a été réaffirmée.

138. Néanmoins, même si la jurisprudence sur la portée précise des instruments internationaux relatifs aux droits de l'homme, tels que le paragraphe 1 de l'article 10 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et l'article 19 du Pacte international relatif aux droits civils et politiques, prête à discussion, il est clair qu'en pratique il reste très difficile pour les gouvernements de concilier préservation du droit à la liberté d'expression, d'une part, et application d'une législation pénale visant l'incitation à commettre des actes terroristes, d'autre part.

3. Pouvoirs en matière de détection et de répression

139. Dans les enquêtes sur les affaires impliquant l'utilisation d'Internet ou d'autres services connexes par des personnes soupçonnées de terrorisme, les services de renseignement ou de détection et de répression devront souvent se livrer à une forme quelconque d'activité intrusive ou coercitive de perquisition, de surveillance ou de contrôle. Pour que les poursuites aboutissent, il est donc important que ces techniques d'enquête soient dûment autorisées par les lois nationales et, comme toujours, que la législation autorisant ces techniques respecte les droits de l'homme fondamentaux, protégés en vertu du droit international des droits de l'homme.

a) Pouvoirs de perquisition, de surveillance et d'interception

140. En Israël, les pouvoirs d'enquête relatifs à la collecte de preuves numériques sur l'Internet, tant dans les affaires pénales générales que dans celles liées au terrorisme, relèvent de la loi sur l'informatique de 1995, qui définit certains de ces pouvoirs. Cette loi a modifié la loi relative aux écoutes téléphoniques, en considérant que l'acquisition de communications échangées entre ordinateurs constituait une "écoute téléphonique", et en permettant aux autorités chargées des enquêtes d'obtenir une autorisation judiciaire, ou administrative dans les affaires urgentes et exceptionnelles, pour obtenir les données transférées lors de communications entre ordinateurs.

141. En 2007, la loi sur les données relatives à la communication a été adoptée. Ce texte avait pour objet d'organiser, de manière plus structurée et progressive, la pratique admise qui consistait à obtenir des données non relatives au contenu auprès des sociétés de téléphonie mobile ou filaire et des fournisseurs d'accès à l'Internet. Cette loi ne s'applique pas aux fournisseurs d'accès à l'Internet qui offrent d'autres prestations de services, comme le stockage ou le partage d'informations, la messagerie électronique, les réseaux sociaux et autres. Actuellement, lorsque les autorités souhaitent obtenir des informations auprès de fournisseurs d'accès à l'Internet, un ancien article de la loi leur permet, de manière générale, de délivrer une assignation et d'obtenir des informations auprès de toute personne disposant de données susceptibles de faire progresser l'enquête.

142. En 2010, le Gouvernement israélien a défendu un projet de loi visant à codifier les pouvoirs d'enquête relatifs aux données physiques et numériques. Ce projet de loi a pour objet d'organiser, de manière élaborée, la collecte de preuves numériques. Il contient un système structuré de pouvoirs qui ne sont pas actuellement prévus dans la législation israélienne, comme la perquisition secrète d'ordinateurs (en cas d'infractions

particulièrement graves), l'obtention d'informations qui doivent être stockées (dans l'avenir) sur un ordinateur donné, la manière dont il convient de se procurer les courriers électroniques stockés en possession du prestataire de services, la perquisition de matériel informatique sur autorisation administrative dans certaines circonstances. Si le projet est adopté, ces mesures s'appliqueront aux affaires de terrorisme impliquant l'utilisation d'Internet.

143. En 2006, le Gouvernement français a adopté une nouvelle législation de lutte contre le terrorisme facilitant, aux fins d'enquête, la surveillance des communications et l'accès de la police aux données relatives aux communications détenues par les opérateurs téléphoniques, les fournisseurs d'accès à l'Internet et les cybercafés.

144. La loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers (loi 2006-64 du 23 janvier 2006) dispose que les fournisseurs de services Internet, les cybercafés, les prestataires d'hébergement et les opérateurs doivent communiquer les données relatives au trafic, les numéros appelés et les adresses IP aux administrations spécialisées dans les cas liés aux enquêtes sur des soupçons d'activités terroristes.

145. En vertu de l'article 6, les opérateurs de téléphonie mobile et les cybercafés sont tenus de conserver les données relatives aux connexions de leurs clients pendant 12 mois et de les communiquer à la police. La loi autorise également l'utilisation de caméras de surveillance dans les espaces publics, tels que les gares, les églises et les mosquées, les magasins, les usines et les centrales nucléaires. L'article 8 autorise la police à effectuer des contrôles automatisés des véhicules et de leurs occupants sur les routes et les autoroutes françaises (notamment en prenant des photographies des numéros d'immatriculation et des occupants des véhicules) et à contrôler les personnes dans les grands rassemblements publics[104].

146. Plus récemment, le 14 mars 2011, le Code français de procédure pénale a été modifié pour doter les autorités de pouvoirs supplémentaires dans les enquêtes relatives au terrorisme. Ces modifications prévoient notamment les pouvoirs de réquisition des documents pertinents (dont la conversion et le transfert des données informatiques), de décryptage de données informatiques protégées, d'infiltration numérique, de captation de données informatiques (images comprises), de mise sur écoute et d'interception d'autres communications. En outre, la loi établit le fondement juridique des activités des agents des services de détection et de répression qui interviennent, entre autres, dans les forums de discussion en ligne dans le cadre d'enquêtes sur les infractions liées à l'incitation au terrorisme. Il s'agit d'une question juridique importante que les gouvernements pourraient souhaiter prendre en considération. Ces articles de loi fournissent aux autorités françaises de détection et de répression la capacité, entre autres, d'obtenir des preuves relatives aux données de connexion des courriers électroniques, à l'activité téléphonique et aux adresses de protocole Internet.

[104] www.edri.org/edrigram/number4.2/frenchlaw.

147. L'expert chinois a fait état d'une réglementation, en vertu de laquelle la police de son pays, lorsqu'elle ouvre une enquête pénale concernant l'utilisation d'Internet, peut ordonner au fournisseur d'accès à l'Internet et au prestataire de communication Internet de soumettre les données et documents pertinents, que la loi les contraint à conserver pendant 60 jours.

148. Au Royaume-Uni, la loi de 2000 intitulée *Regulation of Investigatory Powers Act* (loi portant réglementation des pouvoirs d'enquête) définit un cadre juridique qui régit les cinq types suivants d'activités de surveillance menées par les organismes publics:

- Interception de communications (par exemple, interception d'appels téléphoniques ou accès au contenu de courriers électroniques);
- Surveillance intrusive (par exemple, surveillance clandestine de locaux ou de véhicules privés);
- Surveillance dirigée (par exemple, surveillance clandestine d'une cible identifiée dans un lieu public);
- Sources clandestines de renseignement humain (par exemple, agents infiltrés);
- Données relatives aux communications (par exemple, enregistrements relatifs aux communications mais pas à leur contenu)[105].

149. Cette loi, en sus de déterminer les objectifs dans lesquels ces activités doivent être autorisées et les procédures selon lesquelles elles peuvent l'être, contraint les autorités chargées de la surveillance à examiner si l'exercice de ces pouvoirs, d'une part, et l'atteinte aux droits des personnes surveillées, d'autre part, sont proportionnels et à prendre des mesures pour éviter l'"intrusion collatérale", qui consiste à porter atteinte aux droits d'autres parties que celles visées. La loi érige également en infraction pénale le fait, pour les parties qui détiennent des clefs de cryptage concernant les communications ciblées, de ne pas les fournir aux organismes autorisés[106].

150. En 2000, le Gouvernement indien a adopté une loi sur les technologies de l'information, qu'il a modifiée en 2008, pour prévoir l'infraction de "cyberterrorisme" (art. 66F) et d'autres points connexes à l'Internet. L'article 67C 1) de la loi porte sur la question de la conservation des données, et dispose que les prestataires réglementés "doivent préserver et conserver les informations spécifiées pendant la durée, de la manière et au format prescrits par le Gouvernement central" et érige en infraction pénale (passible d'une peine pouvant atteindre trois ans de prison, et d'une amende) le fait d'enfreindre sciemment cette obligation.

151. L'article 69 1) de la loi dote les autorités gouvernementales du pouvoir d'émettre des instructions concernant "l'interception, le contrôle et le décryptage de toute information générée, transmise, reçue ou stockée dans une ressource informatique quelconque", et définit les obligations légales et les garanties s'attachant à ces actions.

[105] "Summary of surveillance powers under the *Regulation of Investigatory Powers Act*", National Council for Civil Liberties.

[106] Ian Walden, *Computer Crimes and Digital Investigations* (Oxford University Press, 2007), p. 216.

L'article 69A 1) dote les organismes étatiques du pouvoir d'émettre des instructions visant à empêcher le public, au moyen de ressources informatiques, d'accéder à toute information s'ils le jugent nécessaire ou opportun, dans l'intérêt de la souveraineté, de l'intégrité et des relations internationales de l'Inde, ou pour prévenir l'incitation à commettre des infractions "susceptibles d'être connues" connexes, dont le terrorisme. Enfin, l'article 69B dote certains organismes étatiques désignés du pouvoir de contrôler, de collecter et de stocker les données relatives au trafic ou les informations générées, transmises ou reçues via une ressource informatique quelconque.

152. En Nouvelle-Zélande, la loi de 2012 intitulée *Search and Surveillance Act* (loi sur la perquisition et la surveillance) actualise, consolide et harmonise les pouvoirs des services de détection et de répression relatifs à la perquisition, à la surveillance et à l'interception de communications pour tenir compte des nouvelles formes de technologie. La loi crée une nouvelle définition du terme "perquisition de système informatique", et étend cette définition à la perquisition d'ordinateurs qui ne sont pas connectés en interne à un réseau à distance, mais qui sont capables d'y accéder.

153. Afin de renforcer les garanties légales, la loi précise que la perquisition d'ordinateurs à distance n'est autorisée que dans deux situations: lorsqu'un ordinateur a la capacité d'accéder légalement au système informatique faisant l'objet de la perquisition et est donc considéré comme en faisant partie, et lorsqu'il n'existe pas de lieu physique à perquisitionner (par exemple, dans le cas de courriers électroniques auxquels l'utilisateur accède à partir de divers endroits, comme les cybercafés). La loi dispose également que, lorsque la police effectue des perquisitions autorisées de systèmes de données Internet en y accédant à distance, elle doit informer la personne de la perquisition, par courrier envoyé à l'adresse électronique du système perquisitionné.

b) Questions associées à la mise à disposition de capacités d'interception

154. Dans le cadre de leurs activités électroniques de contrôle, de surveillance ou d'interception, les autorités ont besoin de la coopération des opérateurs qui fournissent des télécommunications publiques ou des services connexes. Dans de nombreux cas, les opérateurs du secteur privé sont disposés à apporter leur assistance aux services de détection et de répression qui s'acquittent de leurs fonctions légales, mais le temps et les ressources qu'ils sont prêts à y consacrer gratuitement sont évidemment limités. Par conséquent, il est souhaitable que les gouvernements donnent un fondement juridique clair aux obligations imposées aux parties du secteur privé, et précisent notamment les spécifications techniques requises de leurs réseaux et les modes de prise en charge des frais de mise à disposition de ces capacités.

155. En Israël, l'article 13 de la loi de 1982 relative à la communication dispose que le Premier ministre peut ordonner aux fournisseurs nationaux d'accès à l'Internet d'effectuer les modifications technologiques requises par les forces de sécurité (définies comme la police, les services de sécurité et les autres services spéciaux) dans le cadre des activités de lutte contre le terrorisme. Cette loi ne s'applique qu'aux fournisseurs d'accès à l'Internet, qui en vertu du droit israélien reçoivent leur licence du Ministère des communications. Elle ne s'applique pas aux prestataires de services de stockage des

données ou de gestion de contenus qui opèrent dans le pays, car ils n'ont pas besoin de licence du Ministère.

156. En Nouvelle-Zélande, la loi de 2004 intitulée *Telecommunications (Interception Capability) Act* (loi sur les (capacités d'interception des) télécommunications) précise l'obligation des opérateurs de réseau d'aider les organismes gouvernementaux autorisés à mener des opérations d'interception ou de leur fournir des données relatives aux appels. Cette loi contraint les opérateurs de réseau à s'assurer que chaque réseau ou service de télécommunications publiques détenu, contrôlé ou géré par leurs soins dispose de capacités d'interception. Les réseaux ou services sont réputés disposer de ces capacités lorsque les organismes gouvernementaux peuvent intercepter les télécommunications ou services d'une manière leur permettant d'identifier et d'intercepter les seules télécommunications ciblées, d'obtenir les données et contenus associés aux appels (sous une forme exploitable) et d'assurer une interception non obstructive, en temps voulu et efficace, d'une façon qui protège la vie privée des autres utilisateurs de télécommunications, et évite toute immixtion excessive à leur égard. La loi contraint également un opérateur de réseau à fournir les moyens de décrypter toute télécommunication effectuée sur son réseau si ce contenu a été crypté à l'aide d'un système fourni par ses soins.

157. Reconnaissant le fait que la mise en conformité de certains opérateurs de réseau prend du temps et engendre des frais, la loi accorde aux opérateurs concernés un délai de 18 mois à cinq ans (en fonction du statut du réseau) pour intégrer ces capacités. En outre, le Gouvernement a accepté de prendre en charge les frais d'intégration des capacités d'interception au sein des réseaux qui étaient déjà opérationnels à la date d'entrée en vigueur de la loi mais qui ne disposaient pas de ces capacités.

158. Au Brésil, la loi fédérale n° 9.296 de 1996, ainsi que l'article 5 (XII) de la Constitution fédérale de 1988, régissent les écoutes téléphoniques officielles mises en œuvre par les organismes gouvernementaux autorisés. La loi reconnaît le caractère inviolable des télécommunications, mais elle prévoit, sous réserve d'autorisation judiciaire, des dérogations spécifiques aux fins d'enquête criminelle ou de procédure pénale. La loi définit les procédures à suivre dans les cas d'écoutes téléphoniques, qui interviennent sous la supervision d'un juge. Une fois l'écoute effectuée, ses résultats sont transcrits et communiqués au juge, accompagnés d'un résumé de toutes les mesures prises conformément à l'autorisation accordée (art. 6).

159. Pour remplir leurs obligations légales, les entreprises de télécommunications ont dû créer et former des unités spécialisées, et investir dans les technologies nécessaires. En ce qui concerne les frais de mise à disposition des capacités d'interception, il appartient aux entreprises de télécommunications de fournir les ressources techniques et le personnel nécessaires pour faciliter ces activités. Cette approche traduit le fait qu'en application de la Constitution brésilienne les entreprises de télécommunications opèrent dans le cadre d'une concession octroyée par le Gouvernement et que la prestation de services de télécommunications est considérée comme un service public.

160. En Indonésie, après les attentats de Bali en 2002, le Gouvernement a adopté une législation qui autorise, dans le cadre des enquêtes liées au terrorisme, les services de détection, de répression et de sécurité à intercepter et à examiner les informations

qui sont émises, envoyées, reçues ou stockées électroniquement ou au moyen d'un dispositif optique. La question du délai de conservation des fichiers journaux ou des fichiers Internet est régie par la loi n° 11 de 2008 sur les informations et transactions électroniques, et en particulier par l'alinéa *a* du paragraphe 1 de l'article 6, qui impose à chaque système géré par un prestataire de systèmes électroniques de reproduire de manière exhaustive toute information ou document électronique pendant le délai de conservation prévu par la loi.

161. En Algérie, le Gouvernement a adopté en 2006 une loi autorisant la surveillance sonore et vidéo et l'interception de correspondance, sous réserve d'autorisation et d'exécution sous le contrôle direct du procureur. La même loi autorise la technique de l'infiltration aux fins d'enquête sur le terrorisme ou la criminalité organisée, et permet à l'agent infiltré de commettre au cours de l'opération certaines infractions mineures spécifiées. Le secret de l'identité de l'agent est soigneusement protégé par la loi, mais l'opération d'infiltration doit intervenir sous l'autorité du procureur ou du juge d'instruction[107].

162. En Malaisie, la loi de 1998 relative aux communications et au multimédia contient plusieurs dispositions se rapportant à la réglementation de l'Internet et aux enquêtes criminelles connexes. Par exemple, l'article 249 de la loi, qui porte sur l'accès aux données informatiques pendant les perquisitions, dispose que cet accès comprend l'obtention des "mots de passe, codes de cryptage ou de décryptage, logiciels, matériels informatiques ou autres moyens requis pour permettre la compréhension de données informatisées".

163. En outre, le chapitre 4 de la loi, relatif aux questions d'intérêt national, impose aux opérateurs de services Internet l'obligation générale de "faire de leur mieux" pour que les réseaux qu'ils fournissent ne soient pas utilisés pour commettre toute infraction prévue par la loi malaise (art. 263), et dispose que le ministre responsable peut déterminer, en précisant les exigences techniques correspondantes, qu'un titulaire de licence ou une catégorie de titulaires de licence doit mettre en œuvre les capacités permettant l'interception autorisée de communications (art. 265).

164. Le chapitre 2 de la loi se rapporte à la question des contenus offensants, et interdit aux fournisseurs d'applications de contenus et à toute personne utilisant ces services de fournir des contenus qui soient "indécents, obscènes, faux, menaçants ou de nature offensante avec l'intention d'importuner, de tromper, de menacer ou de harceler toute personne" (art. 211). Les personnes enfreignant ces obligations commettent une infraction et sont passibles d'une amende maximale de 50 000 ringgit (environ 16 200 dollars) et/ou d'une peine d'emprisonnement maximale d'un an, ainsi que d'une amende de 1 000 ringgit (environ 325 dollars) pour chaque journée ou partie de journée pendant laquelle l'infraction se poursuit après la condamnation. L'article 212 de la loi prévoit la désignation d'une entité du secteur d'activité chargée d'élaborer d'un code relatif aux contenus.

165. Aux États-Unis, les opérateurs de télécommunications sont actuellement tenus, en vertu de la loi de 1994 intitulée *Communications Assistance to Law Enforcement Act*

[107] Office des Nations Unies contre la drogue et le crime, *Recueil de cas sur les affaires de terrorisme*, par. 215.

(loi sur l'assistance apportée aux services de détection et de répression en matière de communications), de prévoir des capacités d'interception pour les réseaux téléphoniques et à large bande.

c) Réglementation des cybercafés

166. Il apparaît que des terroristes ont, dans certains cas, utilisé des cybercafés pour mener des actions associées au terrorisme; cependant, il n'existe pas de données sur la proportion de ce type d'actions par rapport à l'activité Internet légitime menée via ces services.

167. La mesure dans laquelle les gouvernements devraient réglementer Internet ou les cybercafés pour lutter contre le terrorisme est un point complexe, étroitement lié aux questions de droits de l'homme. À l'échelle internationale, on observe une disparité des méthodes retenues. Dans certains États, dont l'Égypte, l'Inde, la Jordanie et le Pakistan, les gouvernements appliquent des mesures législatives ou réglementaires spécifiques, qui contraignent les opérateurs de cybercafés à obtenir, conserver et, sur demande, communiquer aux services de détection et de répression l'identification photographique, l'adresse et les données d'usage/de connexion de leurs clients.

168. Si les gouvernements peuvent imposer aux opérateurs de cybercafés des obligations visant à limiter la mauvaise utilisation de ces services par les terroristes, l'utilité de ces mesures est discutable, en particulier lorsqu'il existe des dispositifs, tels que d'autres services Internet accessibles au public [par exemple, ordinateurs disponibles dans les bibliothèques publiques ou zones d'accès sans fil à l'Internet (Wi-Fi)], qui offrent des possibilités similaires d'utilisation anonyme par les terroristes. Il convient de noter qu'en 2005 le Gouvernement italien a imposé des obligations réglementaires aux opérateurs de cybercafés en matière d'identification de leurs clients; cependant, cette réglementation a été abolie fin 2010, en raison notamment de préoccupations quant à l'effet qu'elle pourrait avoir sur le développement des services Internet et leur utilisation par les utilisateurs légitimes.

d) Contrôle de contenus

169. La mesure dans laquelle les gouvernements devraient réglementer les contenus relatifs au terrorisme sur l'Internet est une question très controversée. Les manières de procéder sont extrêmement variables, certains États appliquant des contrôles réglementaires stricts aux fournisseurs de services Internet et autres services connexes, et utilisant parfois des technologies destinées à filtrer ou à bloquer l'accès à certains contenus. D'autres États adoptent une approche plus légère, et s'appuient dans une plus grande mesure sur l'autorégulation du secteur de l'information.

170. Dans son article intitulé "Terrorism and the Internet: should web sites that promote terrorism be shut down?"[108], Barbara Mantel relève que "la plupart des fournisseurs d'accès à l'Internet, des sociétés d'hébergement Web, des sites de partage de

[108] Barbara Mantel, "Terrorism and the Internet: should web sites that promote terrorism be shut down?", *CQ Global Researcher*, vol. 3, n° 11 (novembre 2009).

fichiers et de réseau social ont des conditions d'utilisation qui interdisent certains contenus". Elle note par exemple que le service d'hébergement Small Business Web de Yahoo interdit expressément à ses utilisateurs de l'utiliser pour fournir des ressources ou un soutien matériel à toute organisation désignée par le Gouvernement des États-Unis comme organisation terroriste étrangère. Dans cette mesure, il existe un élément d'autorégulation au sein de la société d'information.

171. Lorsqu'ils évaluent la méthode et le niveau d'intervention dans ce domaine, les gouvernements doivent tenir compte d'un certain nombre de facteurs, dont le lieu où le contenu est hébergé, les garanties constitutionnelles ou autres relatives au droit à la liberté d'expression, le contenu lui-même et les implications stratégiques, en matière de renseignement ou de détection et de répression, du contrôle ou de l'infiltration de certains sites ou du fait de les rendre inaccessibles[109].

172. Au Royaume-Uni, l'article 3 de la loi de 2006 contre le terrorisme offre un outil novateur aux autorités chargées des affaires impliquant d'éventuels actes d'incitation sur Internet. Cet article dote la police du pouvoir de délivrer un avis de "retrait" aux personnes associées à la gestion de sites Web ou autres contenus Internet.

173. Cet article 3 s'applique aux affaires concernant les infractions visées à l'article 1 ou 2 de cette loi dans lesquelles "*a)* une déclaration est publiée ou amenée à être publiée dans le cadre de la prestation ou l'utilisation d'un service fourni électroniquement, ou relativement à celle-ci; ou *b)* des actes relevant de l'article 2 2) [diffusion d'une publication terroriste] ont été commis dans le cadre de la prestation ou l'utilisation d'un tel service, ou relativement à celle-ci".

174. L'article 3 2) dispose que, si la personne à laquelle l'avis a été signifié ne supprime pas le contenu lié au terrorisme, et qu'elle est par la suite accusée des infractions visées à l'article 1 ou 2 de la loi de 2006 contre le terrorisme au titre de ce contenu, il existe au procès une présomption simple qu'elle l'approuvait.

175. Malgré l'existence de ces avis "de retrait" préventifs, ce pouvoir n'a pas encore été utilisé en pratique. Dans la plupart des cas, en particulier lorsque le contenu offensant est hébergé sur des sites Web tiers, il enfreint les conditions d'utilisation du prestataire de services, et les autorités réussissent à en négocier le retrait. En fait, au Royaume-Uni, une cellule spécialisée, la Counter Terrorism Internet Referral Unit, coordonne les réponses nationales aux signalements effectués par le public, le Gouvernement et le secteur d'activité, concernant les contenus Internet liés au terrorisme, et fait office de source centrale et dédiée de conseil aux services de police.

4. Coopération internationale

176. Les États sont tenus, en vertu de nombreux instruments internationaux, régionaux, multilatéraux et bilatéraux relatifs au terrorisme et à la criminalité transnationale

[109] Catherine A. Theohary et John Rollins, "Terrorist use of the Internet: information operations in cyberspace", rapport du Congressional Research Service (8 mars 2011), p. 8.

organisée, d'établir des politiques et des cadres législatifs pour faciliter la coopération internationale en matière d'enquête et de poursuite concernant ce type d'affaires.

177. Outre les politiques et les lois établissant les infractions pénales nécessaires pour répondre aux exigences de double incrimination, les États devraient adopter une législation globale qui offre aux autorités nationales un fondement juridique de coopération internationale avec leurs homologues étrangères dans les enquêtes transnationales relatives au terrorisme. Dans les affaires impliquant l'utilisation d'Internet, il est très probable qu'une coopération internationale efficace, comprenant la capacité à partager des informations, et notamment des données liées à Internet, constitue un facteur clef du succès des poursuites pénales.

178. Nous aborderons de façon plus détaillée les questions relatives à la coopération internationale dans les affaires de terrorisme au chapitre V.

IV. Enquêtes et collecte de renseignements

A. Outils utilisés pour commettre des infractions terroristes impliquant Internet

179. Les progrès technologiques ont offert aux terroristes de nombreux moyens sophistiqués d'utiliser l'Internet à des fins illicites. Pour être efficaces, les enquêtes sur l'activité Internet associent les méthodes d'investigation classiques, la connaissance des outils permettant de mener une activité illicite via l'Internet et l'élaboration de pratiques visant à identifier, appréhender et poursuivre les auteurs de tels actes.

180. Une affaire jugée en France illustre la manière dont différents types de techniques d'enquête, à la fois traditionnelles et se rapportant spécifiquement aux preuves numériques, sont employés de concert pour réunir les preuves nécessaires aux poursuites concernant l'utilisation d'Internet par des terroristes.

***Ministère public* c. *Arnaud, Badache, Guihal* et al.**

Cette affaire concerne Rany Arnaud, Nadir Zahir Badache, Adrien Luciano Guihal et Youssef Laabar, qui ont été déclarés coupables par le tribunal de grande instance de Paris le 26 janvier 2012 et condamnés à des peines de 18 mois à six ans d'emprisonnement pour avoir, entre autres, diffusé des documents liés au terrorisme.

Arnaud, Badache et Guihal ont été arrêtés en France en décembre 2008 après la diffusion par Arnaud, opérant sous le pseudonyme "Abdallah", de messages appelant au djihad contre la France sur un site Web de propagande, minbar-sos.com:

> "N'oubliez pas que la France continue de combattre nos frères en Afghanistan et vous êtes dans une dar ul-harb, accourrez au martyr dès que vous le pouvez, boycottez leur économie, dillapidez leurs richesses, ne participez pas a leur économie et au financement de leur armée". [orthographe respectée]

À la suite de ce message, les autorités ont intercepté le compte Internet d'Arnaud, placé l'individu sous surveillance et mis sur écoute sa ligne téléphonique. Après avoir arrêté Arnaud, les enquêteurs ont procédé à l'examen criminalistique du contenu des ordinateurs qu'il utilisait et ont découvert qu'il avait effectué des recherches sur des questions relatives à la commission d'actes terroristes, et qui concernaient par exemple les produits susceptibles d'être utilisés pour fabriquer des explosifs et des engins incendiaires, la détermination de cibles éventuelles et le repérage des activités d'une société qui utilisait du nitrate d'ammonium. L'enquête a révélé qu'Arnaud avait recruté Guihal et Badache, participé à des rendez-vous et discussions préparatoires sur le projet d'un attentat, pris contact avec des personnes impliquées dans des mouvements djihadistes pour qu'elles l'aident à mettre son

projet à exécution et reçu des fonds pour financer ce dernier. Ces actes constituaient des infractions aux termes des articles 421-2-1, 421-1, 421-5, 422-3, 422-6 et 422-7 du Code pénal français, et des articles 203 et 706-16 et suivants du Code de procédure pénale.

Le tribunal a jugé que le plan auquel M. Arnaud avait prétendument pris part, en association avec les autres délinquants, et qui consistait à placer des explosifs sur un camion devant exploser lorsqu'il atteindrait la cible, présentait une menace particulièrement importante pour l'ordre public. Arnaud a donc été condamné à une peine de six ans d'emprisonnement pour participation à une association de malfaiteurs en vue de la préparation d'un acte de terrorisme, détention frauduleuse de plusieurs faux documents et usage de faux documents administratifs constatant un droit, une identité ou une qualité ou accordant une autorisation. Sur le même chef d'accusation, M. Badache a été condamné à deux ans de prison, dont six mois avec sursis, et M. Guihal à quatre ans, dont un an avec sursis. M. Laabar, qui était jugé pour d'autres actes connexes, a été condamné à 18 mois d'incarcération.

181. Les enquêtes et les poursuites dans les affaires impliquant des preuves numériques nécessitent des compétences spécialisées en matière d'enquêtes criminelles, ainsi qu'une expertise, des connaissances et une expérience permettant d'appliquer ces compétences dans un environnement virtuel. La recevabilité des preuves est *in fine* une question de droit, et relève donc de la compétence du procureur, mais les enquêteurs devraient être au fait des exigences juridiques et procédurales applicables en matière de recevabilité dans le cadre des enquêtes nationales et internationales. Une bonne connaissance des règles de preuve applicables, concernant en particulier les preuves numériques, favorise la collecte d'éléments suffisants et recevables pour assurer le succès des poursuites. Par exemple, les procédures utilisées pour recueillir, préserver et analyser les preuves numériques doivent garantir qu'une "chaîne de conservation" bien établie desdites preuves a été mise en place dès leur obtention, et que celles-ci n'ont pu être altérées entre leur saisie et leur production finale au tribunal[110].

1. Communication sur Internet

a) Voix sur IP

182. Depuis 10 ans, la popularité et la sophistication des applications permettant aux utilisateurs de communiquer en temps réel en recourant à la voix sur IP (VoIP), ou encore à la discussion vidéo ou texte se sont accrues. Certaines de ces applications offrent des fonctions pointues de partage d'informations, et permettent par exemple aux utilisateurs de partager leurs fichiers ou de visualiser à distance et en temps réel l'activité de l'écran d'un autre utilisateur. La VoIP, en particulier, est de plus en plus utilisée pour communiquer via l'Internet. Parmi les prestataires connus de ce type de services, on peut citer Skype et Vonage, qui convertissent le son analogique en format

[110]Voir, par exemple, Association of Chief Police Officers (Royaume-Uni), *Good Practice Guide for Computer-Based Electronic Evidence*. Disponible à l'adresse: www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf.

numérique et compressé, et permettent le transfert de paquets d'informations numériques via l'Internet, à l'aide d'une bande passante relativement faible.

183. Puisque la téléphonie VoIP implique la transmission de paquets de données numériques, et non de signaux analogiques, et que les prestataires de services facturent généralement les abonnés en fonction de leur volume total de données, les appels VoIP interordinateurs ne sont pas facturés à l'appel, à l'inverse de ce qui se pratique pour les appels de téléphonie fixe ou mobile classiques. Cette différence peut avoir des effets significatifs sur les enquêtes, car les services de détection et de répression ont plus de difficultés à corroborer les communications VoIP avec certains marqueurs relatifs, par exemple, à la date et à l'heure de l'appel et à la situation géographique des participants. Cependant, d'autres indicateurs comme les dates et le volume de trafic de données Internet permettent parfois d'identifier les auteurs d'activités illicites sur Internet (voir par. 205 ci-dessous). Par ailleurs, si l'émetteur et le destinataire des appels téléphoniques conventionnels peuvent être retracés via des commutateurs de ligne fixe ou des relais de communication cellulaire permettant leur géolocalisation, les communications VoIP qui reposent entièrement sur Internet et s'effectuent par exemple via les réseaux sans fil, posent parfois des difficultés dans le contexte d'une enquête. Parmi les autres facteurs de complexité découlant de l'utilisation de la technologie VoIP, on peut citer, entre autres, l'acheminement d'appels via les réseaux pair à pair et le cryptage des données d'appel (ces points seront abordés de manière plus détaillée à la section IV.A.2 ci-dessous)[111].

184. Toutefois, les demandes d'information dûment soumises aux prestataires de services VoIP peuvent permettre d'obtenir de précieuses données d'identification telles que l'adresse IP, l'adresse de courrier électronique ou les données de paiement d'une personne.

b) Courriers électroniques

185. Les services de courrier électronique sur le Web offrent également aux terroristes un moyen de communication clandestin, qui peut être détourné à des fins illicites. Les courriers électroniques échangés entre les parties contiennent généralement un certain nombre d'éléments utiles dans le cadre d'une enquête. Un courrier électronique type est composé de l'en-tête de l'enveloppe, de l'en-tête du message, du corps du message et des pièces jointes. En fonction des paramètres du logiciel concerné, seule une version abrégée de l'en-tête de l'enveloppe est parfois affichée, mais l'en-tête complet contient généralement un enregistrement de tous les serveurs par lesquels le message a transité jusqu'à son destinataire final, ainsi que des informations concernant l'adresse IP de l'expéditeur[112]. Les informations contenues dans l'en-tête de l'enveloppe sont moins susceptibles d'altération (bien qu'elles ne soient pas totalement imperméables) que celles figurant dans l'en-tête du message, qui sont généralement fournies par l'utilisateur dans des champs comme "De", "À", "Voie de retour", "Date" et "Heure", tels qu'affichés sur l'ordinateur à partir duquel le message est envoyé[113].

[111] Soumission écrite de l'expert du Raggruppamento Operativo Speciale des Carabinieri (Italie).

[112] États-Unis, Ministère de la justice, Office of Justice Programs, National Institute of Justice, *Investigations Involving the Internet and Computer Networks* (2007), p. 18 sq.

[113] Ibid., p. 20.

186. Parmi les autres techniques couramment utilisées pour limiter les traces électroniques d'échanges entre les parties, et donc la probabilité de détection, on peut citer les communications via des messages sauvegardés et non envoyés dans le dossier Brouillons du compte de messagerie électronique. Ces informations sont alors à la disposition des diverses parties qui utilisent un mot de passe partagé pour accéder au compte. D'autres mesures peuvent également être prises pour éviter la détection, par exemple, l'utilisation d'un terminal d'accès public à distance, comme un cybercafé, pour accéder au brouillon du message. Cette méthode a été utilisée dans le cadre des attentats terroristes de Madrid en 2004.

187. Relativement aux communications par courrier électronique, on peut aussi avoir recours à des techniques d'anonymisation (abordées de manière plus détaillée dans la section IV.A.2 ci-dessous), en déguisant par exemple l'adresse IP associée à l'expéditeur d'un courrier électronique. On peut également utiliser des serveurs d'anonymisation, qui suppriment les informations d'identification de l'en-tête de l'enveloppe avant de transmettre le message au serveur suivant.

L'importance de la coopération internationale dans les enquêtes sur les activités menées sur Internet et liées au terrorisme

L'expert du Raggruppamento Operativo Speciale (Groupe d'opérations spéciales) des Carabinieri (Italie) a souligné le rôle déterminant qu'avaient eu la coopération internationale et les techniques spécialisées dans l'enquête menée sur l'utilisation d'Internet à des fins terroristes par le Parti-Front de libération du peuple révolutionnaire (DHKP-C), une organisation extrémiste turque. Une étroite collaboration entre les agents des services de détection et de répression en Turquie et en Italie a permis aux enquêteurs italiens d'identifier les techniques de cryptage et les autres mesures de sécurité des données utilisées par les membres du DHKP-C pour échanger des informations à des fins terroristes, notamment les services de courrier électronique. En particulier, les membres du DHKP-C utilisaient le logiciel de sténographie Camouflage pour dissimuler des données dans des images de fichiers JPEG et GIF, ainsi que le logiciel WinZip pour crypter des fichiers, qui figuraient en pièces jointes des courriers électroniques (voir la section IV.A.2 ci-dessous). Les enquêteurs italiens ont intercepté ou obtenu d'une autre manière les mots de passe de cryptage, et identifié les programmes leur permettant de déchiffrer les communications. Pour obtenir des preuves numériques à partir des ordinateurs d'un suspect, ils ont effectué une analyse criminalistique de ces ordinateurs à l'aide du logiciel EnCase (voir la section IV.C ci-dessous) et ont eu recours à des techniques d'enquête traditionnelles. Les résultats de cette enquête, ainsi qu'une coopération transfrontalière de grande ampleur, ont conduit à l'arrestation, en avril 2004, de 82 suspects en Turquie et de 59 suspects en Allemagne, en Belgique, en Grèce, en Italie et aux Pays-Bas.

c) Services de messagerie en ligne et forums de discussion

188. Les services de messagerie en ligne et les forums de discussion fournissent d'autres moyens de communiquer en temps réel, avec des degrés variables d'anonymat.

Les services de messagerie en ligne concernent généralement les communications bilatérales, alors que les forums de discussion permettent à des groupes d'individus de communiquer. L'inscription aux services de messagerie en ligne repose généralement sur des informations non vérifiées, fournies par l'utilisateur; cependant, certains services Internet enregistrent aussi l'adresse IP utilisée au moment de l'inscription, qui, sous réserve des garanties légales applicables, peut être demandée par les autorités de détection et de répression. Les communications sont généralement identifiées par un nom d'utilisateur unique, qui est attribué de façon permanente lors de l'inscription ou limité à une session donnée. Les informations partagées au cours d'une session de messagerie en ligne ne sont généralement pas enregistrées par le prestataire de services et sont donc impossibles à extraire une fois la session terminée, sous réserve de récupération facilitée par l'analyse criminalistique du disque dur d'un participant.

189. Les organisations terroristes et leurs sympathisants utilisent parfois des forums de discussion en ligne protégés par mot de passe pour créer un sentiment de communauté dans un environnement mondial. Le prestataire de services est davantage en mesure de contrôler et de conserver les messages échangés sur les forums de discussion que les messages bilatéraux, ce qui augmente les chances d'obtenir des preuves documentaires au cours des enquêtes[114]. Dans certains pays, un agent des services de détection et de répression peut, dans le cadre d'une enquête et dans certaines conditions, enregistrer clandestinement des discussions sur les forums et y participer sous un pseudonyme.

190. En France, par exemple, l'article 706 du Code de procédure pénale prévoit que le procureur ou le juge d'instruction peut autoriser de telles opérations d'infiltration relativement aux infractions commises par le biais de communications électroniques (voir discussion à la section III.C.3 *a*). Ces opérations peuvent notamment avoir pour but de réunir des renseignements ou de prendre d'autres mesures proactives relativement à une menace terroriste perçue. Cependant, il convient de veiller, au début de l'opération, à ce que l'infiltration de forum en ligne ou toute autre discussion sur Internet intervienne de telle manière que la défense ne puisse invoquer un moyen de provocation policière, en soutenant qu'une autorité gouvernementale aurait incité un suspect à commettre une infraction qu'il n'était pas prédisposé à commettre.

d) Réseaux de partage de fichiers et technologie en nuage ("cloud technology"*)*

191. Les sites Web de partage de fichiers, tels que Rapidshare, Dropbox ou Fileshare, offrent aux parties la possibilité de télécharger, partager, localiser et consulter sans difficulté des fichiers multimédias via l'Internet. Les techniques de cryptage et d'anonymisation employées pour d'autres formes de communication sur Internet sont, de la même façon, applicables aux fichiers partagés via, entre autres, les technologies pair-à-pair (P2P) et de protocole de transfert de fichiers (FTP). Dans l'affaire *Hicheur* (voir par. 20 ci-dessus), par exemple, l'accusation a produit des preuves montrant que les

[114] Ibid., pages 34 et suivantes.

fichiers numériques servant aux activités terroristes étaient partagés via Rapidshare, après avoir été cryptés et compressés pour des raisons de sécurité. Certains réseaux de partage de fichiers conservent des journaux de transfert ou des informations de paiement, qui peuvent être utiles dans le contexte d'une enquête.

192. L'informatique en nuage permet aux utilisateurs d'accéder à distance aux données et programmes stockés ou exécutés sur des serveurs de données tiers. Comme le partage de fichiers, l'informatique en nuage offre un moyen pratique de stocker, de partager et de diffuser en toute sécurité des informations en ligne. L'utilisation de cette technologie pour accéder à des informations stockées à distance réduit le volume de données conservées localement sur des ordinateurs individuels, et diminue parallèlement la capacité à récupérer des preuves éventuelles dans le cadre d'une enquête relative à l'utilisation d'Internet par des terroristes.

193. Il arrive que les serveurs de données utilisés pour fournir ces services soient physiquement situés dans un autre pays que celui de l'utilisateur inscrit, pays dans lequel le niveau de réglementation et les moyens de détection et de répression sont différents. Une étroite coordination avec les autorités locales de détection et de répression peut donc s'avérer nécessaire pour obtenir des preuves essentielles dans le cadre d'une procédure judiciaire.

2. Techniques de cryptage de données et d'anonymisation

194. Le cryptage de données consiste à protéger des informations numériques contre la divulgation en les convertissant en cryptogrammes, à l'aide d'un algorithme mathématique et d'une clef de cryptage, afin que seul leur destinataire puisse les comprendre. Les outils de cryptage peuvent se présenter sous forme de matériel, de logiciel ou d'une combinaison des deux. Une fois les informations cryptées, un mot de passe, une phrase de passe, une "clef logicielle", un système d'accès physique, ou une combinaison de ces éléments, est requis pour y accéder. Le cryptage est parfois employé concernant à la fois les données "statiques", contenues dans des dispositifs de stockage, comme des disques durs d'ordinateurs, des supports flash et des téléphones intelligents, et les données "en transit", transmises sur Internet, par exemple via des communications VoIP ou par courrier électronique. Parmi les exemples d'outils logiciels de cryptage courants, on peut citer ceux qui sont intégrés dans les systèmes ou applications d'exploitation des ordinateurs, ainsi que les logiciels autonomes comme Pretty Good Privacy et WinZip[115]. Au Brésil, une enquête a été ouverte sur la base d'une opération de coopération internationale et de partage d'informations à l'encontre d'un suspect qui était présumé participer aux activités d'un site Web djihadiste affilié à des organisations terroristes reconnues, dont Al-Qaida, et modérer et contrôler ces activités. Ce site Web hébergeait des vidéos, des textes et des messages de leaders extrémistes, qui avaient été traduits en anglais pour atteindre un public plus large, et qui étaient également utilisés pour collecter des fonds et mener des campagnes de propagande à caractère raciste.

[115] États-Unis, Ministère de la justice, Office of Justice Programs, National Institute of Justice, *Investigative Uses of Technology: Devices, Tools and Techniques* (2007), p. 50.

L'opération policière ayant conduit à l'arrestation du suspect visait à le surprendre pendant qu'il était connecté à l'Internet et qu'il se livrait à des activités relatives au site Web. En appréhendant le suspect alors que son ordinateur était allumé et que les fichiers pertinents étaient ouverts, les enquêteurs ont pu contourner les clefs symétriques cryptographiques et autres paramètres de cryptage et de sécurité utilisés par le suspect et ses associés. Les enquêteurs ont donc pu accéder à des contenus numériques qui auraient été indisponibles ou plus difficiles à obtenir s'ils s'étaient procuré l'ordinateur une fois celui-ci éteint.

195. Il est également possible de dissimuler l'activité sur Internet, ou l'identité des utilisateurs associés, à l'aide de techniques de pointe, notamment en masquant l'adresse IP source, en usurpant l'adresse IP d'un autre système ou en redirigeant le trafic Internet vers une adresse masquée[116]. Un serveur mandataire permet aux utilisateurs de créer des connexions indirectes vers d'autres services de réseau. Certains serveurs mandataires permettent de configurer le navigateur d'un utilisateur pour acheminer automatiquement le trafic de ce navigateur via un serveur mandataire. Le serveur mandataire demande les services de réseau pour le compte de l'utilisateur, puis achemine les résultats via un nouveau mandataire. L'utilisation de serveurs mandataires peut favoriser divers niveaux d'anonymat. Un serveur mandataire peut masquer l'identité d'un utilisateur en effectuant les requêtes de services de réseau sans révéler l'adresse IP d'où elles proviennent, ou en fournissant intentionnellement une adresse IP faussée. Par exemple, on peut utiliser des applications comme The Onion Router pour protéger l'anonymat des utilisateurs en réacheminant automatiquement l'activité Internet via un réseau de serveurs mandataires pour en masquer l'origine. Le réacheminement du trafic du réseau via de multiples serveurs mandataires, éventuellement situés dans différents pays, complique l'identification de l'initiateur d'une transmission.

196. Par ailleurs, un suspect peut pirater l'adresse IP d'une organisation légitime et naviguer sur Internet en utilisant cette adresse. Toute trace de cette activité sera alors reliée à l'adresse IP de l'organisation compromise. Un suspect peut également accéder à un site Web par l'intermédiaire d'un ordinateur compromis ou stocker un logiciel malveillant (utilisé, par exemple, pour obtenir des coordonnées de carte de crédit ou d'autres informations financières à caractère personnel) sur des sites Web compromis pour éviter d'être identifié.

197. De nombreux logiciels permettent de dissimuler ou de crypter des données transmises sur Internet à des fins illicites. Parmi ces programmes, on peut citer des logiciels tels que Camouflage, qui masque les informations grâce à la stéganographie, ou WinZip, qui crypte les fichiers et les protège par mot de passe. De multiples strates de protection des données peuvent également être employées. Par exemple, Camouflage permet de cacher un fichier en le cryptant et en le joignant à la fin d'un fichier choisi. Ce fichier de couverture conserve ses propriétés initiales, mais est utilisé comme transporteur pour stocker ou transmettre le fichier caché. Ce logiciel peut être utilisé avec

[116] National Institute of Justice, *Investigations Involving the Internet and Computer Networks*, p. 9.

un large éventail de types de fichiers. Cependant, l'examen des données brutes peut permettre de détecter le fichier caché, en montrant l'existence du fichier annexé[117].

198. Au Royaume-Uni, la loi de 2000 portant réglementation des pouvoirs d'enquête confère le caractère d'infraction pénale au fait de refuser de remettre une clef de cryptage sur demande. Cependant, il convient de veiller à ce que les suspects ne tentent pas de contourner cette disposition en utilisant plusieurs strates de cryptage et de multiples clefs pour protéger les différents ensembles de données. Par exemple, un paramètre de TruCrypt, un outil de cryptage gratuit et courant, permet à un suspect de crypter un disque dur et de créer deux mots de passe: l'un pour le disque "propre" et l'autre pour celui contenant le matériel illicite. On peut faire échouer cette tentative en recherchant, lors de l'examen criminalistique du disque dur, s'il existe un "volume manquant" de données. En outre, les infractions de cette nature sont généralement des délits mineurs, passibles de peines maximales de six mois d'emprisonnement. Au Royaume-Uni, cependant, lorsque l'affaire touche à des questions de sécurité nationale, la peine maximale encourue est portée à deux ans d'emprisonnement.

3. Technologie sans fil

199. La technologie de réseau sans fil permet aux ordinateurs et autres appareils d'accéder à Internet à l'aide d'un signal radio, et non d'une connexion câblée. Pour accéder à un réseau Wi-Fi, une certaine proximité avec les ressources du réseau est nécessaire, qui dépend de la puissance du signal sans fil. Les réseaux sans fil sont configurés pour autoriser un accès libre à l'Internet, sans enregistrement, ou sont sécurisés par une phrase de passe ou divers niveaux de cryptage. Il est souvent possible d'accéder aux réseaux sans fil enregistrés au nom de particuliers, d'entreprises ou d'organismes publics à partir de lieux publics. En accédant de façon anonyme à des réseaux Wi-Fi sécurisés ou non, les délinquants parviennent à dissimuler les liens entre leur activité Internet et leurs données d'identification.

200. En outre, on a vu apparaître ces dernières années des prestataires de services comme Fon, qui permettent aux utilisateurs enregistrés de partager une partie de la bande passante Wi-Fi de leur domicile avec d'autres abonnés, en échange d'un accès réciproque au réseau Wi-Fi des abonnés du monde entier. Au cours d'une enquête, l'activité menée sur un réseau Wi-Fi partagé complique de manière significative le processus d'attribution d'un acte à un auteur unique et identifiable[118].

201. Une technique originale concerne l'utilisation de récepteurs radio à haute fréquence (HF) très performants et définis par un logiciel, acheminés via un ordinateur. De cette façon, aucune donnée n'est échangée par le biais d'un serveur et aucun journal n'est créé. Les services de détection, de répression et de renseignement ont plus de difficultés à intercepter des communications échangées de cette façon, en termes tant de localisation des transmetteurs que de prévision en temps réel de la fréquence utilisée pour transmettre les communications.

[117] Soumission écrite de l'expert du Raggruppamento Operativo Speciale des Carabinieri (Italie).

[118] Ibid.

B. Enquêtes sur les affaires terroristes impliquant Internet

1. Approche systématique des enquêtes impliquant l'Internet

202. Dans le cadre d'une enquête visant à lutter contre l'utilisation d'Internet par des terroristes, il est possible d'utiliser un large éventail de données et de services disponibles en ligne. Une approche proactive des stratégies d'enquête et des outils spécialisés connexes, qui tire parti des ressources en constante évolution d'Internet, favorise l'identification efficace des données et des services les plus utiles à l'enquête. Reconnaissant la nécessité d'une méthode systématique d'utilisation des progrès techniques en matière d'Internet, le Raggruppamento Operativo Speciale des Carabinieri (Italie) a élaboré les lignes directrices suivantes, qui ont été diffusées via le programme de maîtrise en informatique criminalistique et cybercriminalité de l'University College Dublin (voir la section IV.G ci-dessous) et mises en œuvre par les services de détection et de répression de nombreux États membres de l'Organisation internationale de police criminelle (INTERPOL) et de l'Office européen de police (Europol).

Protocole d'approche systématique

- *Collecte de données*: cette phase concerne la collecte de certaines données par des méthodes d'enquête traditionnelles, telles que les informations relatives au suspect, aux personnes qui vivent avec lui, à ses collègues ou autres associés et les informations réunies lors d'activités conventionnelles de surveillance des canaux de communication, notamment téléphones fixes et mobiles.
- *Recherche d'autres informations disponibles via les services sur Internet*: cette phase nécessite la présentation de requêtes visant à obtenir des informations collectées et stockées dans les bases de données des services Web de commerce électronique, de communication et de réseau, comme eBay, PayPal, Google et Facebook, ainsi que l'utilisation de moteurs de recherche dédiés, tels que www.123people.com. Les données recueillies par ces services à l'aide des "cookies" fréquemment utilisés fournissent également des informations essentielles dans les cas d'ordinateur ou d'appareil mobile utilisé par plusieurs utilisateurs.
- Les activités menées lors de ces deux phases permettent d'obtenir des informations qui peuvent être combinées et croisées pour créer un profil de la personne ou du groupe objet de l'enquête et qui pourront être analysées à un stade ultérieur de l'enquête.
- *Requêtes auprès de serveurs VoIP*: au cours de cette phase, les autorités de détection et de répression demandent aux prestataires de services VoIP des informations relatives aux personnes objet de l'enquête et à tout membre ou utilisateur connu du même dispositif de mise en réseau. Les informations ainsi recueillies peuvent également être utilisées comme "filtre intelligent" pour vérifier les informations obtenues lors des deux phases antérieures.
- *Analyse*: le gros volume de données obtenues auprès des serveurs VoIP et des fournisseurs des divers services Internet est alors analysé pour déterminer les informations et tendances utiles à l'enquête. Cette analyse est parfois facilitée par des programmes informatiques capables de filtrer les informations ou de fournir des représentations graphiques des données numériques recueillies pour faire ressortir, entre autres, les

tendances, la chronologie, l'existence d'un groupe organisé ou d'une hiérarchie, la géolocalisation des membres de ce groupe, ou les facteurs communs à plusieurs utilisateurs (par exemple source de financement).

- *Détermination des thèmes intéressants*: après une analyse intelligente des données, il est courant d'identifier des thèmes intéressants, sur la base, par exemple, des informations d'abonnés liées à un compte financier, VoIP ou de courrier électronique.
- *Activité d'interception*: au cours de cette phase, les autorités de détection et de répression emploient des tactiques d'interception similaires à celles qui sont utilisées dans le cadre des voies de communication traditionnelles, en les réorientant vers une plate-forme différente: les canaux de communication numériques. L'activité d'interception peut être mise en œuvre concernant les services de télécommunications (large bande de ligne fixe, large bande mobile et communications sans fil), ainsi que les services fournis par les FAI (courriers électroniques, discussions et communications sur forums). En particulier, l'expérience des dernières années a révélé certaines faiblesses des nouvelles technologies de communication qui peuvent être exploitées à des fins d'enquête ou de collecte de renseignements. Il convient de veiller à l'intégrité criminalistique des données collectées et à la corroboration, dans la mesure du possible, des renseignements recueillis, à l'aide d'identificateurs objectifs tels que les coordonnées GPS, les horodateurs ou la vidéosurveillance.

Lorsque le droit national l'autorise, les autorités de détection et de répression emploient également des techniques de surveillance numérique facilitées par l'installation de matériel informatique ou d'applications telles qu'un virus, un "cheval de Troie" ou un enregistreur de frappe sur l'ordinateur du suspect. Elles peuvent y parvenir en accédant directement ou à distance à l'ordinateur, et en tenant compte du profil technique du matériel à compromettre (tel que la présence de protections antivirus ou de pare-feu) et du profil personnel de l'ensemble des utilisateurs de l'ordinateur, afin de cibler le profil le moins sophistiqué.

203. Les services de police coréens ont réagi à la nécessité de normaliser les pratiques nationales en matière de criminalistique numérique en élaborant et en mettant en œuvre deux manuels respectivement intitulés *Standard Guidelines for Handling Digital Evidence* et *Digital Forensics Technical Manual*. Le premier détaille sept étapes de gestion des preuves numériques: préparation, collecte, examen, demande/réception/transport de preuves, analyse, présentation de rapports, et préservation/gestion des preuves. Le second expose les procédures requises et les méthodes appropriées de collecte de preuves numériques, concernant notamment la création de l'environnement, des outils et de l'équipement criminalistiques appropriés, les mesures préparatoires comme la configuration du matériel informatique et des logiciels, les connexions au réseau et la précision temporelle, les mesures visant à obtenir le maximum de preuves numériques, l'analyse indépendante de données sécurisées, et la production du rapport final[119].

2. *Identification d'une adresse IP*

204. L'adresse IP associée à une communication Internet constitue un élément d'identification important, et est donc essentielle dans les enquêtes relatives à l'utilisation

[119] Soumission écrite de l'expert de la République de Corée.

d'Internet par des terroristes. Une adresse IP permet d'identifier le réseau et l'ordinateur utilisés pour accéder à l'Internet. Les adresses IP peuvent être dynamiques (attribuées temporairement pour la durée d'une session en ligne à partir d'un ensemble d'adresses mises à disposition d'un FAI) ou statiques (attribuées de manière fixe, comme les adresses de sites Web). Les adresses IP dynamiques sont généralement affectées aux FAI au sein de blocs organisés par régions. Par conséquent, en l'absence de recours à des techniques d'anonymisation ou autres, on peut souvent utiliser une adresse IP dynamique pour identifier la région ou l'État dans lequel un ordinateur se connecte à Internet.

205. En outre, en réponse à une requête dûment présentée, un FAI est généralement en mesure d'identifier celui de ses comptes d'abonnés qui est associé à une adresse IP à un moment donné. On peut alors utiliser des méthodes d'enquête traditionnelles pour identifier la personne qui contrôle physiquement le compte d'abonné à ce moment précis. Dans l'affaire *Hicheur* (voir par. 20 ci-dessus), les enquêteurs ont pu déterminer l'identité de l'accusé en identifiant l'adresse IP statique utilisée pour accéder à un compte de courrier électronique sous surveillance. Une requête présentée au FAI concerné a permis aux autorités de relier l'adresse IP à un compte d'abonné utilisé par plusieurs occupants d'un logement, dont l'accusé. En interceptant le trafic de données relatif à ce compte d'abonné, les enquêteurs ont également pu établir des liens entre l'adresse IP et l'activité sur un site Web prodjihadiste qui, entre autres, diffusait du matériel aux fins d'entraînement physique et mental de combattants extrémistes. En particulier, les enquêteurs ont pu mettre en corrélation les moments où plusieurs connexions au forum de discussion du site Web intervenaient, et l'augmentation concomitante du volume de données Internet liées au compte personnel de courrier électronique de l'accusé[120].

206. Compte tenu de l'importance du facteur temps dans les enquêtes impliquant l'Internet et du risque d'altération ou de suppression des données numériques dû, entre autres, aux éventuelles contraintes de capacité du serveur du FAI concerné ou de la réglementation sur la protection des données applicable, il convient d'examiner l'opportunité d'une requête au FAI pour préserver les données pertinentes pour l'enquête criminelle, en attendant la mise en œuvre des mesures nécessaires à l'obtention des données à des fins probatoires.

207. Dans le cas d'une enquête relative à un site Web, le nom de domaine pertinent doit d'abord être réduit à une adresse IP. Afin d'identifier l'adresse IP associée, qui est enregistrée auprès de l'Internet Corporation for Assigned Names and Numbers (ICANN), on peut utiliser plusieurs utilitaires dédiés. Les utilitaires courants, disponibles sur Internet, sont notamment "whois" et "nslookup"[121]. À titre d'exemple, une requête whois liée au nom de l'Office des Nations Unies contre la drogue et le crime (www.unodc.org) donne les résultats suivants:

[120] Jugement du 4 mai 2012, affaire n° 0926639036 du tribunal de grande instance de Paris (14e chambre/2), pages 7 et suivantes.

[121] National Institute of Justice, *Investigations Involving the Internet and Computer Networks*, p. 10.

Identifiant de domaine: D91116542-LROR
Nom de domaine: UNODC.ORG
Créé le: 11-Oct-2002 09:23:23 UTC
Dernière mise à jour le: 19-Oct-2004 00:49:30 UTC
Date d'expiration: 11-Oct-2012 09:23:23 UTC
Bureau d'enregistrement: Network Solutions LLC (R63-LROR)
Statut: TRANSFERT CLIENT INTERDIT
Identifiant du déposant: 15108436-NSI
Nom du déposant: Wiessner Alexander
Organisation du déposant: Nations Unies Vienne
Adresse 1 du déposant: Vienna International Centre, P.O. Box 500
Ville du déposant: A-1400 Wien Vienne AT 1400
Code postal du déposant: 99999
Pays du déposant: AT
Numéro de téléphone du déposant: +43.1260604409
Numéro de fax du déposant: +43.1213464409
Adresse électronique du déposant: noc@unVienne.org

Toutefois, ces renseignements sont fournis par le déposant. Dès lors, d'autres mesures peuvent s'avérer nécessaires pour vérifier leur exactitude en toute indépendance. Les domaines peuvent également être loués ou être autrement placés sous le contrôle d'une autre partie que le déposant.

208. Les personnes qui enquêtent sur l'utilisation d'Internet à des fins terroristes doivent également être conscientes du fait que l'activité en ligne relative à une enquête peut être surveillée, enregistrée et reconstituée par des tiers. Par conséquent, il faut éviter de faire des demandes de renseignements en ligne à partir d'ordinateurs permettant de remonter à l'organisation chargée de l'enquête[122].

3. Utilitaires et matériels d'enquête spécialisés

209. Les enquêteurs dotés des compétences techniques appropriées disposent de toute une gamme d'utilitaires et de matériels informatiques spécialisés. Certains, comme "Ping" ou "Traceroute", peuvent être intégrés dans le système d'exploitation d'un ordinateur suspect. Avec Ping, par exemple, on peut envoyer un signal à un ordinateur connecté à Internet pour déterminer s'il est connecté à un moment donné, sous réserve de perturbations causées par un pare-feu ou une autre configuration de réseau. De même, Traceroute permet d'afficher le chemin entre deux ordinateurs en réseau, ce qui peut contribuer à déterminer leur localisation physique.

210. Parmi les autres programmes susceptibles, sous réserve des lois et règlements internes, d'être utilisés concernant, entre autres, l'accès à l'ordinateur et l'interception de communications, on peut citer les "chevaux de Troie" ou "chevaux de Troie

[122] Ibid.

d'administration à distance" (*Remote Administration Trojans*, RAT), qui sont introduits clandestinement dans un système informatique pour collecter des informations ou contrôler à distance la machine compromise. Il est également possible d'installer sur un ordinateur des outils de contrôle de clavier et de les utiliser pour surveiller et enregistrer l'activité du clavier. Les enregistreurs de frappe, qui se présentent sous forme matérielle ou logicielle, aident à obtenir des informations relatives, entre autres, aux mots de passe, aux communications et aux sites Web ou à l'activité localisée menée à l'aide de l'ordinateur surveillé. En outre, des paquets de données "renifleurs" peuvent être utilisés pour rassembler les données pertinentes dans le cadre d'une enquête. Ces renifleurs, qui se présentent sous forme matérielle ou logicielle, collectent directement les données à partir d'un réseau et peuvent fournir des informations relatives à la source et au contenu des communications, ainsi que les contenus communiqués.

C. Préservation et récupération de données criminalistiques

211. Dans les affaires où Internet est utilisé à des fins terroristes, une part importante du processus d'obtention de preuves concerne la récupération de données numériques stockées. Cette récupération a deux objectifs principaux: l'extraction des preuves pertinentes aux fins d'enquête et de poursuites efficaces, et la préservation de l'intégrité de la source des données et de la chaîne de conservation pour assurer la recevabilité des preuves devant le tribunal. Afin de déterminer la meilleure méthode de préservation des preuves, il est important de faire la distinction entre les données volatiles, qui sont stockées dans certains dispositifs, tels que la mémoire vive (RAM) d'un appareil, et peuvent être irrémédiablement perdues en cas d'interruption de l'alimentation électrique, et les données non volatiles, qui sont conservées indépendamment de l'alimentation en électricité de l'appareil. Par exemple, le fait d'éteindre un ordinateur peut altérer les données figurant sur les disques de stockage et dans la mémoire vive, qui contiennent parfois des preuves importantes relatives aux programmes informatiques utilisés par le suspect ou aux sites Web visités. Les données volatiles fournissent des informations relatives aux processus en cours sur l'ordinateur en marche, qui peuvent être utiles dans le cadre d'une enquête, telles que les informations concernant les utilisateurs, les mots de passe, les données cryptées ou les messages instantanés. Parmi les exemples de dispositifs de stockage de données non volatiles, on peut citer les disques durs internes/externes, les lecteurs de disque portables, les périphériques de mémoire flash et les disques zip.

212. Le Département de la sécurité du territoire des États-Unis a présenté succinctement ce processus dans un guide intitulé "Best practices for seizing electronic evidence: a pocket guide for first responders"[123]. Ce guide décrit sommairement les étapes suivantes, qui permettent de préserver les preuves relativement aux enquêtes criminelles impliquant des appareils informatiques:

[123] États-Unis, Département de la sécurité du territoire, "Best practices for seizing electronic evidence: a pocket guide for first responders", 3e éd. (2007). Disponible à l'adresse: www.forwardedge2.com/pdf/bestPractices.pdf.

Meilleures pratiques de préservation des données

- N'utilisez pas l'ordinateur et ne tentez pas de rechercher des preuves.
- Si l'ordinateur est connecté à un réseau, débranchez la source d'alimentation du routeur ou du modem.
- Avant de déplacer une preuve, photographiez l'ordinateur comme vous l'avez trouvé, de face et de dos, ainsi que les cordons ou appareils connectés et l'espace alentour.
- Si l'ordinateur est éteint, ne l'allumez pas.
- Si l'ordinateur est allumé et que quelque chose est affiché sur le moniteur, photographiez l'écran.
- Si l'ordinateur est allumé et que l'écran est vierge, déplacez la souris ou appuyez sur la barre d'espace (vous afficherez ainsi l'image active sur l'écran); lorsque l'image apparaît, photographiez l'écran.
- Pour les ordinateurs de bureau, débranchez le cordon d'alimentation à l'arrière de la tour de l'ordinateur.
- Pour les ordinateurs portables, débranchez le cordon d'alimentation; si l'ordinateur ne s'éteint pas, localisez et enlevez le bloc-batterie (la batterie est généralement placée en dessous, et un bouton ou un commutateur permet habituellement de l'enlever); une fois la batterie ôtée, abstenez-vous de la remettre ou de la stocker dans l'ordinateur (vous empêcherez ainsi le démarrage accidentel de l'ordinateur).
- Faites des schémas et étiquetez les cordons pour pouvoir identifier ultérieurement les appareils connectés.
- Déconnectez tous les cordons et les périphériques de la tour ou de l'ordinateur portable.
- Emballez et transportez tous les éléments (y compris, le cas échéant, le routeur et le modem) comme des objets fragiles.
- Lorsque les termes du mandat de perquisition applicable l'autorisent, saisissez tout support de stockage supplémentaire.
- Conservez tous les supports, y compris la tour, à distance des aimants, des émetteurs radio et des autres éléments susceptibles de les endommager.
- Collectez les manuels d'instruction, la documentation et les notes, en veillant tout particulièrement aux éléments susceptibles de permettre de déterminer les mots de passe ou phrases de passe liés à l'ordinateur.
- Consignez par écrit toutes les étapes de la saisie de l'ordinateur et de ses éléments.

213. Des principes similaires s'appliquent aux appareils portables, tels que les téléphones intelligents et les assistants numériques. Toutefois, il est recommandé de ne pas éteindre l'appareil, car ce geste pourrait activer une protection de mot de passe, et empêcher l'accès aux preuves. Par conséquent, l'appareil devrait, dans la mesure du possible, rester chargé ou faire l'objet d'une analyse spécialisée avant que la batterie ne soit déchargée pour éviter toute perte de données.

214. L'affaire ci-dessous, survenue en Inde, illustre l'importance de l'analyse criminalistique en matière d'identification et de récupération des preuves numériques et autres de l'utilisation d'Internet par des terroristes.

Zia Ul Haq

Zia Ul Haq, qui a été arrêté le 3 mai 2010 et attend actuellement son procès, est présumé être un membre de Lashker e Taiba, un groupe armé basé au Pakistan et luttant contre le contrôle indien au Cachemire. L'accusation invoque notamment les arguments suivants: Zia Ul Haq a été persuadé par la ruse de se livrer au djihad alors qu'il travaillait en Arabie saoudite entre 1999 et 2001; il a été entraîné dans un autre pays que l'Inde à utiliser des armes, des munitions et des explosifs et à communiquer par courrier électronique; il a collecté un chargement d'armes, de munitions et d'explosifs à Delhi en 2005, après en avoir reçu l'instruction par courrier électronique; il a ensuite utilisé l'Internet pour se coordonner avec d'autres membres de Lashker e Taiba et a comploté pour commettre des actes terroristes à l'aide d'armes, de munitions et d'explosifs.

L'accusation a également soutenu que, le 7 mai 2006, Zia Ul Haq avait utilisé des grenades contenues dans le chargement d'armes de Lashker e Taiba lors d'un attentat commis contre le cinéma Odeon à Hyderabad.

Les enquêteurs ont obtenu auprès des fournisseurs d'accès à l'Internet les courriers électroniques échangés entre l'accusé et la personne qui le manipulait, et ont examiné leur contenu. Les ordinateurs du cybercafé qui ont été utilisés par le délinquant ont fait l'objet d'une analyse criminalistique, l'hôtel où il séjournait lorsqu'il était à Delhi pour prendre livraison des grenades a été identifié et l'examen criminalistique a montré que la signature figurant dans le registre des clients correspondait à la sienne. Pendant que l'accusé était détenu en attente de procès, l'Inde a envoyé une commission rogatoire à l'autorité centrale d'un autre pays pour engager une action contre la personne présumée avoir manipulé Zia Ul Haq.

En Inde, Zia Ul Haq a été accusé de diverses infractions, en vertu notamment des articles 15, 16, 17 et 18 de la loi de 1967 intitulée *Unlawful Activities (Prevention) Act* [loi relative aux activités illégales (et à leur prévention)], telle que modifiée en 2004 et 2008, qui prévoit la sanction des activités terroristes, de l'entraînement et du recrutement à des fins terroristes, de la levée de fonds en vue d'activités terroristes et de l'entente criminelle en vue d'activités terroristes.

215. En raison de la fragilité des preuves numériques, leur évaluation, leur obtention et leur examen sont plus efficaces lorsque des experts en criminalistique spécialement formés s'en chargent. En Israël, la législation nationale reconnaît l'importance d'une formation spécialisée puisqu'elle exige que les preuves numériques soient obtenues par des enquêteurs formés en informatique, qui suivent une formation de base et un cours de perfectionnement en interne pour se familiariser avec les systèmes informatiques, divers logiciels de criminalistique et la manière optimale de les utiliser. Lorsque des investigations particulièrement difficiles s'avèrent nécessaires, telles que la récupération de fichiers supprimés, défectueux, codés ou cryptés de manière complexe, il est possible de faire appel à un expert extérieur, qui pourra ensuite être appelé à témoigner pour le compte de l'accusation[124].

[124] Soumission écrite de l'expert d'Israël.

216. Il est recommandé d'effectuer les analyses sur une copie de la preuve originale, afin de préserver l'intégrité des données initiales[125]. Certains outils, tels qu'EnCase de Guidance Software ou Forensic Tool Kit, ou logiciels gratuits, permettent de créer une reproduction des données numériques. Dans la mesure du possible, il convient d'utiliser au moins deux outils différents pour créer les copies, au cas où l'un d'entre eux ne recueillerait pas toutes les données[126].

217. EnCase duplique l'image des données figurant sur l'appareil examiné, et analyse tous les secteurs du disque dur, y compris l'espace non alloué, pour assurer la capture de tout fichier caché ou supprimé. Il est également possible d'utiliser ce logiciel pour, entre autres, analyser la structure du système de fichiers du support numérique, organiser les fichiers en cours d'analyse et générer une représentation graphique ou autre rapport relatif à certaines caractéristiques des fichiers. EnCase génère également un identifiant unique, nommé "valeur de hachage", et l'attribue aux preuves numériques[127].

218. Afin de faciliter l'authentification des preuves numériques dans le cadre d'une procédure judiciaire (voir la section IV.D ci-dessous), la valeur de hachage attribuée aux fichiers numériques, ou à des parties de ceux-ci, s'appuie sur un algorithme mathématique appliqué aux caractéristiques de l'ensemble de données. Toute altération de l'ensemble de données entraînerait la création d'une valeur de hachage différente. Des valeurs de hachage sont générées concernant *a)* le disque dur initial avant la création d'un duplicata de l'image; *b)* la ou les copies dupliquées avant l'examen criminalistique; et *c)* la ou les copies dupliquées après cet examen. Si les valeurs de hachage correspondent, on peut conclure que les preuves numériques n'ont pas été falsifiées et que la copie qui a fait l'objet de l'examen criminalistique peut être considérée comme la source initiale dans le cadre de la procédure judiciaire. Parmi les algorithmes couramment utilisés, citons le MD5 et le SHA[128].

D. Aide à l'authentification des preuves numériques

219. Pour exercer avec efficacité des poursuites en cas de soupçon d'utilisation d'Internet à des fins terroristes, il faut produire des preuves qui ont été correctement collectées et bien documentées (voir la section VI.G.2). Cette condition est nécessaire pour établir l'intégrité des preuves numériques et faire ainsi en sorte qu'elles soient recevables devant le tribunal et persuasives. L'intégrité des preuves numériques peut être établie par une combinaison de techniques d'enquête traditionnelles et spécialisées. Parmi les principaux problèmes, on peut citer la chaîne de conservation de l'appareil utilisé pour

[125] États-Unis, Ministère de la justice, Office of Justice Programs, National Institute of Justice, *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* (2004), p. 1. Disponible à l'adresse: www.ncjrs.gov/pdffiles1/nij/199408.pdf.

[126] EC-Council Press, *Computer Forensics: Investigating Data and Image Files* (Clifton Park, New York, Course Technology Cengage Learning, 2010), p. 2 à 4.

[127] Soumission écrite de l'expert du Raggruppamento Operativo Speciale des Carabinieri (Italie).

[128] Barbara J. Rothstein, Ronald J. Hedges et Elizabeth C. Wiggins, "Managing discovery of electronic information: a pocket guide for judges" (Federal Judicial Center, 2007). Disponible à l'adresse: www.fjc.gov/public/pdf.nsf/lookup/eldscpkt.pdf/$file/eldscpkt.pdf.

stocker ou transmettre des données électroniques et des données effectives, ainsi que les procédures suivies pour obtenir ces données et les écarts par rapport aux procédures établies. En ce qui concerne les méthodes d'enquête traditionnelles, les agents des services de détection et de répression peuvent tenter d'obtenir des informations pour identifier, dans la mesure du possible, les personnes susceptibles d'avoir manipulé les preuves ou d'y avoir eu accès avant leur placement sous séquestre, et déterminer quand, comment et dans quel endroit les preuves ont été collectées.

220. Un procureur est également tenu de démontrer, entre autres, que les informations obtenues constituent une représentation exacte et fidèle des données figurant initialement sur le support concerné et qu'elles peuvent être attribuées à l'accusé. Les valeurs de hachage créées relativement aux preuves numériques concourent fortement à démontrer que ces preuves n'ont pas été compromises. D'autres éléments et témoignages concordants peuvent également être présentés pour établir cette authenticité. L'affaire d'Adam Busby qui, en 2010, a été reconnu coupable par un tribunal irlandais d'avoir envoyé à l'aéroport londonien d'Heathrow un courrier électronique d'alerte à la bombe offre une illustration de cette pratique. Pendant le procès, l'accusation a prouvé que le courrier électronique avait été envoyé à partir d'un ordinateur auquel M. Busby avait accès, et a également produit des copies papier de journaux d'opérations informatiques et des enregistrements de télévision en circuit fermé pour établir le moment auquel le courrier électronique avait été transmis et le fait que l'accusé contrôlait l'ordinateur à ce moment-là.

E. Unités opérationnelles de lutte contre la cybercriminalité

1. Unités nationales ou régionales de lutte contre la cybercriminalité

221. La dépendance croissante à la technologie informatique a entraîné une augmentation spectaculaire des besoins en unités spécialisées de lutte contre la cybercriminalité pour répondre aux demandes d'extraction des preuves informatiques, cette tendance n'étant pas uniquement observée dans les affaires terroristes impliquant l'utilisation d'Internet. La criminalité organisée, comme le trafic de drogues, la traite des êtres humains et la pédophilie internationale offrent des exemples d'affaires dans lesquelles l'utilisation criminelle d'Internet est particulièrement répandue, mais on a observé ces dernières années un nombre croissant de cas impliquant des preuves informatiques ou électroniques sous une forme quelconque. La création d'unités nationales de lutte contre la cybercriminalité dotées de compétences spécialisées en la matière pourrait accroître de manière significative les capacités opérationnelles d'un État de répondre à cette demande. En fonction des exigences géographiques et des critères de ressources, ces unités nationales peuvent être soutenues par des unités régionales plus petites pour répondre aux besoins locaux. En outre, il s'avère parfois plus efficace et rentable de placer les unités régionales sous le commandement d'une direction régionale locale.

222. Les responsabilités des unités nationales ou régionales de lutte contre la cybercriminalité sont notamment les suivantes:

a) Collecter des renseignements provenant de sources librement accessibles au moyen de techniques spécialisées de surveillance en ligne des sites de réseau social, des forums de discussion, des sites Web et des tableaux d'affichage électroniques sur Internet révélant les activités des groupes terroristes (entre autres nombreux éléments criminels). Dans la mesure où des groupes terroristes sont concernés, cette fonction pourrait être intégrée dans les attributions des unités de lutte contre le terrorisme dont le personnel est suffisamment formé et expérimenté pour la mener à bien, mais une formation spécialisée au sein d'un environnement de cybercriminalité est considérée comme essentielle. La fonction de collecte de renseignements requiert également la réalisation d'une évaluation et d'une analyse pour contribuer à élaborer une stratégie de lutte contre la menace constituée par l'utilisation d'Internet par les terroristes. Toutefois, des responsabilités ou des objectifs contradictoires entre les différents services de renseignement nationaux entravent parfois l'harmonisation et la traduction d'indices en plans opérationnels efficaces;

b) Mener des enquêtes spécialisées en matière de cybercriminalité dans les affaires nationales et internationales liées à la technologie, comme celles concernant la fraude sur Internet ou le vol de données et les autres affaires présentant des problèmes techniques, légaux ou procéduraux complexes, et pour lesquelles la direction de l'unité de lutte contre la cybercriminalité estime que les ressources spécialisées de ces unités sont nécessaires;

c) Faire office de lien à l'échelle du secteur d'activité et au niveau international concernant le développement de partenariats avec les principaux acteurs de la lutte contre la cybercriminalité, par exemple, le secteur des services financiers, le secteur des services de télécommunications, le secteur informatique, les services gouvernementaux, les institutions universitaires et les organisations intergouvernementales ou régionales pertinents;

d) Maintenir une unité chargée d'évaluer à l'échelle nationale et internationale les affaires de cybercriminalité pour hiérarchiser les enquêtes. Cette unité peut également être chargée de tenir des statistiques sur l'incidence des affaires de cybercriminalité;

e) Fournir des prestations de formation, recherche et développement, car la complexité et l'évolution constante de la cybercriminalité requièrent l'appui scientifique d'institutions universitaires spécialisées pour que les unités nationales et régionales soient dotées des compétences adéquates et bénéficient de tous les outils technologiques et de la formation nécessaires pour effectuer un examen criminalistique des supports informatiques et enquêter sur la cybercriminalité.

2. *Unités de criminalistique informatique spécialisées dans le triage des données*

223. Des unités de criminalistique informatique spécialisées dans le triage de données pourraient être créées pour soutenir les unités nationales et régionales de lutte contre la cybercriminalité. Le personnel de ces unités serait formé pour procéder à l'expertise, sur le lieu même de la perquisition, des éléments informatiques au moyen d'outils logiciels spéciaux. Un membre d'une telle équipe peut mener un examen initial sur le

site soit pour éliminer de l'enquête certains ordinateurs ou autres équipements informatiques périphériques qui sont dénués de valeur probatoire, soit pour saisir les preuves informatiques en respectant les techniques criminalistiques adéquates et soutenir les équipes locales lorsqu'elles interrogent les suspects à propos des preuves informatiques découvertes. Si nécessaire, les éléments des supports informatiques saisis par les unités de triage peuvent également faire l'objet d'un examen criminalistique complet au sein de l'unité régionale ou nationale compétente de lutte contre la cybercriminalité, selon le cas.

224. Des chercheurs de l'University College Dublin travaillent actuellement au développement d'une gamme de logiciels de criminalistique visant à faciliter l'analyse préliminaire, qui sera mise gratuitement à disposition des agents des services de détection et de répression. Le développement de ces outils fait partie d'une solution stratégique plus large, étudiée par le Centre de cybersécurité et d'enquête sur la cybercriminalité de l'University College Dublin et l'Unité d'enquête sur la criminalité informatique d'An Garda Síochána (le service irlandais de police nationale), visant à aider les unités de lutte contre la cybercriminalité qui manquent de moyens et dont le personnel et les budgets sont limités, à gérer leur charge de travail. Cette initiative a pour objectif de créer un laboratoire de criminalistique "libre". Les enquêteurs y participant recevront des instructions sur la création d'équipements de stockage et de traitement des preuves informatiques, et seront formés à utiliser les outils de criminalistique gratuits.

F. Collecte de renseignements

225. La collecte de renseignements est l'un des éléments essentiels des activités de lutte contre le terrorisme, car les informations ainsi obtenues déclenchent souvent les enquêtes qui conduisent à poursuivre les suspects, ou sont utilisées à titre de preuves au procès, dans la mesure où les lois et les règles de procédure internes le permettent. Toutefois, les différents objectifs dans lesquels les renseignements sont réunis, ainsi que les divers organismes en mesure de les obtenir ou de les utiliser, nécessitent parfois la prise en compte soigneuse d'intérêts divergents. Par exemple, les services de détection, de répression ou de renseignement chargés d'obtenir des renseignements insistent parfois sur la protection de la confidentialité de la source d'information, tandis que les fonctionnaires de justice doivent envisager, entre autres, le droit à un procès équitable d'un accusé et l'égalité d'accès aux preuves produites à son encontre. Il convient de veiller soigneusement à ce que les garde-fous adéquats soient mis en place concernant les droits de l'homme fondamentaux énoncés dans les conventions internationales applicables[129].

226. Dans certains États Membres, les renseignements issus de sources anonymes ne sont pas recevables devant le tribunal, mais sont parfois pris en compte s'ils sont corroborés par des sources autorisées ou par d'autres preuves. En Irlande, par exemple, les

[129]Voir, par exemple, l'article 10 de la Déclaration universelle des droits de l'homme, l'article 14 du Pacte international relatif aux droits civils et politiques, et l'article 6 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

renseignements réunis sur des terroristes peuvent constituer une preuve *prima facie* de l'appartenance d'un individu à une organisation illégale lorsque cette preuve est donnée sous serment par un policier ayant au moins le rang de commissaire divisionnaire. La Cour suprême irlandaise a confirmé la légalité de l'utilisation de ces renseignements, en présence d'éléments corroboratifs, lorsque la peur des représailles empêchait de réunir des preuves directes et compte tenu du rang élevé du policier qui témoignait[130].

227. Plusieurs experts ont également souligné la tension existant entre la nécessité d'encourager la mise à disposition d'informations à propos d'une éventuelle activité terroriste menée via l'Internet et celle d'appréhender et de poursuivre les auteurs de cette activité. Par exemple, une fois l'activité d'un site Web potentiellement liée au terrorisme identifiée, les services de sécurité nationale peuvent examiner les implications à long et à court terme de la réponse opérationnelle. Ces mesures peuvent inclure un contrôle passif de l'activité du site Web à des fins de renseignement, un dialogue clandestin avec d'autres utilisateurs pour obtenir d'autres informations à des fins de lutte contre le terrorisme ou la fermeture du site Web. Les divers objectifs et stratégies des organismes nationaux et étrangers peuvent guider les actions à privilégier[131].

228. Aux États-Unis, un rapport du Congressional Research Service a récemment mis en évidence les éléments pratiques à prendre en compte lorsque l'on estime la valeur des renseignements par rapport au niveau de menace d'une ressource en ligne:

> Par exemple, il a été signalé qu'un site Web djihadiste avait été conçu comme "appât" par la [Central Intelligence Agency] et le Gouvernement saoudien pour attirer et surveiller les activités terroristes. Les analystes des services de renseignement ont utilisé les informations recueillies sur ce site pour repérer les plans opérationnels des djihadistes, ce qui a permis d'arrêter ces derniers avant que les attentats planifiés ne puissent être commis. Cependant, ce site Web aurait également été utilisé pour transmettre aux djihadistes qui arrivaient en Iraq des plans opérationnels visant à mener des attaques contre les troupes américaines. Les débats entre les représentants des [National Security Agency, Central Intelligence Agency, Ministère de la défense, Office of the Director of National Intelligence et National Security Council] ont conduit à déterminer que la menace contre les troupes en opérations était plus élevée que la valeur des renseignements obtenus par la surveillance du site Web, et une équipe informatique de la [Joint Task Force-Global Network Operations] l'a finalement démantelé[132].

Comme l'illustre cette affaire, la coordination entre les différents organismes constitue un facteur important de riposte aux menaces identifiées.

229. D'autres États Membres, comme le Royaume-Uni, ont indiqué accorder, avec des résultats positifs, une place importante au développement de relations de travail et à la conclusion de mémorandums d'accord entre le ministère public, d'une part, et les

[130] *Ministère public (DPP)* c. *Kelly* [2006] 3 I.R. 115.

[131] Catherine Theohary et John Rollins, Congressional Research Service (États-Unis), "Terrorist use of the Internet: information operations in cyberspace" (8 mars 2011), p. 8.

[132] Ibid, p. 13.

services de détection et de répression ou de renseignement, d'autre part. De même, en Colombie, le Centre intégré de renseignement et d'enquête (Centro Integrado de Inteligencia e Investigación, ou CI3) est chargé, à l'échelle nationale, de coordonner les enquêtes sur les soupçons d'activités terroristes en vertu d'une stratégie en six volets. Cette démarche suppose qu'un fonctionnaire de haut rang de la police nationale assume la direction globale des différentes phases de l'enquête, dont la collecte, la vérification et l'analyse des preuves, ainsi que d'une phase judiciaire au cours de laquelle la police recueille des informations sur les parties et les lieux associés à la commission d'infractions[133].

230. L'expert français a exposé la méthode retenue dans son pays pour coordonner les réponses interinstitutionnelles à une activité terroriste identifiée:

- Phase 1: Les services de surveillance et de renseignement identifient une menace en surveillant l'activité Internet.
- Phase 2: Les services de surveillance informent le ministère public de la menace identifiée. Le juge ou le procureur peut alors autoriser les autorités de détection et de répression à placer sous surveillance l'activité Internet d'un suspect identifié. Depuis 2011, la législation permet au juge d'instruction d'autoriser les services de détection et de répression à enregistrer les données informatiques de la personne contrôlée. En outre, les données personnelles (par exemple, nom, numéro de téléphone, numéro de carte de crédit) peuvent être demandées au prestataire de services pertinent.
- Phase 3: L'enquête est menée sur la base des preuves réunies auprès des sources indiquées aux phases 1 et 2.

G. Formation

231. Les agents des services de détection et de répression qui enquêtent sur l'utilisation d'Internet à des fins terroristes doivent bénéficier d'une formation spécialisée sur les aspects techniques de la manière dont les terroristes et autres criminels peuvent utiliser l'Internet à des fins illicites et dont leurs propres services peuvent y avoir recours pour surveiller les activités des groupes terroristes. Cette formation peut être dispensée par le biais d'initiatives du secteur public ou du secteur privé, ou d'une combinaison des deux.

232. Les cours sur la criminalistique des technologies de l'information et les enquêtes relatives à la cybercriminalité peuvent être dispensés au niveau régional ou international par des organisations telles qu'Europol ou INTERPOL. En outre, un certain nombre de pays ont élaboré leurs propres programmes de formation sur la cybercriminalité à l'intention des services de détection et de répression, seuls ou en collaboration avec des instituts universitaires. Cette formation peut également être assurée au moyen de cours ad hoc, de séminaires, de conférences et de sessions pratiques dispensés par des acteurs du secteur public ou du secteur d'activité pertinent.

[133] Office des Nations Unies contre la drogue et le crime, *Recueil de cas sur les affaires de terrorisme*, par. 191.

233. La formation spécialisée est également proposée par des institutions universitaires, telles que l'University College Dublin (Irlande), qui a créé en 2006 le Centre de cybersécurité et d'enquête sur la cybercriminalité. Parmi les programmes dispensés par l'université, on peut citer la maîtrise en informatique criminalistique et enquête sur la cybercriminalité (*Master's degree in forensic computing and cybercrime investigation*), réservée aux agents des services de détection et de répression. D'autres sessions offrent également aux premiers intervenants une formation pour les aider à remplir leur rôle opérationnel dans les affaires de cybercriminalité.

234. Le projet Cybercrime Centres of Excellence Network for Training, Research and Education (2CENTRE), financé par la Commission européenne, a été lancé en 2010 dans le but de créer un réseau de centres d'excellence en matière de formation et de recherche pour lutter contre la cybercriminalité en Europe. Des centres sont en cours de création en Belgique, en Estonie, en France et en Irlande. Chaque centre national est financé en vertu d'un partenariat entre les représentants des services de détection et de répression, du secteur d'activité et du monde universitaire, qui collaborent pour élaborer les programmes de formation et les diplômes pertinents, ainsi que les outils utilisés pour lutter contre la cybercriminalité. Le Centre de cybersécurité et d'enquête sur la cybercriminalité de l'University College Dublin dirige le projet et en assure la coordination[134].

235. Une formation en ligne est également disponible par le biais de la Plate-forme interactive de formation et de coopération en ligne sur la lutte contre le terrorisme de l'ONUDC, qui a été lancée en 2011[135]. Cette plate-forme est un outil interactif spécialement conçu pour former les praticiens de la justice pénale à la lutte contre le terrorisme, tout en les intégrant à une communauté virtuelle unique au sein de laquelle ils peuvent partager leurs expériences et leurs points de vue. La plate-forme permet aux praticiens qui ont déjà participé aux formations dispensées par l'ONUDC de se connecter et de créer des réseaux avec leurs homologues, mais également de se tenir informés des évolutions juridiques en la matière et des possibilités de formation à venir, et de bénéficier d'une formation continue.

[134]Voir www.2centre.eu.

[135]Voir www.unodc.org/unodc/fr/terrorism/unodc-counter-terrorism-learning-platform.html.

V. Coopération internationale

A. Introduction

236. Compte tenu de la vitesse et de la portée mondiale de l'Internet, de l'anonymat relatif dans lequel les terroristes peuvent l'utiliser pour promouvoir leur cause ou faciliter leurs actes, ainsi que des difficultés liées à la localisation, la conservation, la saisie et la production des données, une coopération internationale opportune et efficace entre les services de détection, de répression et de renseignement est un facteur de plus en plus essentiel dans le succès des enquêtes et des poursuites relatives aux affaires de terrorisme.

B. Instruments et arrangements relatifs à la coopération internationale

1. Instruments universels contre le terrorisme

237. Les instruments universels contre le terrorisme, qui se composent des conventions et protocoles internationaux et des résolutions pertinentes du Conseil de sécurité, prévoient des mécanismes globaux de coopération internationale en matière de procédures pénales relatives au terrorisme. Ces instruments créent des dispositions concernant l'extradition, l'entraide judiciaire, le transfert de procédures pénales et le transfèrement de condamnés, l'exécution réciproque des jugements, le gel et la saisie d'avoirs et l'échange d'informations entre les services de détection et de répression.

238. Parmi les éléments clefs des instruments contre le terrorisme en matière de coopération internationale, on peut citer:

- L'obligation de traduire en justice les auteurs d'actes de terrorisme;
- L'obligation d'extrader ou de poursuivre (le principe *aut dedere aut judicare*);
- L'obligation d'établir sa compétence juridictionnelle dans certaines circonstances définies;
- L'interdiction d'invoquer la motivation politique de l'acte pour refuser une demande de coopération;
- Le respect de l'état de droit et des droits de l'homme;
- Le respect du principe de double incrimination;

- Le respect du principe de spécialité;
- Le respect de la règle *ne bis in idem*: interdiction des poursuites pour les mêmes faits[136].

239. Les principes généraux applicables à l'extradition et à l'entraide judiciaire dans les affaires de terrorisme ou de criminalité transnationale organisée font partie des mécanismes globaux énoncés dans les instruments universels de lutte contre le terrorisme et les autres instruments portant sur la criminalité transnationale organisée (par exemple, la Convention des Nations Unies contre la criminalité transnationale organisée)[137]. Le présent document n'a pas pour but d'énoncer ou d'analyser en détail la manière dont ces principes devraient être mis en œuvre en interne par les États. En revanche, il s'emploie à identifier, dans le cadre général de coopération internationale défini par ces instruments, et par rapport aux principes et mécanismes établis, les questions spécifiques aux affaires de terrorisme impliquant l'utilisation d'Internet, afin d'orienter les dirigeants et les praticiens vers les approches ou les stratégies qui reflètent les bonnes pratiques actuelles.

a) Absence d'instrument universel relatif aux questions liées à l'Internet

240. Une fois mis en œuvre, les mécanismes de coopération internationale définis dans les instruments universels contre le terrorisme fourniront probablement un fondement juridique à la coopération dans de nombreuses affaires relatives aux actes commis sur Internet par des personnes adoptant les conduites illégales visées dans ces instruments; néanmoins, aucun d'entre eux ne porte expressément sur ces actes en eux-mêmes. En l'absence d'instrument de lutte contre le terrorisme traitant expressément de cette question, les autorités, lorsqu'elles enquêteront sur ces affaires et les poursuivront, continueront de s'appuyer sur les traités ou arrangements internationaux ou régionaux en vigueur, établis pour faciliter la coopération internationale en matière d'enquête et de poursuite concernant des infractions générales de terrorisme ou de criminalité transnationale organisée.

241. Il est manifeste que l'absence d'instrument universel portant expressément sur les questions liées à l'Internet limite, dans une certaine mesure, la coopération internationale dans les enquêtes et les poursuites relatives aux affaires impliquant l'utilisation d'Internet par des terroristes. Toutefois, le présent document n'a pas pour objectif d'évaluer le bien-fondé des arguments en faveur ou en défaveur de l'utilité de l'élaboration d'un instrument universel global traitant, entre autres, de la coopération internationale dans les affaires pénales (terrorisme inclus) impliquant des questions liées à l'Internet. En revanche, il s'emploie à déterminer les éléments qui, en vertu du cadre international actuel, font obstacle à cette coopération et à définir la manière dont les autorités nationales pourraient utiliser les instruments et arrangements en vigueur pour faciliter ou renforcer la coopération internationale dans les affaires de terrorisme impliquant une forme ou une autre d'utilisation d'Internet.

[136] Office des Nations Unies contre la drogue et le crime, *Manuel pour la coopération internationale en matière pénale contre le terrorisme* (2009), sect. 1.C.

[137] Nations Unies, *Recueil des Traités*, vol. 2225, n° 39574.

b) Autres instruments: la Convention des Nations Unies contre la criminalité transnationale organisée et la Convention du Conseil de l'Europe sur la cybercriminalité

242. La Convention des Nations Unies contre la criminalité transnationale organisée est le principal instrument international ayant trait à la coopération internationale entre les États en matière d'infractions graves. Les articles 16 (Extradition), 18 (Entraide judiciaire), 19 (Enquêtes conjointes) et 27 (Coopération entre les services de détection et de répression) de la Convention contre la criminalité organisée portent sur la coopération internationale. Bien que les actes illicites visés dans cette Convention concernent la criminalité transnationale organisée, et non le terrorisme, les principes et mécanismes de coopération internationale sous-jacents sont très similaires à ceux qui sont exposés dans les instruments universels de lutte contre le terrorisme. À ce titre, les États parties qui ont exécuté les obligations de coopération internationale définies par ces instruments devraient disposer de cadres et de mécanismes largement compatibles.

243. Indépendamment de la Convention du Conseil de l'Europe sur la cybercriminalité, la Convention du Conseil de l'Europe pour la prévention du terrorisme, la Convention européenne d'extradition[138] et ses trois Protocoles additionnels[139], la Convention européenne d'entraide judiciaire en matière pénale[140] et ses deux Protocoles additionnels[141], ainsi que l'Acte 2000/C 197/01 du Conseil de l'Union européenne [du 29 mai 2000] établissant, conformément à l'article 34 du Traité sur l'Union européenne, la convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne pourraient fournir un fondement juridique à la coopération internationale dans les affaires de terrorisme impliquant un élément ou un autre d'utilisation d'Internet.

244. La Convention du Conseil de l'Europe sur la cybercriminalité contient des dispositions visant à encourager la coopération internationale via des mécanismes de coopération policière et judiciaire ainsi que des mesures conservatoires en cas d'urgence comme, par exemple, la communication informelle d'informations spontanées sur demande (art. 26) et l'établissement de points de contact joignables vingt-quatre heures sur vingt-quatre, sept jours sur sept (art. 35). Ces requêtes peuvent s'accompagner d'une demande de respect de la confidentialité et fournissent un mécanisme juridique permettant aux parties à la Convention d'utiliser des moyens de communication informels et de partager des informations, même si leur législation interne ne le prévoit pas.

245. On note que la Convention du Conseil de l'Europe sur la cybercriminalité est ouverte non seulement aux États membres du Conseil de l'Europe et aux États non membres qui ont participé à son élaboration, mais également aux autres États non membres, sous réserve dans ce dernier cas de l'accord unanime des États contractants ayant le droit de siéger au Comité des Ministres.

[138] Conseil de l'Europe, *Série des traités européens*, n° 24.

[139] Ibid., n° 86, 98 et 209.

[140] Ibid., n° 30.

[141] Ibid., n° 99 et 182.

2. *Autres arrangements régionaux ou multilatéraux*

246. Outre les instruments régionaux et internationaux susmentionnés, les États peuvent décider de conclure des traités ou arrangements bilatéraux ou multilatéraux qui créent des dispositions spécifiques relatives à la coopération en matière de cyberactivité liée au terrorisme ou à la criminalité transnationale. L'extradition et l'entraide judiciaire sont généralement régies soit par des traités soit par des instruments de "droit souple" convenus par blocs de pays. Néanmoins, les organisations régionales et sous-régionales jouent également un rôle important en facilitant l'échange d'informations et la coopération en vertu de ces arrangements mutuellement acceptés.

a) Mandat d'arrêt européen: cadre de Schengen

247. Le mandat d'arrêt européen défini dans le cadre de Schengen est un outil de coopération applicable dans tous les États membres de l'Union européenne; il s'est avéré extrêmement utile pour renforcer la coopération judiciaire en matière d'enquêtes et de poursuites pénales, se rapportant notamment au terrorisme en Europe. Une fois délivré, ce mandat contraint, sur la base de la réciprocité, les autorités d'un autre État membre à arrêter et transférer un suspect ou un condamné à l'État émetteur de manière à ce que cette personne puisse être traduite en justice ou effectuer une période de détention. Dans ce contexte, on note que le mandat d'arrêt européen prévoit notamment l'extradition des propres ressortissants d'un État membre, un concept auparavant étranger aux dispositions juridiques (souvent constitutionnelles) de nombreux États appartenant au système européen continental.

b) Mandat européen d'obtention de preuves

248. Depuis son entrée en vigueur en 2009, le mandat européen d'obtention de preuves a, de façon analogue au mandat d'arrêt européen pour les arrestations, créé une procédure simplifiée d'obtention et de transfert entre États membres de preuves (objets, documents, données) qui seront utilisées dans les procédures pénales. Dans le cadre de ce mandat, les preuves recueillies peuvent comprendre les données Internet relatives aux clients[142].

249. À l'aide de ces décisions-cadres et des autres instruments internationaux, les États européens ont, en bloc, mis au point une méthode très perfectionnée et essentiellement coopérative de collecte et de transmission transfrontalière de preuves et d'extradition/de remise de délinquants aux fins de procédures pénales. D'autres gouvernements pourraient examiner, aux niveaux politique et opérationnel, s'il est souhaitable d'adopter une approche collective à l'échelle régionale ou sous-régionale et de l'adapter afin d'harmoniser leurs efforts de coopération en matière d'enquêtes et de poursuites transfrontalières concernant des infractions liées au terrorisme.

[142]Voislav Stojanovski, "The European evidence warrant", in *Dny práva — 2009 — Days of Law: the Conference Proceedings*, 1re éd., David Sehnálek *et al.*, éd. (Brno, République tchèque, Université Masaryk, 2009).

c) Programmes du Commonwealth relatifs à l'extradition et à l'entraide judiciaire

250. À l'image du mandat d'arrêt européen dans le cadre de Schengen, le Programme de transfèrement, entre pays du Commonwealth, des délinquants reconnus coupables (Programme de Londres) offre un mécanisme simplifié d'extradition, et prévoit l'arrestation conservatoire des délinquants sur la base de mandats d'arrêt délivrés par d'autres pays membres, sans nécessité d'évaluation du caractère suffisant des preuves détenues à leur encontre. D'après ce programme, les infractions peuvent donner lieu à une extradition si elles sont réprimées dans les deux pays et passibles d'une peine d'emprisonnement d'au moins deux ans.

251. De la même manière, le Mécanisme du Commonwealth pour l'assistance mutuelle en matière criminelle (Mécanisme de Harare) vise à accroître le niveau et l'étendue de l'assistance en matière pénale entre les pays du Commonwealth, en facilitant l'identification et la localisation des personnes, la signification des documents, l'audition des témoins, la recherche et la saisie des preuves, la comparution des témoins, le transfèrement temporaire des personnes détenues aux fins de témoignage, la production des documents judiciaires ou officiels, la localisation, la saisie et la confiscation des produits ou instruments du crime, et la préservation des données informatiques.

252. Si les Programmes du Commonwealth ne sont pas des traités en tant que tels, ils constituent des exemples d'arrangements non contraignants, ou de "droit souple", en vertu desquels certains pays ont accepté d'incorporer des législations compatibles dans leur droit interne, conformes aux principes convenus, pour simplifier l'extradition et l'entraide judiciaire en matière pénale, notamment dans les enquêtes et les poursuites relatives au terrorisme.

d) Conseil de l'Europe

253. Outre l'élaboration d'instruments visant à promouvoir la coopération internationale dans les affaires relatives à la cybercriminalité, dont le terrorisme, le Conseil de l'Europe a également créé (en vertu de l'article 35 de la Convention du Conseil de l'Europe sur la cybercriminalité) un réseau de points de contact accessible en permanence (sept jours sur sept et vingt-quatre heures sur vingt-quatre), qui a pour but de faciliter la coopération internationale dans les affaires de cybercriminalité. Les projets régionaux CyberCrime@IPA et CyberCrime@EAP du Conseil de l'Europe et de l'Union européenne, entre autres, financent la participation de ces points de contact à des formations, ce qui leur permet d'établir des relations mutuelles et de créer un réseau avec les membres du réseau du Groupe des huit (G8).

254. Depuis 2006, le Conseil de l'Europe aide, par l'intermédiaire de son Projet global sur la cybercriminalité, des pays du monde entier à renforcer leur législation, la formation des juges, des procureurs et des enquêteurs des services de détection et de répression en matière de cybercriminalité et de preuves électroniques, ainsi que la coopération entre les services de détection et de répression et les prestataires de services et la

coopération internationale[143]. Depuis 2010, la question des flux de capitaux d'origine criminelle et des enquêtes financières sur l'Internet, et notamment du financement du terrorisme par ce moyen, constitue un enjeu majeur[144].

e) Plan d'action de l'Union européenne: centre de lutte contre la cybercriminalité

255. Le 26 avril 2010, le Conseil de l'Union européenne a reconnu le rôle essentiel joué par les technologies de l'information et de la communication dans la société moderne et le renforcement du nombre, de la portée et de la sophistication des menaces, ainsi que de leurs effets sur de nombreux pays, ces éléments accentuant la nécessité d'une coopération accrue entre les États membres et le secteur privé. Le Conseil de l'Union européenne a donc adopté des conclusions concernant un plan d'action sur la cybercriminalité, intégré dans le programme de Stockholm pour 2010-2014 et la future Stratégie de sécurité intérieure associée.

256. En vertu de ce plan, les membres ont notamment convenu de mandater la Commission européenne, en coopération avec Europol, pour analyser et faire un rapport sur l'utilité et la faisabilité de créer un centre européen de lutte contre la cybercriminalité visant à renforcer les connaissances, les capacités et la coopération en la matière. Cette tâche a été menée à bien et une proposition a été élaborée, en vertu de laquelle Europol accueillerait une nouvelle structure chargée de recevoir et de traiter les fichiers de travail analytique liés à la criminalité organisée de grande ampleur et au terrorisme.

3. Rôle des autres organisations et accords régionaux de coopération

257. Comme nous l'avons indiqué précédemment, les accords de coopération formelle conclus à l'échelle régionale ou sous-régionale entre les services de détection, de répression ou de renseignement jouent un rôle essentiel dans les efforts de la communauté internationale de renforcement et de coordination des mesures contre le terrorisme et la criminalité transnationale organisée. La coopération prévue par ces arrangements n'est généralement pas fondée sur des traités ou d'autres instruments juridiquement contraignants, mais elle prévoit parfois des mécanismes extrêmement efficaces entre les pays participants.

258. À l'échelle internationale, il existe de nombreux exemples de tels arrangements, mais trois d'entre eux, applicables en Europe, en Afrique et dans le Pacifique, illustrent la manière dont des groupes de pays ayant des intérêts et des objectifs compatibles en termes de détection, de répression et de sécurité peuvent collaborer avec succès pour développer et harmoniser une coopération étroite en matière d'enquêtes criminelles.

259. Le Centre franco-allemand de coopération policière et douanière, également nommé Centre d'Offenburg, a été créé en 1998 pour, entre autres, faciliter la coordination des

[143]Voir www.hub.coe.int/fr/web/coe-portal/what-we-do/rule-of-law/terrorism.

[144]Conseil de l'Europe, Comité d'experts sur l'évaluation des mesures de lutte contre le blanchiment des capitaux et le financement du terrorisme, *Les flux de capitaux d'origine criminelle sur Internet: méthodes, tendances et actions conjuguées des parties prenantes* (2012).

opérations interinstitutions (par exemple, opérations de perquisition et de surveillance et échange des informations recueillies) de part et d'autre de la frontière commune des deux pays. Son personnel se compose de membres des services de police, des douanes et des frontières au niveau fédéral et des États. Il gère chaque année plusieurs milliers de demandes, et sert de plate-forme d'instauration de solutions pragmatiques entre les organismes partenaires et de développement de relations de confiance et de coopération interinstitutions.

260. En Afrique, les membres de l'Organisation de coopération régionale des chefs de police de l'Afrique australe et de l'Organisation de coopération des chefs de police de l'Afrique de l'Est se sont entendus sur le principe d'une coopération entre les services de police dans certains domaines. Cette coopération concerne notamment l'échange régulier d'informations relatives à la criminalité, la planification, la coordination et l'exécution d'opérations conjointes (dont d'infiltration), le contrôle des frontières et la prévention de la criminalité dans les zones frontalières et les opérations de suivi, ainsi que la livraison surveillée de substances illégales ou de tout autre objet, et, si nécessaire, l'assistance technique et l'expertise[145].

261. Le Centre de coordination de la lutte contre la criminalité transnationale dans la région du Pacifique offre une plate-forme de collecte, de coordination, d'analyse et de partage des données en matière de renseignement criminel recueillies via un réseau d'unités nationales de lutte contre la criminalité transnationale situées dans les pays membres de toute la région. Le Centre, qui est géré par des fonctionnaires secondés par des agents de différents services de détection, de répression et des frontières des pays insulaires du Pacifique, permet à ses membres d'avoir accès à INTERPOL et à d'autres services mondiaux de détection et de répression, via le réseau international de la police fédérale australienne, qui soutient l'initiative.

262. De même, des pays qui ne sont pas nécessairement proches sur le plan géographique, mais qui ont des intérêts communs dans certains domaines thématiques relatifs à la détection, la répression et la sécurité, pourraient conclure des arrangements collectifs prévoyant l'échange d'informations et le partage de renseignements.

a) Groupe Egmont des cellules de renseignements financiers

263. Parmi les exemples d'arrangements de ce type ayant des implications sur les enquêtes relatives au financement du terrorisme, on peut citer le Groupe Egmont des cellules de renseignements financiers. Les enquêtes sur les soupçons de financement du terrorisme impliquent inéluctablement la collecte, le partage et l'analyse de documents financiers ou bancaires situés dans un ou plusieurs pays. Dans ces affaires, il est probable que la capacité des cellules de renseignements financiers à coopérer et à partager ces informations contribue au succès de l'enquête et des poursuites. Le Groupe Egmont, un organisme international créé en 1995, s'emploie à promouvoir et à améliorer la

[145] Charles Goredema, "Inter-State cooperation", in *African Commitments to Combating Organised Crime and Terrorism: A review of eight NEPAD countries* (Initiative africaine sur la sécurité humaine, 2004). Disponible à l'adresse: www.iss.co.za/pubs/Other/ahsi/Goredema_Botha/pt1chap5.pdf.

coopération entre les cellules de renseignements financiers dans leur combat contre le blanchiment de capitaux et le financement du terrorisme, et à favoriser notamment le développement et la systématisation de la coopération internationale dans l'échange réciproque d'informations. Le Groupe Egmont recommande à ses membres de conclure des mémorandums d'accord dans lesquels ils conviennent d'échanger les renseignements financiers se rapportant aux enquêtes et aux poursuites relatives au financement du terrorisme, au blanchiment de capitaux et aux activités criminelles connexes.

264. Pour que leurs cellules nationales de renseignements financiers puissent coopérer efficacement avec leurs homologues étrangères, les autorités devraient examiner l'opportunité de conclure les accords ou arrangements appropriés en matière de partage d'informations. Le mémorandum d'accord type proposé par le Groupe Egmont donne des orientations utiles sur le type de questions qu'il conviendrait d'aborder.

b) Organisation internationale de police criminelle

265. De nombreux instruments internationaux, dont la Convention internationale pour la répression du financement du terrorisme[146] (art. 18, par. 4) et la Convention des Nations Unies contre la criminalité transnationale organisée (art. 18, par. 13), ainsi que diverses résolutions du Conseil de sécurité, dont la résolution 1617 (2005), encouragent expressément les pays à travailler dans le cadre d'INTERPOL en matière de coopération relative à l'échange d'informations.

266. L'une des principales fonctions d'INTERPOL consiste à promouvoir la coopération internationale entre les services internationaux de détection et de répression, ainsi que l'échange rapide et sécurisé et l'analyse d'informations relatives aux activités criminelles. INTERPOL remplit cette fonction via son système I-24/7, qui est mis à disposition des agents des services de détection et de répression de tous les pays membres.

267. Grâce au système I-24/7, les bureaux centraux nationaux peuvent rechercher et croiser toute une série de données, notamment des informations sur les personnes soupçonnées de terrorisme, et différentes bases de données. Ce système a pour but de faciliter les enquêtes criminelles en fournissant une plus large gamme d'informations aux enquêteurs.

268. En sus du réseau I-24/7, INTERPOL promeut, via son programme sur la cybercriminalité, l'échange d'informations entre les pays membres grâce à des groupes de travail régionaux et des conférences. INTERPOL dispense des formations visant à créer et à maintenir des normes professionnelles, coordonne les opérations internationales et y contribue, établit une liste mondiale d'agents de contact pour les enquêtes relatives à la cybercriminalité, aide les pays membres à enquêter sur les cyberattaques ou la cybercriminalité par le biais de services d'investigation et de bases de données, développe des partenariats stratégiques avec d'autres organisations internationales et entités du secteur privé, identifie les menaces émergentes et partage ces renseignements avec

[146] Nations Unies, *Recueil des Traités*, vol. 2178, n° 38349.

les pays membres, et fournit un portail Web sécurisé permettant d'accéder aux informations et documents opérationnels[147].

269. Depuis 2009, INTERPOL collabore étroitement avec l'University College Dublin pour proposer une formation spécialisée et des échanges universitaires visant à promouvoir l'expertise des services de détection et de répression en matière d'enquêtes sur la cybercriminalité. En août 2011, des enquêteurs et des spécialistes en criminalistique informatique de 21 pays ont participé à la première session de l'Université d'été sur la cybercriminalité d'INTERPOL/University College Dublin. Ce programme de deux semaines, qui a été élaboré par l'Université, comprenait des exercices de simulation et a été dispensé par des professionnels des services de détection et de répression, de l'University College Dublin et du secteur privé. Cette formation visait à développer les connaissances et compétences théoriques et pratiques des enquêteurs dans toute une gamme de domaines pour les aider à mener plus efficacement leurs investigations sur la cybercriminalité. Elle a permis aux participants d'acquérir des compétences dans des domaines tels que la création d'image de disque dur, la criminalistique relative aux données réelles et aux téléphones portables, les enquêtes sur le blanchiment de capitaux, les techniques de perquisition et de saisie, les enquêtes sur les systèmes VoIP et sans fil ainsi que la détection et l'analyse de logiciels malveillants[148].

270. Enfin, l'unité de lutte contre la criminalité liée aux technologies de pointe d'INTERPOL facilite la coopération opérationnelle entre les pays membres en organisant, à l'échelle mondiale et régionale, des réunions de groupes d'experts sur la cybercriminalité et des ateliers de formation, et en assurant la coopération entre les services de détection et de répression, le secteur d'activité concerné et le monde universitaire. Cette unité aide également les pays membres en cas de cyberattaque et dans les enquêtes sur la cybercriminalité, par le biais de services d'investigation et de bases de données.

c) Office européen de police

271. Une partie importante du mandat d'Europol consiste à améliorer l'efficacité de la coopération entre les autorités de détection et de répression des États membres de l'Union européenne en matière de prévention et de lutte contre le terrorisme et les autres formes de criminalité transnationale organisée. Europol joue un rôle essentiel dans le groupe de travail européen contre la cybercriminalité (European Cybercrime Task Force), un groupe d'experts composés de représentants d'Europol, d'Eurojust et de la Commission européenne, qui œuvrent de concert avec les chefs des unités de lutte contre la cybercriminalité de l'Union européenne pour faciliter l'action transfrontalière en la matière. Europol apporte le soutien suivant aux États membres de l'Union européenne:

- Base de données sur la cybercriminalité: Europol fournit aux États membres de l'Union européenne un soutien en matière d'enquête et d'analyse concernant la cybercriminalité, et facilite la coopération transfrontalière et l'échange d'informations.

[147] Voir www.interpol.int/fr/Internet/Criminalit%C3%A9/Cybercriminalit%C3%A9.

[148] Ibid.

- Le document intitulé "Threat Assessment on Internet Facilitated Organised Crime (iOCTA)" évalue les tendances actuelles et futures en matière de cybercriminalité, et notamment d'activités terroristes et d'attaques contre les réseaux électroniques, et inspire à la fois l'activité opérationnelle et la politique de l'Union européenne.
- Les systèmes Internet Crime Reporting Online System (ICROS) et Internet and Forensic Expert Forum (IFOREX) sont en cours de développement. Ils permettront de centraliser les signalements effectués par les autorités des États membres de l'Union européenne de cybercriminalité, hébergeront des données techniques et accueilleront des formations destinées aux services de détection et de répression[149].

272. En outre, Europol est, au niveau opérationnel et en collaboration avec Eurojust, fortement impliqué dans la création et l'assistance d'équipes d'enquête conjointe et soutient les États membres en leur proposant des fichiers de travail analytique, une coordination par cas et des réunions tactiques. Sur la plate-forme de fichiers de travail analytique, les données nominatives (par exemple, informations sur les témoins, victimes, numéros de téléphone, lieux, véhicules et événements) sont stockées et soumises à un processus d'analyse dynamique qui relie les objets, les entités et les données présents dans les différentes demandes d'informations et enquêtes nationales. Les données sont étiquetées à l'aide d'un "code de gestion" qui indique clairement les conditions d'utilisation de certains éléments particuliers.

d) Eurojust

273. Dans le cadre de son mandat, Eurojust est notamment chargé, dans le domaine de la lutte contre le terrorisme, de faciliter l'échange d'informations entre les autorités judiciaires des différents États membres intervenant dans les enquêtes et les poursuites[150], d'aider les autorités judiciaires des États membres à délivrer et exécuter les mandats d'arrêt européens, et de favoriser les mesures d'enquête et de collecte des preuves nécessaires à la poursuite des infractions (par exemple, dépositions de témoins, preuves scientifiques, perquisitions et saisies, interception de communications). Les 27 membres nationaux d'Eurojust (juges, procureurs ou autorités de police dotées de compétences équivalentes dans leurs États respectifs) sont basés à La Haye (Pays-Bas), et sont en contact permanent avec les autorités nationales de leurs États respectifs. Celles-ci peuvent demander le soutien d'Eurojust au cours de certaines enquêtes ou poursuites en matière de terrorisme (par exemple, résolution de conflits de juridiction ou facilitation de la collecte de preuves).

[149]Voir "Cybercrime presents a major challenge for law enforcement", communiqué de presse de l'Office européen de police, 3 janvier 2011. Disponible à l'adresse: www.europol.europa.eu/content/press/cybercrime-presents-major-challenge-law-enforcement-523.

[150]La décision 2005/671/JAI du Conseil de l'Union européenne du 20 septembre 2005 sur l'échange d'informations et la coopération concernant les infractions terroristes contraint tous les États membres à désigner des correspondants nationaux en matière de terrorisme, qui doivent informer Eurojust (l'unité de coopération judiciaire de l'Union européenne) de toutes les activités terroristes dans leur pays, des premières étapes de l'interrogatoire des suspects à la phase de mise en accusation, en passant par la délivrance de mandats d'arrêt européens, les demandes d'entraide judiciaire et les jugements.

274. Par ailleurs, Eurojust encourage et soutient la création et le travail d'équipes communes d'enquête en fournissant des informations et des conseils aux praticiens. Il est de plus en plus admis que ces équipes constituent un instrument efficace en matière de riposte judiciaire à la criminalité transfrontalière et un lieu adéquat d'échange d'informations opérationnelles sur certaines affaires de terrorisme. Les membres nationaux d'Eurojust peuvent participer à des équipes communes d'enquête, soit en agissant pour le compte d'Eurojust, soit en leur qualité d'autorités nationales compétentes en matière de terrorisme. Dans une affaire survenue au Danemark, par exemple, une demande de création d'équipe commune d'enquête a été transmise aux autorités belges, et les bureaux danois et belge d'Eurojust sont intervenus pour instituer l'équipe entre les deux autorités nationales compétentes. Eurojust fournit également une assistance financière et logistique à ces équipes et accueille le secrétariat permanent pour les équipes communes d'enquête.

275. La publication d'Eurojust intitulée *Terrorism Convictions Monitor* a pour objet de fournir aux praticiens des exemples de jugements de certains pays qui pourraient servir à d'autres, concernant en particulier l'interprétation de la législation de l'Union européenne sur le terrorisme. Dans son numéro de septembre 2010, elle a publié une analyse approfondie de deux espèces présentant des caractéristiques communes, telles que le terrorisme djihadiste, la radicalisation et l'utilisation d'Internet[151]. L'une d'entre elles, communiquée par les autorités belges, est l'affaire *Malika El Aroud* et al., mentionnée ci-dessous (voir par. 377). L'équipe de lutte contre le terrorisme d'Eurojust organise régulièrement des réunions tactiques et stratégiques sur les tendances en matière de terrorisme, au cours desquelles des magistrats et des spécialistes de la législation pertinente issus de pays membres ou non de l'Union européenne partagent leur expertise sur des questions concrètes. On peut citer, à titre d'exemple, une réunion stratégique organisée en 2010 à propos de l'utilisation de la technologie VoIP à des fins terroristes et de la nécessité d'interception légale, ainsi qu'une réunion tactique tenue en avril 2011 sur l'extrémisme/le terrorisme violent. Lors de ces réunions, les spécialistes identifient les problèmes communs, et communiquent les meilleures pratiques et les connaissances en résultant aux décideurs de l'Union européenne, tout en déterminant les façons d'améliorer la coordination en matière de lutte contre le terrorisme.

C. Cadres législatifs nationaux

276. L'existence, au niveau national, d'un cadre législatif de coopération internationale constitue un élément fondamental d'une structure efficace de facilitation de cette coopération dans les enquêtes et les poursuites concernant des affaires de terrorisme. Cette législation devrait incorporer dans le droit interne d'un pays les principes de coopération internationale énoncés dans les instruments universels contre le terrorisme.

277. Outre la production d'un certain nombre de documents visant à aider les pays à incorporer dans leur législation les mécanismes de coopération internationale, le Service

[151] Le *Terrorism Convictions Monitor* est disponible sur demande auprès de l'équipe de lutte contre le terrorisme d'Eurojust.

de la prévention du terrorisme de l'ONUDC offre des prestations de conseil, de formation et de renforcement des capacités dans le cadre des services proposés aux pays en matière d'application des obligations internationales de lutte contre le terrorisme.

D. Mesures non législatives

278. L'adhésion aux instruments bilatéraux et multilatéraux et l'adoption de la législation connexe sont des composantes fondamentales d'un régime efficace de coopération internationale, mais ne suffisent pas. Parmi les éléments déterminants figure la présence d'une autorité centrale dotée de moyens suffisants, intervenant en amont et capable, en s'appuyant sur les mécanismes disponibles (à la fois formels et informels), de faciliter la coopération de manière opportune et efficace.

279. L'existence d'une coordination interinstitutions efficace entre les services de détection et de répression, les services de renseignement spécialisés (par exemple, les cellules de renseignements financiers) et les autorités centrales au niveau national, accompagnée de la législation nécessaire et de procédures claires et simplifiées de gestion des requêtes, constitue une condition préalable importante au succès de la coopération internationale.

280. L'affaire suivante, qui fait l'objet de poursuites en Colombie, constitue un bon exemple de coopération formelle et informelle approfondie entre les autorités, tant nationales qu'internationales.

Affaire impliquant les Forces armées révolutionnaires de Colombie (FARC)

Le 1er mars 2008, les forces armées colombiennes ont mené diverses opérations contre des membres présumés des Forces armées révolutionnaires de Colombie (FARC). Au cours de ces opérations, un individu soupçonné d'être l'un des principaux leaders et plusieurs autres membres de l'organisation ont été tués, et des preuves ont été découvertes, dont des appareils électroniques comme des ordinateurs, des agendas numériques et des clefs USB. Les objets contenant des preuves numériques ont été transmis à la police judiciaire colombienne pour qu'elle puisse les utiliser lors d'éventuelles enquêtes criminelles et poursuites.

Les données extraites des appareils numériques ont fait ressortir des informations relatives au réseau international de soutien de l'organisation, et notamment des liens avec plusieurs pays d'Amérique centrale, d'Amérique du Sud et d'Europe. Ce réseau avait pour principaux objectifs de collecter des fonds pour financer les activités des FARC, de recruter de nouveaux membres et de promouvoir la politique de l'organisation, en obtenant notamment le retrait de son nom des listes relatives au terrorisme dressées par l'Union européenne et par certains pays. Sur le fondement des preuves découvertes, le Procureur colombien a ouvert une enquête criminelle contre les personnes supposées soutenir et financer les FARC.

Les autorités colombiennes ont partagé ces preuves avec leurs homologues espagnoles, ce qui a permis d'identifier le leader des FARC dans ce pays, connu sous le nom d'emprunt "Leonardo". "Leonardo" est arrivé en Espagne en 2000, et a obtenu l'asile politique.

Le Procureur colombien a obtenu suffisamment de preuves pour ordonner la délivrance d'un mandat d'arrêt aux fins d'extradition contre "Leonardo", et a utilisé les voies

diplomatiques et autres canaux légaux de coopération internationale pour demander son extradition afin qu'il soit jugé en Colombie.

"Leonardo" a été arrêté en Espagne, et la perquisition de son domicile et de son lieu de travail a permis de découvrir des documents et des appareils électroniques qui prouvaient ses liens avec les infractions objet de l'enquête. Il a ensuite été libéré sous caution, son statut de réfugié empêchant son extradition immédiate.

Une procédure pénale par contumace a été engagée en Colombie à l'encontre de "Leonardo" au titre de son implication présumée dans le financement du terrorisme. La Cour suprême de justice colombienne a jugé que les informations obtenues au cours de l'opération du 1er mars 2008 et découvertes sur les appareils électroniques saisis étaient irrecevables. Par la suite, le Procureur, en collaboration avec ses homologues des pays où se trouvaient des membres du réseau de soutien des FARC, a utilisé toutes les voies de coopération internationale disponibles pour identifier les membres du réseau en Espagne et dans d'autres pays européens, et collecter d'autres preuves étayant l'accusation.

Par ailleurs, dans leur réponse aux commissions rogatoires délivrées par le Procureur colombien, les autorités judiciaires espagnoles ont transmis toutes les informations recueillies lors des raids et des perquisitions organisés au domicile de "Leonardo". Selon la police judiciaire espagnole, ces informations établissaient la culpabilité de "Leonardo" et d'autres personnes concernant la constitution d'une cellule terroriste des FARC en Espagne. Elles contribuaient également à établir la culpabilité de "Leonardo" en matière de financement du terrorisme et renforçaient la présomption de relations entre "Leonardo" et les personnes poursuivies pour leurs liens avec le groupe terroriste Euskadi Ta Askatasuna (ETA) (Patrie basque et liberté). Les perquisitions effectuées en Espagne ont entraîné la saisie d'autres preuves documentaires et numériques qui, pour l'essentiel, étaient similaires aux preuves qui avaient été déclarées irrecevables. À l'aide des nouvelles preuves fournies par les autorités espagnoles, le Procureur colombien a pu poursuivre la procédure engagée à l'encontre de "Leonardo". De plus, les nouvelles preuves montraient les efforts déployés par les FARC pour permettre à ses membres d'accéder aux universités, aux organisations non gouvernementales et autres entités étatiques afin de rechercher des possibilités de financement et de recruter de nouveaux membres.

Ces preuves ont également étayé l'existence d'une "commission internationale" au sein des FARC, qui gérait un programme de sécurité des communications, particulièrement celles transmises via l'Internet ou les ondes radio (moyens permanents de communication entre les leaders de l'organisation et les membres du réseau international de soutien) en cryptant les informations transmises, en utilisant la stéganographie pour dissimuler les messages, en envoyant des courriers électroniques de type spam et en supprimant les historiques de navigation pour empêcher les services d'enquête ou les autorités judiciaires de découvrir ces informations. À cet égard, les autorités espagnoles et colombiennes ont coopéré pour "casser" les codes et déchiffrer le contenu des messages transmis par les leaders présumés des FARC en Colombie et en Espagne.

Avant d'engager la procédure contre "Leonardo", le Procureur colombien a demandé au juge que les nouvelles preuves soient réputées constituer des "preuves reçues ultérieurement" et d'une "source indépendante". Cette requête, à laquelle le juge a fait droit, a permis d'inclure ces preuves dans la procédure judiciaire sans que puissent être invoqués les motifs pour lesquels les preuves similaires auraient sinon été exclues.

Les poursuites engagées par contumace contre "Leonardo" pour financement du terrorisme sont en cours en Colombie, en attente de l'issue de la procédure d'extradition.

281. Dans cette espèce, les autorités ont tiré parti à la fois des mécanismes formels d'entraide judiciaire et de leurs relations informelles. Il existe des disparités concernant la mesure dans laquelle les autorités des différents pays peuvent fournir une entraide en l'absence de traité ou de demande formelle, mais dans de nombreux cas, elles disposent d'une certaine capacité à offrir une assistance sur la base de demandes informelles d'autorités d'autres pays en matière de terrorisme. La réunion du groupe d'experts a fait ressortir plusieurs cas et circonstances dans lesquels cette coopération informelle avait été ou pouvait être utilisée pour enquêter avec succès sur des affaires impliquant l'utilisation d'Internet par des terroristes.

1. L'importance des relations

282. Au niveau opérationnel, il est extrêmement important que les services nationaux de détection, de répression et chargés des poursuites favorisent, établissent et maintiennent des relations de confiance avec leurs homologues étrangers dont la coopération pourrait s'avérer nécessaire dans le cadre d'enquêtes criminelles transfrontalières.

283. Compte tenu du caractère transnational de la plupart des actes de terrorisme et de l'activité criminelle connexe, de la complexité et du caractère délicat des enquêtes fondées sur le renseignement, et de la nécessité d'agir sans délai dans le cadre d'événements et d'enquêtes qui évoluent rapidement, la confiance entre les services de détection, de répression et chargés des poursuites au niveau national et international constitue souvent un facteur crucial de succès des enquêtes et des poursuites. Ce point est particulièrement important dans le contexte d'Internet, où la préservation, par exemple, de données d'usage et de preuves numériques conservées sur des ordinateurs et autres appareils portables se trouvant dans plusieurs pays, est souvent essentielle dans l'exercice des poursuites pénales, et doit intervenir dans des délais très courts. Les contacts personnels avec les homologues d'autres pays, la connaissance de leurs procédures et les relations de confiance contribuent à une coopération internationale efficace.

284. Les modes de coopération informelle diffèrent selon les pays, mais il est possible d'identifier certains éléments de bonnes pratiques dans les enquêtes liées au terrorisme.

a) Élaboration de mécanismes d'échange d'informations efficaces: le recours à des agents de liaison

285. Lors de la réunion du groupe d'experts, plusieurs spécialistes ont relevé que leurs services nationaux de détection et de répression géraient un réseau de postes de liaison internationaux qui facilitait considérablement les demandes de coopération internationale. Par exemple, le Bureau de police criminelle fédéral allemand (*Bundeskriminalamt*) a des agents de liaison et des contacts directs dans près de 150 pays. En outre, le réseau européen European Expert Network on Terrorism Issues, créé en 2007, rassemble des experts du monde universitaire et des services de police et de renseignement, et s'est avéré être un mode très efficace de partage multidisciplinaire d'informations et d'expertise.

286. L'affaire *R.* c. *Namouh* offre un exemple de coopération internationale fructueuse, mise en œuvre de manière totalement informelle entre les autorités autrichiennes et canadiennes de détection, de répression et chargées des poursuites dans une affaire concernant des personnes vivant dans leurs pays et utilisant l'Internet pour se livrer à des activités liées au terrorisme.

R.* c. *Said Namouh

M. Said Namouh était un ressortissant marocain qui vivait dans une petite ville canadienne.

Le 10 mars 2007, une vidéo sous forme de lettre "ouverte" lue par le Sheik Ayman al-Zawahiri a été publiée sur un site Internet. Dans celle-ci, Al-Zawahiri conseillait aux Gouvernements autrichien et allemand de retirer leurs troupes de la mission de maintien de la paix en Afghanistan; à défaut, ils en subiraient les conséquences. À un moment, Al-Zawahiri déclarait:

> La paix est une affaire réciproque; si nous sommes en sécurité, vous serez en sécurité. Si nous sommes en paix, vous serez en paix et si nous allons être tués, avec la permission de Dieu, vous allez être combattus et tués. Cela est l'équation exacte. Essayez alors, de la comprendre si vous comprenez.

Cette vidéo, accompagnée des déclarations d'Al-Zawahiri, avait pour toile de fond une mosaïque d'images composées notamment de voitures blindées avec des drapeaux nationaux et d'importants politiciens autrichiens et allemands. À certains endroits, on voyait des photos d'Al-Zawahiri et d'autres personnes au visage couvert.

Après la diffusion de la vidéo, les autorités autrichiennes ont ouvert une enquête et ont mis sur écoute diverses communications de Mohammed Mahmoud, un ressortissant autrichien vivant à Vienne. Ces communications, constituées de sessions VoIP et de discussions menées en arabe sur Internet, ont révélé que M. Mahmoud communiquait avec une personne vivant au Canada sur des questions liées au djihad, et notamment des projets d'attaque terroriste, probablement en Europe. Les participants discutaient de l'utilisation d'explosifs et d'autres préparatifs relatifs à l'attaque.

À la suite de l'activité d'interception, les enquêteurs ont déterminé que Said Namouh, qui vivait au Canada, avait participé aux communications susmentionnées. En juillet 2007, la Gendarmerie royale du Canada est intervenue dans l'enquête, dont la coordination entre les autorités autrichiennes et canadiennes était assurée par l'agent de liaison des services de détection et de répression du Canada, basé à Vienne. Malgré l'existence d'un traité d'entraide judiciaire formel entre l'Autriche et le Canada, aucune demande n'a été présentée en vertu de ce traité; la coopération est intervenue de manière totalement informelle.

L'enquête a révélé qu'entre novembre 2006 et septembre 2007, une personne qui utilisait la connexion de M. Namouh avait passé un temps considérable sur le Web et été en contact permanent avec des djihadistes du monde entier, par l'intermédiaire notamment du Global Islamic Media Front (GIMF), l'un des plus anciens et des plus importants groupes djihadistes virtuels. Soutenu par le Centre Al-Fajr, le GIMF fait office de branche médiatique de l'Armée de l'Islam [Jaish al-Islam]. Entre autres activités, le GIMF diffuse de la propagande

et fournit aux djihadistes les outils (par exemple, manuels sur les explosifs, logiciels de cryptage) nécessaires pour mener le djihad. Une grande partie de l'activité de M. Namouh sur Internet concernait la publication de messages sur divers forums de discussion fréquentés par les djihadistes.

En mai 2007, Alan Johnston, un journaliste de la BBC, a été enlevé à Gaza par l'"Armée de l'Islam". Le GIMF a publié plusieurs vidéos relatives à cet événement, dont l'une du 9 mai 2007 dans laquelle l'Armée de l'Islam revendiquait la responsabilité de l'enlèvement, et deux des 20 et 25 juin dans lesquelles elle menaçait d'exécuter l'otage si certaines demandes n'étaient pas satisfaites. Fort heureusement, M. Johnston a été libéré sain et sauf le 3 juillet 2007.

Les 7 et 8 mai, les autorités ont intercepté les communications de M. Namouh sur un forum Internet, qui ont révélé qu'il participait à des discussions relatives à l'enlèvement d'Alan Johnston, et tout particulièrement à la préparation du message du GIMF en revendiquant la responsabilité. Ce message a été diffusé peu après, le 9 mai. Selon une transcription de l'échange sur Internet du 8 mai, produit au procès à titre de preuve (et traduit de l'arabe au français), M. Namouh a publié le message suivant: "Mon bien-aimé frère Abou Obayda, reste avec nous sur la ligne, qu'Allah te comble de biens, pour que puisse voir ce qu'il faut faire; la déclaration sera émise aujourd'hui, si Allah le voudra".

Au total, entre le 3 juin et le 9 septembre 2007, 31 conversations ont eu lieu entre M. Namouh et M. Mahmoud. Elles ont révélé qu'ils projetaient de commettre un attentat à l'explosif dans un lieu non précisé d'Europe et qu'ils discutaient de la manière de se procurer ou de fabriquer des ceintures explosives, de questions de financement et de projets de voyage pour rencontrer d'autres personnes au Maghreb et en Égypte afin de finaliser les préparatifs. Ces conversations laissaient penser que M. Namouh avait l'intention de commettre un attentat-suicide.

Le 12 septembre 2007, craignant que ces projets ne soient sur le point d'être exécutés, les autorités autrichiennes et canadiennes ont procédé simultanément à l'arrestation de M. Namouh et de M. Mahmoud.

Au Canada, M. Namouh a été accusé de complot à l'engin explosif (dans un lieu non précisé d'Europe), de participation aux activités d'un groupe terroriste, de facilitation d'une activité terroriste et d'extorsion contre un gouvernement étranger (menace vidéo contre l'Autriche et l'Allemagne).

Au procès, l'avocat de la défense de M. Namouh a contesté plusieurs aspects de l'accusation, en invoquant notamment des arguments constitutionnels fondés sur le droit à la liberté d'expression (relativement à la question de savoir si le GIMF était une organisation terroriste). La défense a soulevé des objections quant à l'objectivité du principal témoin expert appelé par l'accusation pour témoigner sur le mouvement Al-Qaida et ses ramifications, sur le djihadisme mondial (notamment virtuel), sur les méthodes et le style de propagande du GIMF et sur l'utilisation d'Internet par l'organisation. La défense a également contesté le fait que les activités menées par le GIMF et les groupes associés constituaient des actes de terrorisme, ainsi que la fiabilité des preuves relatives à l'interception de communications sur Internet en Autriche et au Canada et l'exactitude des traductions de l'arabe au français des enregistrements de ces communications. La défense a demandé au tribunal de considérer que les différents messages transmis par M. Namouh pour le compte du GIMF devaient être entendus au sens figuré et non comme des actes encourageant les actes de terrorisme.

En examinant les arguments de la défense relatifs à la nature des éléments mis en ligne ou communiqués pour le compte du GIMF, le tribunal a conclu ce qui suit:

> "Le Tribunal n'a aucun doute à ce sujet. Le contexte de ces messages fait clairement référence à des actions réelles encouragées par le GIMF. La mort et la destruction sont partout. Le Jihad dont le GIMF fait la promotion est de nature violente. Cette promotion constitue nettement un encouragement et parfois une menace d'activités terroristes. De ce fait, cette activité s'inscrit clairement dans la définition d'activité terroriste au sens de l'article 83.01 C.cr."

En concluant que M. Namouh était coupable d'encouragement d'actes de terrorisme, le tribunal s'est référé aux communications interceptées contenant des déclarations qui montraient le caractère zélé et actif de sa participation aux activités du GIMF. Du point de vue du tribunal, plusieurs messages étaient également pertinents, dont celui du 12 décembre 2006 (voir ci-dessous), dans lequel l'accusé exprimait son souhait de dissimuler ses activités, et celles du GIMF, en supprimant les données informatiques l'incriminant:

> [TRADUCTION]
> "Urgent Urgent Urgent
> "La paix, la miséricorde et les bénédictions d'Allah sur vous
> "Je veux effacer tous les films et livres jihadistes qui se trouvent sur mon ordinateur sans laisser d'empreintes, qu'Allah vous bénisse; car j'ai des doutes qu'une personne a inspecté mon ordinateur.
> "La paix, la miséricorde et les bénédictions d'Allah sur vous."

Dans d'autres communications, l'intéressé s'enquérait de l'utilisation de logiciels d'anonymisation et d'outils similaires pour dissimuler ses activités. Après le procès intervenu en octobre 2009, il a été déclaré coupable de tous les chefs d'accusation; il a été condamné à la réclusion criminelle à perpétuité.

b) Enquêtes conjointes

287. Le concept d'"enquête conjointe" est mentionné dans certains traités internationaux (par exemple, l'article 19 de la Convention des Nations Unies contre la criminalité transnationale organisée), mais les instruments universels de lutte contre le terrorisme ne comportent aucune référence expresse à cette stratégie. Néanmoins, cette méthode est parfaitement conforme aux principes sous-jacents et à l'esprit des dispositions de ces instruments ayant trait à la coopération internationale. Certains pays, en particulier européens, l'ont adoptée avec succès dans un certain nombre d'enquêtes liées au terrorisme, et il convient de noter le rôle important joué par Europol dans la création et le soutien d'équipes d'enquête conjointe. Ces équipes, qui sont composées à la fois d'agents des services nationaux de détection et de répression et de fonctionnaires d'Europol, ont pour objectif principal de mener des enquêtes dans un but spécifique et pendant une durée limitée dans un ou plusieurs États membres[152].

[152] Eveline R. Hertzberger, *Counter-Terrorism Intelligence Cooperation in the European Union* (Turin, Italie, Institut interrégional de recherche des Nations Unies sur la criminalité et la justice, juillet 2007).

288. Europol collabore avec un système d'unités nationales, qui sont ses interlocutrices désignées au sein des forces de police nationales. Ce mode d'organisation facilite et encourage l'échange d'informations entre les États membres au moyen d'un réseau numérique sécurisé, et offre un système de 17 fichiers de travail analytique au sein du cadre juridique d'Europol, visant principalement à permettre aux autorités participantes d'assurer une entière coordination et coopération.

289. Il est difficile d'évaluer la mesure dans laquelle les pays ont ainsi collaboré au niveau mondial, mais les discussions menées lors de la réunion du groupe d'experts ont fait ressortir que les communautés internationales chargées de la détection, la répression et la sécurité étaient de plus en plus conscientes du fait que, compte tenu de la nature du terrorisme moderne et des modes opératoires utilisés par les terroristes, une coopération étroite était un facteur croissant de succès des efforts visant à perturber, prévenir et poursuivre les actes terroristes.

E. Coopération formelle *versus* coopération informelle

290. Dans les affaires de terrorisme comportant un élément transfrontalier, la coopération internationale peut revêtir de nombreuses formes, en fonction de la nature de l'infraction concernée, du type d'assistance recherché, de la législation nationale applicable et de l'existence et du statut de tout traité ou arrangement s'y rapportant.

291. En dépit de l'amélioration de leur niveau global de performance et d'efficacité, les procédures formelles d'entraide judiciaire en matière pénale restent des processus de longue haleine, qui nécessitent un travail administratif considérable tant pour le pays requérant que pour le pays requis. Dans de nombreuses affaires de terrorisme, en particulier celles qui concernent des infractions connexes à Internet, la coopération informelle devient tout aussi importante que les voies formelles, car elle permet de gagner du temps dans des situations où il est essentiel d'agir sans délai (par exemple, préserver des données relatives à l'usage d'Internet) pour que les poursuites aboutissent. Les participants à la réunion du groupe d'experts ont souligné qu'il était important que, dans la mesure du possible, les autorités nationales de renseignement, de détection et de répression et les procureurs élaborent et utilisent de manière proactive des mécanismes favorisant les canaux tant informels que formels de coopération internationale.

292. Dans de nombreux cas, par exemple lorsque les autorités d'un pays ont demandé la préservation de données détenues par un fournisseur d'accès à l'Internet d'un autre pays, les autorités devraient pouvoir coopérer de manière informelle pour préserver ces données aux fins d'enquêtes ou de poursuites relatives à une infraction pénale.

293. Les questions juridiques associées à la conduite d'une enquête criminelle relative à Internet, et notamment celles qui se rapportent à la compétence juridictionnelle, sont parfois extrêmement complexes. Lorsque les enquêteurs d'un pays ont besoin d'accéder aux informations détenues sur des ordinateurs situés dans un autre pays, des questions délicates peuvent se poser concernant l'autorisation légale et le fondement de leurs actions. Les autorités d'un pays peuvent traiter directement avec les parties détenant

les informations qu'elles recherchent dans un autre pays, mais les réponses varient. En règle générale, il est souhaitable que les autorités collaborent avec leurs homologues étrangères, si possible de manière informelle, pour obtenir ces informations.

294. La forme et le mode de coopération dépendent en grande partie de la nature et de l'objectif de l'assistance demandée. Par exemple, si les autorités d'un pays sont parfois en mesure d'offrir une assistance informelle à leurs homologues étrangères en demandant aux FAI de préserver volontairement des données relatives à Internet, la perquisition et la saisie de ces données nécessitent généralement une autorisation judiciaire, qui ne peut être obtenue que par des moyens formels.

295. Le recours à des demandes formelles est parfois la seule méthode permettant aux autorités de fournir la coopération requise. Dans ce cas, il importe que les pays soient dotés d'une législation et de procédures qui prévoient des réponses opportunes et efficaces aux demandes, pour optimiser, dans la mesure du possible, les chances de succès.

1. Coopération informelle

296. Compte tenu de l'importance potentielle et de l'urgence de localiser et d'obtenir les données relatives à Internet dans les enquêtes sur le terrorisme, et vu la probabilité que ces données soient détenues dans un autre pays, les enquêteurs doivent examiner les moyens d'action formels et informels. Les voies formelles d'entraide judiciaire offrent une plus grande certitude concernant les questions juridiques associées, mais elles prennent plus de temps et impliquent davantage de travail administratif que les canaux informels.

297. Lors de la réunion du groupe d'experts, le spécialiste canadien a souligné le rôle crucial qu'une coopération informelle étroite entre la Gendarmerie royale du Canada et l'Agence fédérale autrichienne de protection de l'État et de lutte contre le terrorisme (*Bundesamt für Verfassungsschutz und Terrorismusbekämpfung*), facilitée par l'agent de liaison canadien basé à Vienne, avait joué dans l'aboutissement des poursuites dans un cas donné. D'autres experts ont mentionné des exemples similaires dans lesquels le recours aux agents de liaison pour faciliter la coopération informelle avait eu un rôle déterminant dans le succès final.

298. Il est probable que les données relatives à Internet telles que les données d'usage des clients détenues par les FAI constituent des preuves déterminantes dans les affaires de terrorisme impliquant l'utilisation d'ordinateurs et de l'Internet. Si les enquêteurs parviennent à entrer en possession des ordinateurs utilisés par un suspect, ainsi que des données d'usage détenues par les FAI, ils ont plus de chances d'établir le lien entre le suspect et la commission d'une infraction.

299. De ce fait, il importe que les enquêteurs et les procureurs soient pleinement conscients de l'importance potentielle des données relatives à Internet et de la nécessité de prendre le plus rapidement possible des mesures pour les préserver, d'une manière qui garantisse leur recevabilité à titre de preuves lors d'une procédure judiciaire

ultérieure. Dans la mesure du possible, les services nationaux de détection et de répression devraient élaborer, soit directement avec les FAI soit avec les organismes équivalents d'autres pays, des procédures claires, comportant des éléments tant formels qu'informels, visant à assurer le plus rapidement possible la conservation et la production des données d'usage Internet requises dans une enquête criminelle.

300. Aux États-Unis, où sont hébergés la plupart des principaux FAI, les autorités ont recours à une "double" approche pour aider leurs homologues étrangères en matière de conservation et de production des données relatives à Internet détenues par les FAI basés dans leur pays, à d'éventuelles fins probatoires. Selon cette méthode, les demandes étrangères de conservation et de production des informations relatives aux comptes utilisateurs des fournisseurs d'accès à l'Internet pourraient être gérées de deux manières:

a) *Processus informels*. Les autorités chargées d'une enquête peuvent garantir la conservation par des moyens informels de données relatives à Internet détenues aux États-Unis de deux façons: i) les autorités étrangères établissent une relation avec le FAI concerné et lui demandent directement et de manière informelle de conserver les données requises; ou ii) en l'absence de relation directe, elles effectuent une demande informelle via le FBI (Federal Bureau of Investigation), qui présentera la requête au FAI;

b) *Processus formels.* Dans ce cas, les autorités étrangères effectuent une demande formelle d'entraide judiciaire concernant les données relatives à un compte d'utilisateur donné, qui transite par le Bureau des affaires internationales du Ministère de la justice américain. À réception, la demande est examinée par la section chargée de la lutte contre le terrorisme, qui détermine si elle est liée à une enquête menée aux États-Unis. Dans la négative, la requête est soumise à un tribunal fédéral afin d'obtenir le mandat autorisant la collecte et la transmission des informations requises aux autorités du pays requérant.

301. La méthode susmentionnée de production des données se rapportant aux FAI a été utilisée avec succès par les autorités britanniques et américaines dans plusieurs enquêtes sur le terrorisme. Dans une espèce, cette procédure a permis à un FAI basé aux États-Unis de fournir une cache importante de données Internet qui ont constitué des preuves déterminantes dans des poursuites menées au Royaume-Uni.

F. Défis et problèmes

302. Par nature, l'empreinte géographique virtuelle, la structure éclatée et les technologies en constante évolution associées à Internet constituent des défis et des problèmes permanents pour les autorités de détection, de répression et de justice pénale chargées des enquêtes et des poursuites en matière de terrorisme. La discussion intervenue lors de la réunion du groupe d'experts a mis en relief certains domaines qui posent problème en termes de coopération internationale. Ces points comprennent la difficulté, dans certains cas, à satisfaire les exigences de double incrimination dans les demandes d'extradition et d'entraide judiciaire. De nombreux experts ont été confrontés à des affaires dans lesquelles les demandes d'entraide judiciaire ou d'extradition ont été

retardées ou rejetées à cause d'une difficulté à satisfaire cette exigence. Dans certains cas, cette difficulté résultait d'une incompatibilité entre les dispositions relatives à l'infraction pénale, mais dans d'autres, elle découlait d'une conception trop restrictive de l'interprétation par les magistrats des dispositions relatives à l'incrimination. Plusieurs experts ont estimé que cette situation mettait en évidence la nécessité de formation des magistrats sur les questions de coopération internationale.

1. Protection des informations sensibles

303. Lors de la réunion du groupe d'experts, les spécialistes de plusieurs pays ont fait état des défis permanents liés au partage par les services nationaux de détection, de répression et de renseignement d'éléments sensibles avec leurs homologues étrangers. Dans les affaires de terrorisme, les enquêtes criminelles et les poursuites pénales reposent inévitablement sur le renseignement, au moins à leur début, et touchent à des informations sensibles qui sont détenues par quelques personnes et étroitement protégées. La divulgation de telles informations comporte des risques considérables, non seulement pour leur source mais également pour l'organisme ou les organismes qui les détiennent, en particulier si cette divulgation risque ou est susceptible de compromettre une enquête ou une opération en cours ou à venir.

304. Pour les autorités nationales, l'évaluation du fait de savoir s'il faut partager ces informations et dans quelles circonstances ou conditions peut s'avérer une tâche complexe, car elle les contraint à concilier un certain nombre de facteurs. Néanmoins, quels que soient les critères retenus, l'organisme divulguant ces informations doit, dans tous les cas et indépendamment des circonstances, être certain que l'organisme qui les reçoit fournit les garanties et mesures de protection convenues aux informations détenues.

2. Souveraineté

305. Le concept de souveraineté, et notamment le droit des nations de déterminer leur propre statut politique et d'exercer une souveraineté permanente dans les limites de leur compétence territoriale, constitue un principe largement reconnu en droit international et au titre des relations internationales. Les affaires nécessitant une enquête ou des poursuites concernant les activités transfrontalières de terroristes ou d'autres criminels pourraient avoir des implications en matière de souveraineté dans les pays où des investigations doivent être effectuées.

306. Dans certains cas, les préoccupations, légitimes ou non, des autorités nationales à propos du sentiment d'intrusion dans la souveraineté de leur État peuvent limiter l'efficacité de la coopération internationale en matière pénale. Par conséquent, il importe que les enquêteurs et les procureurs, lorsqu'ils envisagent de mener des actions impliquant la collecte de preuves relatives aux ordinateurs ou à l'Internet, soient attentifs aux implications que ces actions pourraient avoir en termes de souveraineté sur d'autres États (par exemple, autorités d'un pays perquisitionnant à distance l'ordinateur utilisé par un suspect qui se trouve dans un autre pays).

307. De manière générale, les autorités nationales envisageant des mesures d'enquête relatives à des personnes ou des objets qui se trouvent dans un autre pays devraient, dans la mesure du possible, en informer leurs homologues du pays concerné et coordonner leurs actions avec elles.

3. Conservation et production de données relatives à Internet

308. Comme nous l'avons déjà indiqué, dans de nombreuses affaires de terrorisme, une part importante des preuves contre les suspects se rapporte à certains aspects de leur activité sur Internet (par exemple, informations de facturation de carte de crédit et données d'usage relatives aux communications sur Internet, telles que courriers électroniques, VoIP, Skype, ou aux réseaux sociaux ou autres sites Web). Dans de nombreux cas, les autorités chargées de l'enquête devront veiller à ce que les données Internet soient conservées et préservées pour être ultérieurement utilisées à titre de preuves dans la procédure. À cet égard, il importe de relever la distinction entre la notion de "conservation" des données et celle de "préservation" des données. Dans de nombreux pays, la loi contraint les FAI à conserver certains types de données pendant une période spécifiée. En revanche, la préservation fait référence à l'obligation imposée à un FAI, conformément à une ordonnance judiciaire, un mandat ou une instruction, de préserver les données dans des conditions précisées pour qu'elles soient produites à titre de preuves dans une procédure pénale.

309. L'un des principaux problèmes rencontrés par tous les services de détection et de répression est l'absence de cadre internationalement reconnu de conservation des données détenues par les FAI. Les gouvernements de nombreux pays ont imposé des obligations juridiques aux FAI locaux en la matière, mais à l'échelle internationale, il n'existe pas de période uniformisée, unique, universellement convenue de conservation.

310. Dès lors, si les enquêteurs des pays ayant imposé aux FAI des obligations de conservation des données n'ont guère de doute, dans les enquêtes purement nationales, quant au type de données Internet conservées et au délai de conservation, il en va différemment des enquêtes dans lesquelles ils doivent collecter des données détenues par un FAI d'un autre pays.

311. Aux États-Unis, l'optique actuelle consiste à contraindre les FAI à conserver les données d'usage sur demande spécifique des services de détection et de répression, les prestataires appliquant des politiques très variables de stockage des données, dont la durée peut aller de quelques jours à plusieurs mois.

312. Des efforts ont été faits, notamment au sein de l'Union européenne, pour parvenir à une certaine cohérence, mais cette question s'est avérée problématique, y compris dans ce cadre. En vertu de la directive 2006/24/CE du Parlement européen et du Conseil de l'Union européenne du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, les États membres de l'Union européenne sont tenus, lorsqu'ils prennent des mesures concernant la conservation des données détenues

par les prestataires de services de communications électroniques et de réseaux publics de communication, de s'assurer que les prestataires réglementés conservent les données relatives aux communications spécifiées pendant une période comprise entre six mois et deux ans. Néanmoins, malgré cette directive, il n'existe pas de période de conservation unique et cohérente, applicable à tous les FAI hébergés au sein de l'Union européenne, puisque cette période est comprise entre six mois et deux ans. Par conséquent, le doute est moindre dans le contexte de l'Union européenne, mais il existe des disparités entre les durées de conservation.

313. Plusieurs participants à la réunion du groupe d'experts ont estimé que l'élaboration d'un cadre réglementaire universellement accepté, imposant des obligations cohérentes à tous les FAI quant au type et à la durée de conservation des données d'usage des clients, serait extrêmement utile aux services de détection, de répression et de renseignement qui enquêtent sur les affaires de terrorisme.

314. En l'absence de normes ou d'obligations universellement acceptées et imposées aux FAI et autres prestataires de communication en la matière, il importe que les enquêteurs et les procureurs déterminent le plus tôt possible si de telles données existent et pendant quel délai, si elles sont pertinentes dans le cadre des poursuites et où elles se trouvent, ainsi que la durée, le cas échéant, pendant laquelle elles doivent être conservées par la partie qui les détient. En cas de doute, il est prudent que les autorités contactent leurs homologues du pays où se trouvent les données et prennent les mesures (formelles et informelles) nécessaires pour assurer la préservation des données aux fins de production éventuelle. En fonction des circonstances, et notamment de leur connaissance du FAI pertinent ou de leurs relations avec celui-ci, les autorités pourraient envisager de contacter directement le FAI et de demander une assistance informelle. Cependant, compte tenu du caractère délicat des questions de confidentialité des informations relatives aux clients et des lois nationales relatives à la vie privée, le niveau de réactivité des FAI à ces demandes directes et informelles risque d'être extrêmement variable. Dans tous les cas, il serait prudent que les enquêteurs et les procureurs communiquent et coordonnent leurs efforts avec leurs homologues étrangers pour garantir la préservation et la production de ces informations.

4. Exigences en matière de preuves

315. Pour que les témoignages, pièces ou autres informations soient recevables dans une procédure pénale, les enquêteurs et les procureurs doivent veiller avec le plus grand soin à ce que la méthode utilisée pour collecter, préserver, produire ou transmettre les preuves soit pleinement conforme aux lois, aux principes juridiques et aux règles de preuve applicables. Un défaut d'observation des exigences relatives à la recevabilité des preuves peut affaiblir l'accusation, au point que les autorités se voient parfois contraintes de suspendre ou de retirer les charges. Dans l'affaire *Namouh*, les procureurs canadiens ont pu, grâce à une étroite collaboration avec leurs homologues autrichiens, faire en sorte que les preuves indispensables relatives à l'utilisation par les accusés de forums de discussion et de sites Web soient collectées et transmises au Canada et y soient recevables, alors même qu'il existait entre les deux pays des disparités en matière de règles de preuve.

316. Dans les affaires de terrorisme, de nombreuses questions peuvent poser aux autorités de considérables difficultés en matière de recevabilité de certains types d'informations. Surmonter ces difficultés reste un défi permanent pour tous les praticiens intervenant dans les enquêtes et les poursuites concernant les affaires de terrorisme, qui présentent souvent des caractéristiques susceptibles de porter atteinte à la recevabilité des informations. Le caractère transnational des affaires de terrorisme, y compris l'utilisation fréquente de renseignements (souvent fournis par des partenaires étrangers dans des conditions strictes) ou le recours à des méthodes extrêmement spécialisées, souvent clandestines et intrusives, de perquisition, de surveillance et d'interception pour recueillir les preuves, risque de constituer un obstacle important pour les autorités qui cherchent à présenter des preuves recevables à une cour de justice ou à un tribunal.

317. Dans le contexte du terrorisme, et notamment en ce qui concerne les questions de preuves relatives à l'Internet ou à la technologie informatique, l'approche générale adoptée par les enquêteurs et les procureurs reste la même. Parmi les questions particulièrement importantes figureront probablement la nécessité d'assurer, le plus rapidement possible, la possession physique des ordinateurs ou appareils similaires présumés utilisés par les suspects, et celle de mettre en œuvre les mesures adaptées, conformément aux bonnes pratiques reconnues, pour protéger l'intégrité de ces pièces (à savoir, la chaîne de conservation et de preuves) et engager les opérations de criminalistique numérique. Le non-respect de ces procédures pourrait avoir une incidence sur la recevabilité de ce type de preuves. Parmi les autres preuves susceptibles de nécessiter une attention particulière, on peut citer le matériel obtenu à la suite d'une perquisition et/ou d'activités de surveillance, opérations qui ne doivent intervenir que dans les conditions définies par l'autorisation judiciaire appropriée.

318. Lorsque les enquêteurs gèrent des questions de preuves, il est important qu'ils aient une compréhension suffisante des règles et principes juridiques applicables aux mesures qu'ils prennent et/ou qu'ils communiquent étroitement avec les procureurs, à la fois en les tenant informés et en leur demandant des avis juridiques. Lorsque les autorités d'un pays recueillent des preuves qui seront utilisées dans le cadre de poursuites engagées dans un autre pays, une communication et une coordination étroites avec leurs homologues étrangères quant aux mesures prises pour collecter et préserver ces preuves sont essentielles. Dans le cadre de cette coordination, il importe que les autorités qui prennent des mesures d'enquête comprennent clairement les exigences et implications liées à leurs actions dans le pays où les preuves seront finalement utilisées. Les questions liées à la recevabilité des preuves étrangères dans les affaires de terrorisme sont abordées de manière plus détaillée dans le *Recueil de cas sur les affaires de terrorisme* de l'ONUDC[153].

5. Double incrimination

319. Parmi les points fréquemment visés dans les instruments universels de lutte contre le terrorisme et les autres instruments internationaux, régionaux et bilatéraux relatifs au

[153]Voir Office des Nations Unies contre la drogue et le crime, *Recueil de cas sur les affaires de terrorisme*, par. 292 à 295.

terrorisme et à la criminalité transnationale organisée, figure la disposition selon laquelle seule une conduite illégale qui constitue une infraction pénale à la fois dans l'État requérant et dans l'État requis peut constituer la base d'une coopération internationale. Cette exigence, dite de "double incrimination", peut présenter des difficultés dans l'ensemble des enquêtes et poursuites pénales impliquant un élément quelconque de coopération internationale (et pas uniquement celles qui se rapportent au terrorisme). Plusieurs participants à la réunion du groupe d'experts ont indiqué que la question de la double incrimination constituait un problème fondamental et persistant, qui conduisait souvent au rejet des demandes d'entraide judiciaire ou d'extradition lorsque les autorités du pays requis estimaient que cette exigence n'avait pas été satisfaite.

320. Dans le contexte du terrorisme, en l'absence d'obligation universelle des États d'incriminer certains actes illégaux commis sur Internet, les autorités centrales se fonderont probablement, lorsqu'elles présenteront ou recevront des demandes de coopération internationale, sur les infractions pénales établies en vertu de leur législation relative au terrorisme ou de leur Code pénal national. Par exemple, en cas d'allégations d'actes d'incitation au terrorisme commis sur Internet, il peut s'avérer nécessaire, en raison des différences d'approches juridiques adoptées par les États, de fonder les demandes de coopération internationale sur des infractions inchoatives comme l'incitation.

321. Il est souhaitable que les gouvernements, lorsqu'ils se penchent sur cette question et qu'ils incriminent les conduites illégales associées au terrorisme, formulent les infractions en des termes aussi proches que possibles de ceux qui sont employés dans les instruments pertinents. De surcroît, dans la mesure autorisée par les systèmes juridiques nationaux, la législation ne devrait pas être rédigée de façon trop restrictive concernant la question de la double incrimination; elle fournirait ainsi aux autorités centrales et aux juges un champ d'application suffisant sur lequel s'appuyer, et leur permettrait d'évaluer la substance des actes illégaux objet de la demande et de ne pas se fonder sur une approche trop étroite. Si les États adoptent cette méthode de manière uniforme, tous les avantages de l'harmonisation législative visée par ces instruments seront acquis et le risque de problèmes relatifs à la double incrimination diminuera.

322. Si les questions concernant la double incrimination peuvent créer des difficultés dans les affaires pénales impliquant une coopération internationale de façon générale, elles risquent de s'avérer particulièrement problématiques dans les espèces concernant certaines infractions relatives au terrorisme commises au moyen d'Internet (par exemple, incitation), dans lesquelles le risque d'incompatibilité entre le cadre législatif et constitutionnel national des États correspondants est plus important. Lors de la réunion du groupe d'experts, l'exemple de la position des États-Unis en matière d'extradition des personnes accusées d'incitation a été évoqué. Dans ce pays, il existe de solides garanties constitutionnelles relatives à la liberté d'expression, qui sont énoncées par le Premier amendement à la Constitution des États-Unis. En vertu du droit américain, les déclarations constituant un plaidoyer indépendant en faveur d'une position idéologique, religieuse ou politique ne sont pas considérées comme des actes criminels en soi, même si elles constituent des actes équivalant à la communication d'informations en vue ou afin de contrôler une organisation terroriste, ou entrent dans le champ d'application de l'infraction d'incitation. Du fait de cette position, les demandes d'entraide judiciaire

ou d'extradition relatives à des allégations d'actes d'incitation impliquant un élément constitutif survenu aux États-Unis pourraient poser problème en matière de double incrimination, et exiger des autorités des deux pays qu'elles adoptent une approche souple et pragmatique.

323. Outre l'existence d'une législation compatible et l'adoption d'une démarche souple pour l'appliquer, il est important que les enquêteurs, les procureurs et les magistrats soient bien formés et qu'ils comprennent la manière dont les mécanismes de coopération internationale s'inscrivent dans la riposte de la communauté internationale au terrorisme et à la criminalité transnationale organisée.

6. Disparités en matière d'application des garanties constitutionnelles et relatives aux droits de l'homme

324. Les questions relatives aux garanties constitutionnelles et aux droits de l'homme touchent à de nombreux éléments associés aux enquêtes et aux poursuites relatives au terrorisme, notamment liés à la coopération internationale. Là encore, sur la base de l'exemple des actes relatifs à l'incitation au terrorisme, il apparaît que des conceptions nationales différentes de l'application des droits constitutionnels et/ou des droits de l'homme peuvent se traduire en approches juridiques distinctes. Cette disparité peut créer des difficultés dans les affaires de coopération internationale où les États cherchent à demander ou fournir une assistance. Par exemple, lorsque les autorités d'un pays présentent à leurs homologues d'un autre pays une demande concernant des données relatives à des déclarations qui ont été faites sur Internet et qui constituent une incitation à commettre des actes de terrorisme dans leur juridiction, il est très pertinent de savoir si les actes allégués constituent également une infraction dans le pays requis. Dans le contexte plus large du contrôle d'Internet, lorsque les autorités d'un pays demandent la suppression d'un contenu qui, selon elles, incite au terrorisme et qui est hébergé sur un serveur situé dans un autre pays, il est possible que les lois applicables et les garanties constitutionnelles concernant des droits tels que la liberté d'expression soient différentes.

325. La situation concernant certains types de courriers électroniques ou de contenus Internet relatifs au terrorisme acheminés via des FAI implantés aux États-Unis, ou stockés sur leurs serveurs, est particulièrement pertinente. En fonction de la nature et du contexte de ces contenus, ces affaires, qui relèvent de la compétence des États-Unis, peuvent poser problème compte tenu des solides garanties accordées à la liberté d'expression par le Premier amendement à la Constitution des États-Unis. Dans ces affaires, les autorités des différents pays doivent communiquer étroitement pour déterminer les mesures pouvant, le cas échéant, être prises à titre préventif ou en termes de poursuites, ces mesures devant être conformes à leurs lois nationales, leurs normes juridiques et culturelles, et leurs obligations internationales de lutte contre le terrorisme respectives.

7. Compétence concurrente

326. Les affaires de terrorisme dans lesquelles les actes constitutifs d'infraction sont commis sur Internet soulèvent parfois des questions complexes de compétence, en

particulier lorsqu'un suspect se trouve dans un pays et utilise des sites Internet ou des services hébergés par des FAI situés dans un autre pays. On a observé de nombreux cas où des personnes résidant dans un pays avaient créé, administré et maintenu dans un autre pays des sites Web en vue de promouvoir le djihad et à d'autres fins liées au terrorisme.

327. L'affaire belge *Malika El Aroud* et al. (voir par. 377) en est un exemple. L'intéressée, qui vivait en Belgique, administrait un site Web hébergé au Canada, qu'elle utilisait pour promouvoir le djihad et à d'autres fins visant à soutenir des activités terroristes. Dans ce type de situation, le succès des poursuites dépend fortement de l'efficacité de la coopération internationale.

328. Le droit international ne prévoit pas de règle contraignante régissant la manière dont les États devraient gérer les situations dans lesquelles plusieurs d'entre eux pourraient faire valoir leur compétence pour connaître d'une infraction impliquant le même suspect. Les États disposent d'un large pouvoir discrétionnaire quant aux critères appliqués, mais ils doivent généralement mettre en balance ou évaluer différents facteurs. Ces facteurs peuvent comprendre la "connectivité" existant entre l'infraction alléguée et les États concernés, notamment la nationalité du suspect, le lieu où les différents actes constitutifs de l'infraction se sont déroulés, l'endroit où se trouvent les témoins et les preuves pertinents, et les difficultés éventuelles de collecte, de transmission ou de production des preuves dans un pays donné. Dans certains États, dont la Belgique, le Canada et l'Espagne, certaines formes de compétence juridictionnelle sont considérées comme subsidiaires à d'autres. Les États ayant des liens étroits avec une infraction (par exemple, si celle-ci est commise sur leur territoire ou par l'un de leurs ressortissants) sont considérés comme dotés d'une compétence principale, tandis que les États compétents sur d'autres fondements n'interviennent que lorsque l'État doté d'une compétence principale n'est pas disposé ou en mesure de poursuivre l'infraction[154].

329. Certains pays, dont le Canada, appliquent le critère "du rapport réel et substantiel" pour déterminer s'ils sont compétents sur le plan pénal[155]. En Israël, lorsqu'une demande de coopération internationale est reçue, elle fait l'objet d'une enquête à l'échelle nationale visant à définir s'il peut être prouvé qu'une infraction qui devrait être poursuivie en vertu du droit israélien a été commise. Si cette enquête ne débouche pas sur des poursuites, les autorités israéliennes transmettront par les voies formelles toutes les preuves disponibles [et transféreront le délinquant suspecté] au pays requérant pour que l'infraction y soit poursuivie. Au Royaume-Uni, la législation et la jurisprudence portant sur certaines infractions relatives au terrorisme et impliquant des activités commises en dehors du pays (notamment via l'Internet) autorisent les autorités britanniques à faire valoir leur compétence s'il peut être démontré qu'une "mesure substantielle" (*substantial measure*) des activités constituant l'infraction a eu lieu au Royaume-Uni, et que l'on peut raisonnablement soutenir que ces poursuites ne devraient pas être gérées par un autre pays.

[154] Association internationale du barreau, Legal Practice Division, *Report of the Task Force on Extraterritorial Jurisdiction* (2008), p. 172 et 173.

[155] *R.* c. *Hape* [2007] 2 SCR.292, 2007 SCC 26, par. 62.

330. Pour résoudre les problèmes de compétence concurrente ou de coopération internationale connexe, les autorités centrales (souvent les procureurs) doivent être très tôt conscientes de la nécessité d'une communication immédiate et commune avec leurs homologues d'autres pays qui pourraient avoir intérêt à engager une procédure contre le même suspect. La décision relative au moment et à la manière d'engager cette communication devrait être prise au cas par cas, en fonction des divers facteurs en jeu dans l'espèce donnée. Sur ces questions, les procureurs peuvent trouver des conseils dans le document intitulé "Attorney General's Domestic Guidance for Handling Criminal Cases affecting both England, Wales or Northern Ireland and the United States of America", publié en 2007 par le Procureur général du Royaume-Uni et celui des États-Unis[156], qui prévoit, dans le contexte des "affaires criminelles les plus graves, les plus sensibles ou les plus complexes" (auxquelles le document se rapporte) une amélioration du partage d'informations et de la communication entre les procureurs des deux pays. Comme critère de prise de contact, le rapport indique ce qui suit: "apparaît-il qu'il existe une réelle possibilité qu'un procureur de [autre pays] puisse avoir un intérêt à poursuivre l'affaire? Une telle affaire aurait habituellement des liens avec [autre pays]". Bien que le moment et le mode de communication concernant les questions de compétence et de coopération internationale varient en fonction des circonstances, les procureurs pourraient considérer ce critère comme susceptible de les guider dans leur travail.

8. Lois nationales relatives à la vie privée et à la protection des données

331. La législation nationale relative à la protection des données ou à la vie privée restreint souvent la capacité des services de détection, de répression et de renseignement à partager des informations avec leurs homologues nationaux et étrangers. Là encore, la conciliation du droit humain à la vie privée et de l'intérêt légitime de l'État à enquêter et à poursuivre avec efficacité les infractions constitue un défi permanent pour les gouvernements et, dans certains cas (notamment en matière de réponses au terrorisme), une source de préoccupation[157].

332. Outre une législation fournissant des indications précises aux enquêteurs, aux procureurs et (dans le cas des données Internet) aux FAI détenant des données à propos des obligations liées à la collecte et à l'utilisation de données personnelles, il importe que le pays établisse et actionne des mécanismes efficaces de surveillance des services de renseignement, de détection et de répression. Les gouvernements devraient veiller à ce que les mécanismes adaptés soient intégrés dans leur droit interne pour permettre aux autorités de partager avec leurs homologues nationales et étrangères, sous réserve des garanties relatives à la vie privée appropriées, les informations pertinentes dans le cadre des enquêtes et des poursuites concernant les affaires de terrorisme.

[156] Disponible à l'adresse: www.publications.parliament.uk/pa/ld200607/ldlwa/70125ws1.pdf.

[157] Voir le rapport de 2009 du Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste (A/HRC/10/3), dans lequel le Rapporteur spécial a exprimé ses préoccupations concernant l'immixtion dans les droits individuels à la vie privée consécutive à une surveillance accrue et à un partage des renseignements entre les organismes publics.

9. Demandes fondées sur un traité versus *demandes non fondées sur un traité*

333. À l'échelle nationale, les approches visant à faciliter les demandes de coopération non fondées sur un traité diffèrent, certains pays ayant une capacité restreinte à fournir une coopération formelle en l'absence de traité. C'est pourquoi les instruments universels contre le terrorisme et la criminalité transnationale organisée contiennent des dispositions visant à faire en sorte que ces instruments soient eux-mêmes considérés comme le fondement juridique de la coopération et que certains actes illégaux soient réputés constituer des infractions remplissant les conditions requises aux fins d'entraide judiciaire et d'extradition dans le droit interne des États parties.

334. De nombreux pays, dont la Chine, se fondent sur le principe de réciprocité pour fournir une coopération internationale. En vertu du droit chinois, les services de détection et de répression et les autorités judiciaires peuvent mettre en œuvre une coopération internationale, y compris une entraide ou une coopération judiciaire (extradition incluse), sur la base d'un traité. En l'absence de traité, la réciprocité peut constituer un fondement juridique de coopération en matière d'entraide et d'extradition. Lors de la réunion du groupe d'experts, le spécialiste chinois a exposé un exemple de coopération réussie entre les autorités de son pays et les autorités américaines. Cette coopération a entraîné la fermeture du plus important site Web pornographique en langue chinoise du monde, qui était hébergé aux États-Unis et visait les utilisateurs d'Internet en Chine et dans d'autres pays d'Asie.

335. Plusieurs participants à la réunion du groupe d'experts ont mentionné les questions liées au caractère sensible de la plupart des informations (souvent fondées sur le renseignement) associées aux enquêtes relatives au terrorisme, et les difficultés inhérentes, non seulement dans le contexte international mais également à l'échelle nationale, rencontrées par les organismes qui souhaitent partager ces informations avec leurs homologues. Plusieurs experts ont souligné que ces informations étaient souvent extrêmement sensibles et qu'il était difficile de les partager en l'absence de mécanisme d'échange formel, assorti de conditions appropriées d'utilisation et de divulgation.

336. Nous examinerons cette question de façon plus détaillée dans le prochain chapitre, relatif aux poursuites, dans le contexte des questions liées à la conversion de matériel de renseignement en preuves recevables et à la communication de preuves dans les procédures pénales.

VI. Poursuites

A. Introduction

337. Un aspect essentiel du cadre juridique universel contre le terrorisme, et de la Stratégie antiterroriste mondiale des Nations Unies, concerne l'obligation faite aux États de refuser l'asile aux auteurs d'actes terroristes, et de les traduire en justice quel que soit l'endroit où ces actes se produisent. Pour atteindre ce dernier objectif, les pays doivent disposer non seulement d'une législation efficace qui incrimine les actes terroristes et facilite la coopération internationale, mais également d'une capacité à mettre en œuvre des techniques d'enquête spécialisées et des stratégies visant à assurer la collecte, la préservation, la production et la recevabilité des preuves (souvent fondées sur le renseignement) lorsqu'ils exercent des poursuites à l'encontre de personnes soupçonnées de terrorisme, tout en garantissant le respect des normes internationales de traitement des accusés.

338. Le rôle des procureurs dans les affaires de terrorisme est de plus en plus complexe et exigeant. Outre la responsabilité de la procédure pénale, les procureurs sont davantage impliqués dans les phases d'enquête et de collecte de renseignements, puisqu'ils donnent des indications sur les implications juridiques et stratégiques des diverses techniques d'enquête ou les contrôlent. Dans le présent chapitre, nous examinerons le rôle des procureurs dans les affaires impliquant l'utilisation d'Internet par les terroristes, en vue de déterminer, du point de vue d'un procureur, les défis ou les obstacles communs, ainsi que les stratégies et les méthodes qui se sont avérées efficaces pour poursuivre avec succès les auteurs d'infractions.

B. Une approche des poursuites pénales fondée sur l'état de droit

339. Des enquêtes et des poursuites qui ne sont pas menées en pleine conformité avec les principes généralement associés aux normes internationales relatives à l'état de droit et aux droits de l'homme mettent en danger l'intégrité même du tissu des normes et structures sociales et institutionnelles que les terroristes tentent de fragiliser. Par conséquent, il est fondamental d'exercer des poursuites à l'encontre des auteurs d'actes terroristes en mettant tout en œuvre pour assurer un procès équitable et un traitement équitable des accusés.

340. Le principe reconnu selon lequel le droit pénal devrait accorder aux personnes soupçonnées de terrorisme les mêmes garanties procédurales qu'aux autres suspects est fortement ancré et illustré dans les instruments universels contre le terrorisme et au niveau politique international. On peut citer l'un des nombreux exemples de

reconnaissance de haut niveau de ce principe: la résolution 59/195 de l'Assemblée générale, sur les droits de l'homme et le terrorisme, dans laquelle l'Assemblée a souligné la nécessité d'intensifier la coopération internationale contre le terrorisme, conformément au droit international, y compris aux droits internationaux de l'homme et au droit international humanitaire. En sus d'intégrer ce principe fondamental au niveau politique, l'Organisation des Nations Unies, par l'intermédiaire de son Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, rend régulièrement compte au Conseil des droits de l'homme et à l'Assemblée générale des sujets de préoccupation relatifs aux aspects des droits de l'homme des mesures de justice pénale visant le terrorisme, et effectue des recommandations pour que les acteurs pertinents prennent des mesures correctives. Le Rapporteur spécial a notamment soulevé des questions liées à la détention et à la mise en accusation des suspects[158].

341. Plusieurs publications traitent expressément du respect des droits de l'homme et de l'état de droit, et visent à promouvoir cet aspect, dans les attributions des procureurs et des agents de justice pénale intervenant en matière de terrorisme. En 2003, le Haut-Commissariat aux droits de l'homme a publié le *Récapitulatif de la jurisprudence de l'Organisation des Nations Unies et des organisations régionales concernant la protection des droits de l'homme dans la lutte antiterroriste*. Au sein du Conseil de l'Europe, qui a pleinement reconnu et intégré l'obligation de faire de la protection des droits de l'homme un principe fondamental dans les instruments portant sur la prévention de la criminalité et la justice pénale, et notamment le terrorisme, ce principe est réaffirmé dans les Lignes directrices du Comité des Ministres du Conseil de l'Europe sur les droits de l'homme et la lutte contre le terrorisme, adoptées le 11 juillet 2002[159]. Ces documents donnent des indications utiles aux procureurs qui interviennent dans le domaine de la lutte antiterroriste.

C. Rôle des procureurs dans les affaires de terrorisme

342. Le rôle du procureur en matière de procédure pénale, notamment dans les affaires de terrorisme, varie selon les pays. Dans certains cas, et en particulier dans les pays de droit romano-germanique, les procureurs sont officiellement chargés de contrôler la conduite des enquêtes criminelles, de superviser les équipes d'enquêteurs pendant toute l'enquête, de prendre des décisions concernant les perquisitions et les activités de surveillance, de porter des accusations ou de présenter des charges, de gérer les questions de coopération internationale et d'assurer la direction de la procédure devant les tribunaux.

343. Dans un système judiciaire de type inquisitoire comme le système français, le procureur est généralement chargé d'engager l'action judiciaire et d'ouvrir l'enquête

[158] Ibid.

[159] Tout texte créé au sein du Conseil de l'Europe, qu'il s'agisse d'une convention contraignante ou d'un instrument de "droit souple", tel qu'une recommandation ou une résolution adoptée par l'Assemblée parlementaire ou le Comité des Ministres, y compris toute directive sur divers sujets, doit être conforme à la jurisprudence abondante de la Cour européenne des droits de l'homme sur la question concernée.

préliminaire, en définissant l'étendue de l'infraction; cependant, un juge d'instruction mène l'enquête judiciaire officielle, et collecte et examine les preuves. Lorsque la culpabilité de la personne peut être exclue, le juge d'instruction rend un non-lieu; dans le cas contraire, un procès se déroule devant un autre juge. Dans les affaires de terrorisme, le procureur de la République peut, en sus de présenter les arguments de l'accusation au juge, déposer ou soumettre une requête concernant de nouvelles investigations.

344. Dans d'autres pays, en particulier ceux de *common law*, l'implication directe ou la responsabilité du procureur dans la conduite des enquêtes criminelles est traditionnellement moindre, puisque ces enquêtes sont habituellement menées par les services de détection et de répression. Dans ces pays, le procureur assume généralement la responsabilité officielle de la conduite des poursuites, depuis l'accusation ou présentation des charges jusqu'à l'issue finale de la procédure. Au Nigéria, par exemple, la police nationale est chargée de mener l'enquête criminelle. Une fois celle-ci achevée, l'affaire est transmise aux services de poursuite chargés de la mise en accusation et de la conduite de la procédure pénale.

345. Une approche similaire est adoptée en Indonésie, où il existe une séparation entre l'enquête et les poursuites. Après le début d'une enquête criminelle, l'enquêteur doit informer le procureur des progrès accomplis (art. 109, par. 1, du Code de procédure pénale indonésien) et, une fois l'enquête terminée, transmettre le dossier au procureur (art. 110, par. 1, du Code de procédure pénale), qui décidera si l'affaire doit faire l'objet d'un procès (art. 139 du Code de procédure pénale).

346. Quelles que soient les spécificités de la juridiction concernée, les procureurs voient leur rôle continuer d'évoluer dans les affaires de terrorisme et doivent répondre à des exigences accrues, consécutives aux développements permanents intervenant en matière de type, de méthode et de complexité des infractions terroristes, de lois de lutte antiterroriste, de techniques d'enquête et de dispositifs de coopération internationale.

347. L'expérience montre que les procureurs doivent intervenir de plus en plus directement dans les enquêtes, et pas simplement dans la phase des poursuites. Ils jouent un rôle plus technique et stratégique, non seulement en inspirant la politique et la législation de lutte contre le terrorisme mais également en fournissant au cours des enquêtes des conseils et des indications juridiques et stratégiques qui auront une influence sur le succès des poursuites. L'expérience montre qu'ils joueront probablement ce rôle dans le cadre d'une équipe multidisciplinaire et plurijuridictionnelle[160].

348. En outre, compte tenu de la visibilité accrue des poursuites en matière de terrorisme et de l'attention qui leur est portée, notamment de la couverture médiatique et du contrôle exercé par les groupes et les organismes internationaux de défense des droits de l'homme, les procureurs jouent un rôle crucial en veillant à ce que les enquêtes

[160]Yvon Dandurand, "The role of prosecutors in promoting and strengthening the rule of law", document présenté au deuxième Sommet mondial des magistrats et chefs de parquet, tenu à Doha du 14 au 16 novembre 2005.

et les poursuites soient non seulement menées de manière équitable, efficace et respectueuse des normes internationales de droits de l'homme, mais également perçues comme telles.

D. La phase d'enquête

349. Au cours de la phase de collecte de renseignements ou d'enquête des opérations antiterroristes, les procureurs sont souvent appelés à donner des conseils juridiques sur les questions liées à l'utilisation de techniques d'enquête spécialisées.

1. Techniques d'enquête spécialisées

350. Les nouvelles technologies et techniques de perquisition et de surveillance offrent aux services de renseignement, de détection et de répression des possibilités accrues de cibler les activités terroristes sur l'Internet, mais elles comportent également des risques juridiques dans le cadre des poursuites, auxquels les procureurs doivent rester constamment vigilants. En outre, compte tenu des disparités existant entre les droits nationaux en matière de collecte et de recevabilité des preuves, ces risques sont plus élevés lorsque les actes à l'origine des preuves ne se sont pas déroulés dans le pays où les poursuites sont exercées. Au niveau européen, le Conseil de l'Europe, conscient de ces risques et des questions de droits de l'homme sous-jacentes, a élaboré une recommandation relative aux techniques d'enquête spéciales en relation avec des infractions graves, y compris des actes de terrorisme[161], qui contient, entre autres, des principes généraux, des lignes directrices opérationnelles et un chapitre sur la coopération internationale.

351. Les risques juridiques connexes aux nouvelles techniques d'enquête renforcent la nécessité pour les procureurs d'intervenir le plus tôt possible dans les décisions prises pendant la phase d'enquête pour vérifier que les actions mises en œuvre pour collecter d'éventuelles preuves ne compromettent pas le succès des poursuites. Nous aborderons de façon plus détaillée les questions liées à la recevabilité des preuves ultérieurement dans le présent chapitre.

352. L'évolution rapide et constante des capacités techniques des services de renseignement, de détection et de répression en matière de surveillance des activités terroristes, ainsi que de contrôle et de collecte de renseignements ou de preuves, souligne l'importance déterminante du rôle du procureur concernant les conseils donnés aux enquêteurs sur les implications juridiques de ces actions en termes de poursuites. En outre, compte tenu de la nécessité croissante pour les autorités, particulièrement en cas d'activités transnationales liées à Internet, de se coordonner et de collaborer avec leurs homologues étrangères concernant les questions juridiques connexes (par exemple, la préservation de données relatives à Internet détenues par des FAI), il est de plus en plus important que les procureurs soient consultés et impliqués dès que possible dans les décisions relatives aux stratégies d'enquête.

[161] Comité des Ministres du Conseil de l'Europe, recommandation Rec(2005)10 (20 avril 2005).

2. *Le recours à des équipes multidisciplinaires*

353. Les autorités font de plus en plus appel à des équipes multidisciplinaires/pluri-institutionnelles, composées de membres des services de détection, de répression et de renseignement, ainsi que de procureurs, pour interdire, perturber et poursuivre les activités terroristes. Le haut niveau de confiance, de coordination et de communication qui, selon les participants à la réunion du groupe d'experts, est essentiel à une coopération internationale efficace, doit également exister entre les services nationaux de détection, de répression, de renseignement et chargés des poursuites. Il n'existe pas d'approche unique permettant de favoriser ces éléments, mais une bonne compréhension des mandats et du rôle des organismes contributeurs, des pouvoirs et des mécanismes de partage d'informations appropriés (reposant éventuellement sur des mémorandums d'accord ou des arrangements similaires), ainsi que des réunions de coordination ou des activités de formation régulières contribueront à renforcer ces importants partenariats nationaux.

354. Il existe des disparités dans la manière dont les autorités des différents pays coordonnent et gèrent les enquêtes pluri-institutionnelles, mais on observe de fortes similitudes. Aux États-Unis, les autorités emploient une méthode s'appuyant sur des équipes multidisciplinaires issues de tous les organismes compétents, y compris du ministère public, pour mener les enquêtes relatives au terrorisme.

355. Selon cette approche, les procureurs se joignent aux équipes des services de renseignement, de détection et de répression et autres organismes spécialisés qui contrôlent, évaluent et réévaluent en permanence les différents aspects des enquêtes menées sur les soupçons d'activités terroristes, et en font intégralement partie. Des équipes de travail antiterroristes et/ou des équipes de travail conjointes coordonnent les efforts des services de détection et de répression et des bureaux du procureur au niveau des États, et à l'échelon local et fédéral. De nombreux bureaux du procureur au niveau des États et à l'échelon fédéral participent à ces équipes de travail, et leurs méthodes et leurs tâches vont de la participation à des réunions interinstitutions à la co-implantation de personnel en passant par la prestation de conseils juridiques pour obtenir des mandats de perquisition, l'étude des affaires et l'émission de recommandations sur les chefs d'accusation[162].

356. Au Canada, les autorités font appel à des Équipes intégrées de la sécurité nationale (EISN). Dans l'affaire *Namouh*, l'EISN se composait de la Gendarmerie royale du Canada, de l'Agence des services frontaliers du Canada, du Service canadien du renseignement de sécurité, de la Sûreté du Québec, du Service de police de la Ville de Montréal et du Service des poursuites pénales du Canada.

357. Au Japon, il est courant que la police, même si elle est légalement indépendante, signale l'affaire au procureur dès le début d'une enquête relative au terrorisme, et le

[162] M. Elaine Nugent *et al.*, *Local Prosecutors' Response to Terrorism* (Alexandrie, Virginie, American Prosecutors Research Institute, 2005).

consulte lors de l'évaluation des preuves et de l'interprétation des lois[163]. L'Égypte a adopté une approche similaire.

358. Pour accroître l'efficacité des poursuites antiterroristes et en assurer le bon déroulement, les gouvernements créent souvent, au sein des organismes nationaux compétents, des départements ou des unités spécialisés. C'est le cas de l'Indonésie, qui a adopté un certain nombre de mesures spéciales, dont la création au sein du bureau du procureur général d'une équipe de travail en matière de terrorisme et de criminalité transnationale. Cette équipe de travail est chargée de faciliter et d'accélérer les activités de détection et de répression, pendant la phase d'enquête, en se coordonnant avec la police (par exemple, implication du procureur pendant l'interrogatoire des suspects), et lors des poursuites ultérieures, jusqu'à l'exécution finale de la décision du tribunal.

359. Au niveau international, il existe des disparités concernant les moyens utilisés par les procureurs pour intervenir et s'intégrer dans les enquêtes criminelles, mais la méthode générale adoptée dans de nombreux pays souligne l'opportunité d'une telle intégration et d'une approche globale et multidisciplinaire des décisions stratégiques et opérationnelles prises pendant la phase d'enquête des affaires de terrorisme.

E. Coopération internationale

360. Nous avons déjà abordé les questions liées à la coopération internationale dans le chapitre VI et il est inutile de les évoquer à nouveau. Les questions soulevées lors de la réunion du groupe d'experts et concernant spécifiquement les procureurs dans les affaires impliquant des éléments de coopération internationale se rapportent à la médiation et à la résolution des questions relatives au mode de coopération, aux problèmes de compétence, aux exigences de double incrimination et à la recevabilité des preuves étrangères, qui, d'après l'expérience vécue, présente un défi permanent. Tous les États ayant intérêt à poursuivre avec succès les infractions liées au terrorisme, il est important non seulement qu'ils aient mis en place les cadres législatifs nécessaires pour faciliter cette coopération mais également que les procureurs résolvent ces questions de manière proactive et collaborative.

F. La phase d'accusation

1. Décisions sur l'opportunité de poursuivre

361. Dans la plupart des pays, les procureurs disposent d'un large pouvoir d'appréciation pour décider s'ils doivent engager une procédure pénale, et sur quels chefs d'accusation. Ces décisions sont souvent prises conformément aux lignes directrices ou aux codes qui visent à assurer l'exercice juste, transparent et cohérent de ce pouvoir discrétionnaire. À titre d'exemple, les procureurs britanniques s'appuient sur le Code for Crown Prosecutors, qui prévoit un seuil d'accusation, fondé sur la suffisance des

[163] Office des Nations Unies contre la drogue et le crime, *Recueil de cas sur les affaires de terrorisme*, par. 212.

preuves et l'intérêt général. Ils doivent avoir acquis la conviction que les preuves produites montrent une "perspective réaliste de condamnation" ("*realistic prospect of conviction*") avant d'accuser un suspect[164]. L'Égypte a adopté une approche similaire.

362. Dans le contexte du terrorisme, l'intérêt général sera probablement un élément très important de la décision, étant donné la nécessité, dans tous les cas où cela est possible, de poursuivre les actes terroristes ou les infractions connexes pour protéger le public et prévenir des infractions similaires. Dans de nombreux cas, les questions liées à la suffisance des preuves disponibles constituent des facteurs déterminants, et la capacité à utiliser des éléments fondés sur le renseignement sans compromettre les sources et les méthodes de collecte ou les autres enquêtes aura une incidence sur ce point. Pour cette raison, les procureurs décident dans certains cas de poursuivre les suspects en vertu de chefs d'accusation non spécifiques au terrorisme afin de protéger l'intégrité du matériel de renseignement.

2. Recours aux infractions pénales générales ou non spécifiques au terrorisme

363. Dans les cas où elles doivent intervenir afin d'empêcher la commission d'actes terroristes avant d'avoir obtenu suffisamment de preuves pour engager des poursuites au titre des actes en cours de planification, les autorités doivent parfois s'appuyer sur d'autres dispositions pénales pour fonder juridiquement leurs actions. Dans de nombreuses espèces où les suspects ont utilisé l'Internet dans le cadre d'activités criminelles, les autorités ont eu recours avec succès à des infractions pénales telles que l'incitation, l'entente criminelle, la participation à un groupe terroriste ou le fait de lui fournir un soutien matériel, et non à des infractions matérielles liées aux actes terroristes dont la planification est en cours. Dans ce contexte, l'existence d'infractions telles que l'incitation, l'entente criminelle ou l'association de malfaiteurs est particulièrement utile. Dans certains cas, les autorités ont utilisé d'autres infractions pénales générales, telles que la fraude ou les infractions relatives à la possession ou à l'utilisation d'objets illégaux (par exemple, faux documents d'identité ou de voyage, armes), qui permettent aux enquêteurs et aux procureurs d'interrompre ou de compromettre les activités des groupes terroristes avant l'exécution des attaques ou des activités planifiées.

G. La phase du procès: questions de preuves

1. Questions relatives à l'utilisation de preuves fondées sur le renseignement

364. Pour les autorités, l'intégration des activités de renseignement dans les systèmes de justice pénale reste un problème fondamental en matière de lutte contre le terrorisme. Comme nous l'avons indiqué précédemment, dans de nombreuses affaires, les preuves utilisées par l'accusation proviennent de sources fondées sur le renseignement. Lors des poursuites, les autorités de tous les pays sont fréquemment confrontées à la difficulté

[164] Crown Prosecution Service, "The Code for Crown Prosecutors" (Londres, 2010). Disponible à l'adresse: www.cps.gov.uk/publications/docs/code2010english.pdf.

de protéger le matériel sensible étayant ce type de preuves tout en respectant l'obligation de garantir aux accusés un procès équitable et une défense effective, et notamment de communiquer à la défense tous les arguments pertinents de l'accusation.

2. Questions relatives à la collecte et à l'utilisation de preuves numériques

365. Dans les affaires de terrorisme impliquant l'utilisation d'ordinateurs, d'appareils similaires ou de l'Internet, les preuves numériques constituent une partie importante de l'accusation. Lorsque le suspect n'était pas physiquement présent à l'endroit où l'acte terroriste s'est produit, mais a néanmoins soutenu sa commission via une action quelconque sur l'Internet, la production d'éléments montrant ses "empreintes digitales numériques" peut constituer une preuve irréfutable de sa complicité et de sa culpabilité.

366. L'expérience montre que l'utilisation de preuves numériques soulève inéluctablement des questions relatives à leur recevabilité. Par conséquent, il est essentiel de veiller, tout au long de l'enquête et des poursuites, à la parfaite conformité des méthodes de collecte, de préservation, d'analyse et de production de ces éléments aux règles probatoires ou procédurales pertinentes, et au respect des bonnes pratiques établies.

367. Les preuves numériques sont parfois complexes sur le plan technique et font intervenir des termes et des concepts que le juge, le jury ou le tribunal chargé de statuer ne connaît pas bien. Les procureurs doivent examiner, en étroite coordination avec les enquêteurs et les experts, la meilleure manière de présenter ces preuves, d'une façon qui soit facile à comprendre et incontestable. À cet égard, l'utilisation de diagrammes et d'aides visuelles similaires montrant les mouvements de données ou les liens entre les ordinateurs et les utilisateurs pourrait s'avérer utile.

368. En cas de poursuites fondées sur une forme ou une autre d'utilisation d'un ordinateur, le parquet devra montrer dans son argumentation que l'accusé était bien, au moment déterminant, l'utilisateur de l'ordinateur, de l'appareil ou du service Internet utilisé pour commettre l'infraction, et établir les liens prouvant ce fait. Il peut le faire de plusieurs manières: *a)* l'accusé peut faire une confession ou admettre les faits; *b)* la présence de l'accusé devant l'ordinateur peut être établie par des moyens indirects (par exemple, il était la seule personne présente à l'endroit où l'ordinateur se trouvait, il était au moment déterminant l'utilisateur enregistré du matériel ou du logiciel en cause, ou l'ordinateur contient d'autres informations qu'il est le seul à connaître); ou *c)* le parquet peut analyser le contenu de l'appareil ou du service que l'accusé est présumé avoir utilisé. Cette démarche implique parfois que le procureur produise des preuves relatives aux caractéristiques du matériel découvert dans l'appareil (par exemple, un document) ou un commentaire effectué dans une communication interceptée qui est propre à l'accusé. Enfin, les timbres dateurs figurant sur les fichiers numériques peuvent permettre, bien qu'ils ne soient pas infaillibles, de relier de manière convaincante l'accusé à l'appareil considéré au moment déterminant de la commission d'une infraction[165].

[165] États-Unis, Ministère de la justice, Office of Justice Programs, National Institute of Justice, *Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors* (2007), chap. 4, sect. IV. Disponible à l'adresse: www.ncjrs.gov/pdffiles1/nij/211314.pdf.

369. Si les détails peuvent varier, l'approche générale adoptée par les tribunaux de nombreux pays pour déterminer la recevabilité des preuves dans un procès pénal repose sur la pertinence et la fiabilité: la preuve qu'une partie cherche à apporter est-elle pertinente, et est-elle fiable? Dans le cas d'une preuve numérique pertinente, le défi pour les procureurs consiste souvent à convaincre le tribunal de sa fiabilité, en termes à la fois de contenu et de méthode utilisée pour la recueillir et la produire. Le processus visant à convaincre un tribunal de la recevabilité d'une preuve numérique nécessite souvent de prouver la légalité des méthodes utilisées pour la recueillir et préserver son intégrité entre le moment de sa collecte et celui de sa production au tribunal. On nomme les procédures opérationnelles et juridiques de préservation de l'intégrité des preuves, la "chaîne de conservation" ou la "chaîne de preuves". Dans la plupart des pays, il existe des règles juridiques strictes relatives à cette chaîne, qui exigent que les preuves soient immédiatement enregistrées, centralisées, scellées et protégées contre toute contamination dans l'attente du procès, dans certains cas sous la surveillance d'un fonctionnaire judiciaire.

370. Dans les affaires de terrorisme impliquant la collecte et l'utilisation de communications interceptées ou de preuves criminalistiques numériques, les procureurs devraient vérifier, en étroite collaboration avec les services de renseignement, de détection et de répression, que ces preuves ont été recueillies en toute légalité, et préservées et produites d'une manière qui réponde aux exigences de la juridiction devant laquelle elles seront finalement utilisées. La collecte et la production de données numériques à titre de preuves recevables, en particulier lorsqu'elles sont détenues à distance par un suspect ou un tiers apparenté se trouvant dans un autre pays, sont des tâches difficiles pour les enquêteurs comme pour les procureurs. Outre les difficultés techniques liées au recueil et à la préservation de l'intégrité des données requises, la nécessité de s'appuyer dans certaines situations sur la coopération de services étrangers de renseignement, de détection, de répression ou chargés des poursuites, agissant en vertu de lois et de procédures différentes, peut rendre ces processus particulièrement longs et exigeants en termes de ressources.

371. Dans les enquêtes impliquant la collecte de données numériques se trouvant dans un seul pays, les questions relatives à la recevabilité risquent de tourner essentiellement autour du fondement juridique sur lequel elles ont été recueillies et de leur gestion et préservation ultérieures (à savoir, la chaîne de conservation ou de preuves). Comme toujours, il convient de veiller à ce que le fondement juridique de la collecte, de l'examen criminalistique, de la préservation et de la production de ces éléments soit pleinement conforme aux règles et procédures applicables à la recevabilité des preuves.

372. Lorsque les données numériques sont collectées dans un ou plusieurs pays pour être utilisées dans une procédure pénale menée dans un pays différent, la situation est nettement plus complexe et nécessite une attention toute particulière de la part des enquêteurs et des procureurs.

373. Dès que possible après avoir identifié la partie détentrice des données pertinentes dans le cadre d'une enquête et les avoir localisées dans un pays étranger, les enquêteurs et les procureurs devraient étudier les moyens formels et informels d'obtenir ces

données et de les préserver à des fins probatoires. Dans la mesure du possible, il convient de favoriser les voies informelles, pourvu que les méthodes de collecte, de préservation et de transmission au pays destinataire soient conformes aux règles et procédures applicables. Aux fins de collecte, les enquêteurs doivent parfois demander à leurs homologues étrangers d'obtenir des mandats de perquisition permettant de rechercher et de saisir les données ou envisager d'utiliser d'autres moyens (par exemple, pages Web accessibles à tous) ou de faire appel à des témoins étrangers volontaires.

374. Une affaire jugée en Allemagne en 2009 et ayant abouti à la condamnation de quatre membres de l'Union du Jihad islamique illustre la dimension et la complexité de nombreuses enquêtes et poursuites en matière de terrorisme. L'affaire, qui a donné lieu à une enquête de plus de neuf mois, a mobilisé plus de 500 policiers et nécessité beaucoup d'heures d'interception électronique et de surveillance, la collecte de nombreuses pièces et une coopération internationale approfondie entre les autorités allemandes et leurs homologues turques et américaines. La dimension et la complexité de cette affaire mettent en évidence l'importance des moyens qui sont parfois requis pour mener une enquête et exercer des poursuites, et la nécessité et les atouts d'une approche en équipe.

Fritz Gelowicz, Adem Yilmaz, Daniel Schneider et Atilla Selek

En septembre 2007, après une enquête de grande ampleur, les autorités allemandes, agissant sur la base de renseignements reçus de leurs homologues américaines, ont arrêté quatre membres de l'Union du Jihad islamique (souvent désignés sous le nom de "cellule du Sauerland"), qui étaient en train de finaliser les préparatifs d'une série d'attentats à l'explosif dans divers lieux publics en Allemagne. Les cibles étaient notamment des boîtes de nuit situées à Munich, Cologne, Francfort, Düsseldorf et Dortmund, ainsi que la base de la force aérienne américaine de Ramstein. Le volume total du matériel explosif que les accusés pensaient avoir rassemblé (les autorités l'avaient en fait clandestinement remplacé par une substance moins forte et inoffensive) était énorme, et aurait permis de commettre des attentats plus puissants que ceux de Madrid (2004) et de Londres (2005).

Trois des accusés (Gelowicz, Schneider et Selek) étaient Allemands, et le quatrième, Yilmaz, était Turc. Sur plusieurs mois, les intéressés avaient acquis 780 kg de peroxyde d'hydrogène auprès de fournisseurs légitimes. Le 4 septembre 2007, les autorités les ont arrêtés alors qu'ils se rencontraient dans une maison de vacances située dans la région allemande du Sauerland et commençaient à "préparer" le peroxyde d'hydrogène en y ajoutant d'autres ingrédients pour multiplier ses effets explosifs. (À leur insu, les autorités avaient auparavant remplacé la solution de peroxyde d'hydrogène par une solution moins forte et inoffensive.)

En août 2008, les procureurs fédéraux ont mis en accusation Gelowicz, Schneider et Yilmaz. Selek a été extradé de Turquie en novembre 2008 sur la base d'une demande d'extradition présentée en vertu de la Convention européenne d'extradition et a été mis en accusation en décembre 2008. Les chefs d'accusation étaient notamment les suivants: entente criminelle en vue de la commission d'un meurtre, préparation d'une explosion et appartenance à une organisation terroriste.

Le procès des quatre accusés a débuté en avril 2009, et au bout de trois mois, ces derniers ont décidé de reconnaître les faits qui leur étaient reprochés. La quantité de preuves que l'accusation avait l'intention de produire était considérable: 521 dossiers à feuillets mobiles (de quoi remplir un rayon d'étagère de 42 mètres) et 219 témoins. Une grande partie des arguments de l'accusation se rapportait au contrôle électronique et à la surveillance à grande échelle qui avaient été mis en œuvre par les autorités allemandes pendant l'enquête. Les techniques électroniques comprenaient la mise sur écoute de conversations entre les accusés, l'installation d'appareils d'écoute dans les véhicules et dans la maison où ils se rencontraient pour préparer le peroxyde d'hydrogène destiné à fabriquer l'engin explosif, ainsi que l'interception de leurs courriers électroniques. L'accusation a proposé de produire de multiples preuves numériques; il est toutefois apparu que, pendant qu'ils complotaient, les intéressés prenaient des précautions contre la surveillance ou le contrôle. Au cours de l'enquête qui a duré neuf mois, les autorités ont été confrontées à un certain nombre de défis techniques. Par exemple, les accusés communiquaient à l'aide de brouillons de courriers électroniques (à savoir, en ouvrant et en lisant des brouillons de messages dans les comptes de messagerie électronique) pour éviter d'être écoutés par les services de détection et de répression, utilisaient les connexions LAN sans fil non sécurisées de particuliers parfaitement innocents et cryptaient leurs communications via des services VoIP (par exemple, Skype).

Gelowicz, le meneur présumé du groupe, avait accédé à Internet en utilisant au hasard des réseaux LAN résidentiels privés non sécurisés. Il avait également employé au moins 14 comptes de messagerie électronique, changé les plaques d'immatriculation de son véhicule et utilisé un scanner de la police pour contrôler le trafic radio de celle-ci. Il avait enfin protégé les données figurant sur son ordinateur au moyen d'un cryptage que les experts en criminalistique n'ont pas réussi à déchiffrer. Gelowicz a finalement fourni la clé de cryptage, mais les enquêteurs n'ont trouvé que des traces de données broyées.

Pendant le procès, la défense a contesté la validité des arguments de l'accusation. Elle a mis en doute le fondement de l'enquête, qui, selon elle, était viciée en soi, puisqu'elle reposait sur des renseignements américains provenant notamment d'un contrôle électronique des communications des accusés, qui était illégal et avait été transmis en violation de leurs droits définis par la Constitution allemande.

Le 4 mars 2010, les quatre individus ont été déclarés coupables de tous les chefs d'accusation et condamnés. Gelowicz et Schneider ont été condamnés à 12 ans d'emprisonnement, Yilmaz à 11 ans et Selek à cinq ans.

3. Questions relatives à l'utilisation de preuves étrangères

375. Les principes juridiques et les procédures relatifs à la collecte et à la recevabilité des preuves diffèrent selon les pays. L'un des principaux défis rencontrés par les enquêteurs et les procureurs dans les enquêtes criminelles et les poursuites à caractère transfrontalier (à la fois dans le pays requis et le pays requérant) consiste à s'assurer que les preuves nécessaires sont collectées, préservées, transmises et produites conformément aux procédures juridiques et règles applicables dans les juridictions concernées, sous une forme qui soit recevable à l'endroit où le procès se déroule.

376. Le processus de "transmission" des différents éléments des preuves entre les pays est parfois complexe et chronophage, mais constitue un facteur essentiel de succès. Les

avocats de la défense invoqueront presque certainement toutes les failles juridiques des méthodes de collecte ou de production des preuves utilisées au procès.

377. L'affaire belge *Malika El Aroud* et al. souligne le type de problèmes susceptibles de se poser dans ce contexte. Cette espèce se rapportait aux activités d'un groupe d'accusés impliqués dans la création et l'administration de plusieurs sites Web en vue de diffuser de la propagande et des informations utiles aux terroristes, et utilisés comme forum de communication. Plusieurs des accusés vivaient en Belgique, mais le principal site Web sur lequel ils menaient leurs activités (minbar-sos.com) était hébergé au Canada.

***Malika El Aroud* et al.**

Introduction

En décembre 2008, après une enquête complexe, de longue haleine, de grande ampleur et coordonnée entre les autorités françaises, belges, suisses, italiennes, turques, américaines et canadiennes de renseignement, de détection, de répression et chargées des poursuites, plusieurs personnes soupçonnées d'avoir des liens avec l'organisation terroriste Al-Qaida ont été arrêtées. Un certain nombre d'accusations ont été portées à leur encontre en France et en Belgique, notamment participation comme membres d'un groupe terroriste, financement du terrorisme et fourniture d'informations et de moyens matériels à un groupe terroriste.

Pour commettre les actes à l'origine de ces accusations, les suspects ont abondamment utilisé l'Internet. L'enquête sur leurs activités a nécessité une surveillance électronique complexe, des mises sur écoute et d'autres formes de contrôle par les services de renseignement, de détection et de répression. Pour aboutir, les autorités de plusieurs pays ont dû coopérer, de manière formelle et informelle.

Cette espèce est un exemple de coopération parfaitement réussie entre les autorités nationales des États participants, en matière de poursuites pénales relatives au terrorisme présentant des aspects liés à Internet, et illustre de nombreux aspects des bonnes pratiques mentionnées dans la présente publication. Des références à ces aspects figurent tout au long des chapitres V et VI, portant respectivement sur la coopération internationale et les poursuites.

Cette espèce, qui présentait des liens avec d'autres affaires intervenues dans divers pays, concernait principalement les activités de Malika El Aroud, ressortissante belge d'origine marocaine, et de son mari, Moez Garsallaoui, ressortissant tunisien. Tous deux étaient activement impliqués dans la diffusion de propagande djihadiste radicale ainsi que dans le recrutement, l'organisation, la direction et le financement d'une opération visant à faire en sorte qu'un groupe de jeunes Belges et Français prennent part au djihad en Afghanistan et dans d'autres pays.

S'il a mené une partie de ces activités par d'autres moyens, le couple a abondamment utilisé l'Internet, notamment pour communiquer. Outre El Aroud et Moez Garsallaoui (qui, comme son complice Hicham Beyayo, a été jugé par contumace), les accusés étaient Ali el Ghanouti, Said Arissi, Jean-Christophe Trefois, Abdulaziz Bastin, Mohamed el Amin-Bastin et Hicham Bouhali Zrioul.

L'espèce belge présentait des liens étroits avec une affaire française concernant Walid Othmani Hamadi Aziri, Samira Ghamri Melouk, Hicham Berrached et Youssef el Morabit, qui ont été jugés et condamnés par le tribunal de grande instance de Paris[a], et avec une enquête et des poursuites menées en Italie contre Bassam Avachi et Raphaël Gendron.

Contexte

En août 2007, les autorités belges ont reçu de leurs homologues françaises des informations relatives aux activités menées sur le site Web Minbar SOS (lui-même hébergé au Canada) qui, d'après les soupçons, était utilisé pour diffuser de la propagande salafiste appelant au djihad contre la France. Le site était prétendument administré par El Aroud et Garsallaoui. Lorsque l'enquête s'est élargie, d'autres sites Web similaires ont été identifiés.

Les autorités soupçonnaient qu'El Aroud et Garsallaoui, agissant de concert via le site, identifiaient et recrutaient des individus en Belgique pour combattre en Afghanistan. El Aroud a publié des documents incendiaires qui appelaient les jeunes gens à s'engager pour le djihad.

Malika El Aroud et Moez Garsallaoui

Malika el Aroud et Moez Garsallaoui étaient déjà connus des services européens de lutte contre le terrorisme. En 2003, El Aroud avait été jugée et acquittée par un tribunal belge pour son implication présumée dans un réseau de soutien logistique djihadiste utilisé dans le meurtre d'un chef de la résistance anti-Taliban en septembre 2001. L'un des deux assaillants était le premier mari de M[me] El Aroud.

En 2007, El Aroud a été poursuivie en Suisse, avec Garsallaoui, son second mari, pour avoir fourni un "appui à une organisation criminelle" et pour "incitation publique à la violence et au crime" via différents sites Web qu'ils avaient tous les deux créés en Suisse. Elle a été déclarée coupable et condamnée à une peine de six mois de prison avec sursis par le tribunal pénal fédéral de Bellinzone.

Le 21 décembre 2007, El Aroud a été arrêtée en Belgique, car elle était soupçonnée d'avoir tenté d'aider un détenu, Nizar T., à s'évader. Toutefois, elle a été libérée au bout de vingt-quatre heures, en raison d'une insuffisance de preuves. En 2004, Nizar T. avait été déclaré coupable par un tribunal belge et condamné à une peine de 10 ans d'emprisonnement pour avoir préparé une attaque terroriste sur la base militaire américaine de Kleine-Brogel en 2002. Cette arrestation est survenue alors que l'enquête relative à ses activités sur Minbar SOS était déjà en cours.

Les sites Web

Les sites Web créés par El Aroud, dont Minbar SOS, étaient utilisés comme plates-formes de publication de documents de propagande (par exemple, vidéos et photographies), de diffusion de livres et publications et de communication. Chacun des membres se voyait fournir un nom d'utilisateur/pseudonyme et une adresse électronique lui permettant d'échanger des messages privés, parfois cryptés, sur des forums de discussion fermés, hébergés sur ces sites. Ceux-ci contenaient des instructions, des renseignements, de la propagande et des appels constants à un djihad de grande ampleur. Certains matériels comprenaient

des références claires à la direction d'Al-Qaida, ainsi que des messages relatifs à des attaques de troupes américaines en Iraq.

Des messages contenant des menaces explicites (par exemple, un message intitulé "Contre le terrorisme français en Afghanistan, une seule solution") ont été publiés, accompagnés d'une carte du réseau parisien de trains de banlieue (RER) sur laquelle certaines grandes stations avaient été surlignées avec des symboles de contamination radioactive ou biologique. Certains messages donnaient des instructions explicites sur la manière de transférer des fonds à des membres du djihad. Fin 2008, Minbar SOS, le site principal, comptait plus de 1 400 abonnés.

Dans le cadre d'une enquête conjointe, les autorités belges et françaises ont intercepté des communications sur des sites Web, des courriers électroniques et des appels téléphoniques, et ont surveillé et reconstitué les flux financiers. Néanmoins, alors que les services de sécurité belges surveillaient étroitement l'activité menée sur Minbar SOS pour recruter des combattants pour l'Afghanistan, ils n'ont pas pu faire grand-chose pour empêcher El Aroud d'administrer le site, en raison des solides garanties apportées par le droit belge à la liberté d'expression.

Le tribunal français chargé de la procédure judiciaire concernant cette affaire a observé ce qui suit, en faisant référence aux sites Web:

> L'activité sur ces sites Web ne peut être analysée comme une simple recherche d'information ou de renseignement, mais au contraire, caractérise une participation consciente à une entreprise/mission orientée vers le terrorisme.

En outre, lorsqu'ils ont témoigné au procès, les accusés Saïd Arissi et Hicham Beyayo ont respectivement déclaré: "Je me considère comme une victime de la propagande Internet" et "des sites Web comme Ribaat et Minbar SOS influencent des personnes comme moi qui sont parties combattre". Ces déclarations illustrent l'influence que les activités menées sur le site ont eue sur certaines personnes.

Dans une rare interview parue dans *The New York Times* du 28 mai 2008, El Aroud s'est elle-même nommée "une guerrière sainte pour Al-Qaida". Elle insiste sur le fait que […] elle n'a aucune intention de prendre les armes elle-même. En revanche, elle contraint par la menace les hommes musulmans à aller combattre et rallie les femmes à la cause. "Ce n'est pas mon rôle de déclencher des bombes, c'est ridicule. J'ai une arme, c'est d'écrire. C'est mon jihad. Vous pouvez faire beaucoup de choses avec des mots. Écrire est aussi une bombe."[b]

Voyage de recrues vers les zones tribales sous administration fédérale du Pakistan

Outre les activités menées sur les sites Web, Garsallaoui s'est également rendu dans les quartiers d'immigrants de Bruxelles pour recruter directement. Hicham Beyayo, un ressortissant belge d'origine marocaine âgé de 23 ans qui a été arrêté et était un administrateur du site Minbar SOS avant de se rendre au Pakistan, a reconnu avoir été recruté de cette manière.

Garsallaoui ne limitait pas ses activités à la Belgique; il a également recruté deux abonnés français de Minbar SOS. L'un de ces individus, qui s'est rendu dans les zones tribales sous administration fédérale du Pakistan et a ensuite été arrêté, a décrit les appels au "djihad" sur Minbar SOS comme "incessants" et a déclaré que la propagande vidéo vue sur le site lui avait donné envie de se porter volontaire.

En décembre 2007, Garsallaoui et six recrues, dont Hicham Beyayo, Ali el Ghanouti et Y. Harrizi, se sont rendus dans les zones tribales sous administration fédérale du Pakistan via la Turquie et la République islamique d'Iran. Le groupe y est resté jusqu'au second semestre 2008. Pendant ce séjour, Garsallaoui était en contact régulier avec El Aroud par courrier électronique et parfois via Skype. En sus d'envoyer des photographies et d'autres matériels de propagande, il publiait des déclarations et suivait régulièrement les forums sur Minbar SOS.

Le 26 septembre 2008, Garsallaoui a publié une déclaration sur Minbar SOS qui appelait à mener des attaques en Europe: "La solution, mes frères et mes sœurs, ce n'est pas des fatwas mais des boooooooms", disait l'article.

Les arrestations

Au second semestre 2008, certains des suspects sont retournés en Belgique sur une période de quelques mois. Les services de sécurité belges ont été placés en alerte après le retour d'El-Ghanouti et Harrizi des zones tribales sous administration fédérale, et le 4 décembre 2008, Beyayo lui-même est revenu en Belgique.

Différentes explications sont avancées concernant les raisons du retour des recrues en Belgique à ce moment-là. Certains suspects ont laissé entendre qu'ils n'étaient pas satisfaits du traitement reçu et des conditions dans les zones tribales sous administration fédérale, notamment des restrictions quant à leur capacité à participer au djihad, et ont nié l'existence de toute "cellule dormante" visant à mener des attaques en Belgique. Toutefois, les autorités belges ont considéré que les indications issues des communications interceptées fournissaient de fortes raisons de soupçonner que le groupe était en phase finale de planification d'un attentat-suicide (faisant éventuellement appel à Hicham Beyayo) en Belgique, ce qui nécessitait une action immédiate de leur part.

Le 11 décembre, une semaine après le retour de Beyayo, les autorités belges ont investi 16 lieux en Belgique et arrêté neuf suspects, dont El Aroud, Garsallaoui et Beyayo. Des opérations similaires ont été menées en France et en Italie.

Procédures pénales

Belgique

Au procès, les avocats de la défense ont contesté différents aspects de l'accusation, notamment les fondements de la procédure et la recevabilité de certaines preuves, dont les données relatives à Internet obtenues de manière informelle auprès du FBI et se rapportant à des FAI basés aux États-Unis. Nous aborderons ultérieurement et de manière plus détaillée les questions relatives à ce type de preuves.

Beyayo avait été interrogé par les autorités marocaines le 20 mai 2008. Ses avocats ont invoqué l'existence d'une violation de son droit à un procès équitable, sur la base de soupçons d'actes de torture commis par les autorités marocaines sur les détenus suspectés de terrorisme. Le tribunal a rejeté ces arguments.

Activités de Bryan Neal Vinas (États-Unis)

En janvier 2009, Bryan Neal Vinas, un ressortissant des États-Unis, s'est rendu en Afghanistan, et a tenté de tuer des soldats américains au cours d'une attaque à la roquette

lancée par Al-Qaida contre une base militaire. Il a été arrêté et renvoyé aux États-Unis, où il a été accusé d'entente criminelle en vue de tuer des ressortissants américains, de fourniture d'un soutien matériel à Al-Qaida et de participation à un entraînement militaire de ce groupe. Vinas a plaidé coupable et a été condamné à purger une peine d'emprisonnement.

Les autorités belges qui poursuivaient Beyayo, un complice d'El Aroud, ont produit des preuves issues du procès de Vinas visant à établir l'étendue de leurs activités et de leur implication dans le réseau Al-Qaida. Dans ses déclarations, Vinas reconnaissait avoir rencontré certaines des recrues belges. La défense a contesté la recevabilité de cette preuve pour un certain nombre de motifs, mais le tribunal a rejeté ces arguments.

Issue du procès

Après le procès, le tribunal de première instance de Bruxelles a statué le 10 mai 2010 sur le cas de neuf personnes qui avaient été poursuivies pour différents chefs d'accusation, divisés en trois groupes: A, B et C.

Les chefs d'accusation des groupes A et C concernaient respectivement la participation comme chef d'un groupe terroriste et la participation aux activités d'un groupe terroriste, en fournissant notamment des informations ou des moyens matériels ou par le biais de toute forme de financement des activités d'un groupe terroriste, en sachant que cette participation contribuerait à la commission par ce groupe d'un crime ou d'une infraction.

Les chefs d'accusation du groupe B concernaient notamment la commission d'infractions ou l'assistance dans l'exécution d'infractions au moyen de dons, de promesses, de menaces, d'abus d'autorité ou de pouvoir, de complots ou de stratagèmes dans l'intention de commettre des infractions contre des personnes ou des biens pour leur causer un préjudice grave, ainsi que d'infractions qui, de par leur nature ou leur contexte, pouvaient causer un préjudice grave à un pays ou à une organisation internationale et qui étaient commises intentionnellement dans le but d'intimider gravement une population ou de contraindre les autorités publiques ou une organisation internationale à agir, ou à déstabiliser gravement ou détruire les structures politiques, constitutionnelles, économiques ou sociales fondamentales d'un pays ou d'une organisation internationale.

Les condamnations suivantes ont été prononcées au titre des chefs d'accusation du groupe A:

- Malika El Aroud: huit ans d'emprisonnement et une amende de 5 000 euros;
- Moez Garsallaoui: huit ans d'emprisonnement et une amende de 5 000 euros (par contumace);
- Hicham Beyayo: cinq ans d'emprisonnement et une amende de 1 000 euros (par contumace).

Les condamnations suivantes ont été prononcées au titre des chefs d'accusation du groupe B:

- Ali el Ghanouti: acquitté;
- Said Arissi: acquitté.

Les condamnations suivantes ont été prononcées au titre des chefs d'accusation du groupe C:

- Ali el Ghanouti: trois ans d'emprisonnement et une amende de 500 euros;
- Said Arissi: 40 mois d'emprisonnement et une amende de 500 euros;
- Hicham Bouhali Zrioul: cinq ans d'emprisonnement et une amende de 2 000 euros (par contumace);
- Abdulaziz Bastin: 40 mois d'emprisonnement et une amende de 500 euros;
- Mohamed el Amin-Bastin: 40 mois d'emprisonnement et une amende de 500 euros;
- Jean-Christophe Trefois: acquitté.

France

En France, cinq suspects (tous Français originaires d'Afrique du Nord) ont été jugés devant le tribunal de grande instance de Paris. Walid Othmani, Hamadi Aziri, Samira Ghamri Melouk, Hicham Berrached et Youssef el Morabit ont été accusés de diverses infractions: financement du terrorisme, entente en vue de la commission d'un acte terroriste et participation à un groupe constitué dans le but de préparer un acte terroriste défini à l'article 421-1 du Code pénal français.

Italie

Bassam Ayachi et Raphaël Gendron (tous deux ressortissants français) ont été accusés par les autorités italiennes d'association de malfaiteurs dans un but terroriste en vertu du paragraphe 1 de l'article 207 *bis* du Code pénal italien, qui prévoit une peine de sept à 15 ans d'emprisonnement pour toute personne jugée coupable de constitution, promotion, organisation, gestion ou financement de groupes qui ont l'intention de mener des activités violentes dans un but terroriste ou en vue de détruire la structure démocratique de l'État, et une peine de cinq à 10 ans d'emprisonnement pour les individus qui s'associent à ces groupes.

Au cours de l'affaire, des liens ont été établis entre les deux défendeurs et certains des accusés de la procédure belge, ainsi que des éléments de preuve communs, notamment la présence sur un DVD d'une lettre de suicide écrite par l'un des suspects belges.

Le 3 juin 2011, Ayachi et Gendron ont été condamnés à huit ans d'emprisonnement.

Source: Eurojust, *Terrorism Convictions Monitor*, n° 8, septembre 2010.

[a] Jugement du 18 février 2011 (n° d'affaire 1015239014).

[b] Voir "Al Qaeda Warrior uses Internet to Rally Women", *The New York Times* (28 mai 2008). Disponible à l'adresse: www.nytimes.com/2008/05/28/world/europe/28terror.html?_r=1&pagewanted=all.

378. Dans l'affaire *El Aroud*, l'accusation a produit des données relatives à des messages publiés sur Internet et à des discussions intervenues sur les forums. Dans le cas des courriers électroniques (qui étaient envoyés à partir de comptes Yahoo et Microsoft), les données étaient détenues sur des serveurs situés aux États-Unis. Après une demande informelle d'assistance, les autorités belges ont reçu du FBI (dans un délai de deux semaines) un CD contenant les données relatives aux comptes de courrier électronique

spécifiés et à d'autres comptes connexes. Le FBI a indiqué que ces éléments avaient été volontairement fournis par Yahoo et Microsoft, comme l'autorisent les dispositions de la loi américaine intitulée *Patriot Act*.

379. La défense a contesté la recevabilité de ces éléments, et soutenu que les procédures utilisées pour les collecter, les transmettre et les produire étaient illégales, puisque ces preuves avaient été recueillies en l'absence de mandat de perquisition. La défense a également invoqué le fait que les procédures informelles utilisées ne respectaient pas les méthodes usuelles d'échange international d'informations judiciaires, et enfreignaient ainsi le paragraphe 1 de l'article 7 de la loi belge du 9 décembre 2004 sur l'entraide judiciaire internationale en matière pénale.

380. Le tribunal a rejeté cet argument, considérant que: *a)* l'échange d'informations n'était pas intervenu dans le cadre de l'entraide judiciaire; *b)* au moment déterminant, aucun juge d'instruction n'avait été désigné au titre de l'affaire, qui était gérée de manière informelle entre les différents services de police; et *c)* la procédure utilisée était justifiée par l'urgence (à savoir, la découverte d'une lettre de suicide publiée sur le site Web Minbar SOS par l'un des suspects, laissant penser qu'une attaque sur le sol français orchestrée par Malika El Aroud et ses complices était imminente). Le tribunal a jugé que pour cette raison, le Magistrat fédéral était fondé à conclure que cette coopération policière d'urgence reposait sur les motifs du paragraphe *b)* de l'article 15 de la Convention internationale pour la répression des attentats terroristes à l'explosif (1997)[166], qui dispose que les États parties collaborent "… en échangeant des renseignements exacts et vérifiés en conformité avec les dispositions de leur législation interne et en coordonnant les mesures administratives et autres prises, le cas échéant, afin de prévenir la perpétration des infractions visées à l'article 2"[167].

381. Enfin, le tribunal a jugé que, puisque la transmission par les autorités américaines des informations à la police belge avait un fondement juridique valable, ces informations pouvaient de facto être utilisées par les autorités judiciaires belges. Le tribunal a ajouté que l'analyse relative aux adresses de courrier électronique basées aux États-Unis (ou à la plupart d'entre elles) avait été intégrée au dossier judiciaire après une commission rogatoire exécutée en France[168].

382. Cette instance met en relief l'attention qu'il convient de porter, pendant la phase d'enquête des affaires impliquant l'utilisation de preuves étrangères, aux méthodes utilisées pour collecter et transmettre ces preuves. Elle confirme l'importance, soulignée à plusieurs reprises lors de la réunion du groupe d'experts, d'intégrer dès que possible les procureurs à l'enquête, pour identifier et arbitrer les éventuelles questions de preuves avant le procès.

383. Dans l'affaire *Namouh* (Canada), l'accusation a dû produire au procès des preuves recueillies par un policier autrichien, ce qui a posé problème. Selon le droit autrichien,

[166] Nations Unies, *Recueil des Traités*, vol. 2178, n° 38349.

[167] Eurojust, *Terrorism Conviction Monitor*, n° 8, septembre 2010.

[168] Ibid.

les éléments fournis par le policier pouvaient être admis à titre de preuves sous forme de déposition écrite. En revanche, ce n'était pas le cas en vertu du droit canadien qui, de manière générale, exclut les preuves par commune renommée et exige que les témoins comparaissent au tribunal et témoignent verbalement. Pour faciliter la production des preuves du policier, les procureurs canadiens ont dû collaborer étroitement avec la police et les procureurs autrichiens, et leur expliquer les règles applicables en droit canadien, ainsi qu'avec l'avocat de la défense pour faciliter la conclusion d'un accord acceptant la production sous forme écrite des preuves du policier.

4. Le recours aux témoignages d'experts

384. Dans les affaires de terrorisme, le procureur est souvent tenu de produire des témoignages d'experts pour prouver un ou plusieurs aspects de son argumentation. Toutefois, ce type de preuves pose de très nombreuses questions. À partir des poursuites déjà exercées en matière d'activité sur Internet relative au terrorisme, il est possible de définir à grands traits certains domaines dans lesquels les enquêteurs ou les procureurs pourraient devoir envisager ce point.

385. Le domaine de la technologie et de la communication continue d'évoluer rapidement, et présente une complexité et une spécialisation croissantes. Il est probable que les procureurs aient besoin de plusieurs témoins experts pour expliquer certains aspects techniques, différents mais liés, des systèmes informatiques ou de communication ou d'activités connexes au cours de la même procédure, en particulier lorsqu'il est prouvé qu'un suspect a utilisé un ordinateur, un appareil ou un service Internet donné[169].

386. Outre les éléments de criminalistique informatique en cas d'allégation de participation ou de soutien matériel à des groupes terroristes, ou d'incitation, de recrutement ou d'entraînement, des témoignages d'experts pourraient s'avérer nécessaires concernant l'idéologie, les objectifs, les activités et les structures organisationnelles de groupes terroristes ou d'individus donnés.

387. Lorsque l'intervention d'un témoin expert est requise, trois phases ou étapes se présentent généralement: *a)* détermination claire des questions qui nécessitent un avis d'expert (et de leur objet); *b)* identification d'un expert qualifié; et *c)* vérification du fait que cet expert utilise des moyens recevables[170].

a) Détermination claire des questions

388. Les procureurs devraient, en étroite coordination avec les enquêteurs, déterminer dès que possible les questions qui, selon eux, nécessiteront des témoignages d'experts et charger ces experts d'entreprendre l'analyse requise, en leur fournissant des conseils précis sur les éléments de preuve déterminants.

[169]Walden, *Computer Crimes and Digital Investigations*, p. 383.

[170]National Institute of Justice, *Digital Evidence in the Courtroom*, chap. 3, sect. III.E.

b) Identification d'un expert qualifié

389. Lorsqu'ils choisissent les experts qui témoigneront sur certains aspects spécialisés des preuves, les procureurs doivent se demander s'il convient de faire appel à des experts gouvernementaux ou non. Le recours aux experts gouvernementaux est autorisé et offre certains avantages, mais n'est pas nécessairement souhaitable si les processus de communication préalables au procès ou de contre-interrogatoire par la défense risquent de permettre l'identification de sources de renseignement sensibles et des méthodes d'obtention des informations étayant leurs avis. Afin d'éviter ce piège, les procureurs préféreront peut-être faire appel à des universitaires ou à des experts non gouvernementaux, susceptibles de s'appuyer sur des informations accessibles au public et pouvant être aisément divulguées sans risque de compromettre les sources de renseignement ou les méthodes utilisées[171].

390. L'affaire *Namouh*, dans laquelle deux témoins ont été appelés à expliquer les objectifs et les modes opératoires du Global Islamic Media Front (GIMF), est un bon exemple d'instance dans laquelle l'accusation a fait intervenir des experts non gouvernementaux. Le contexte de ces témoignages est expliqué au paragraphe 394 ci-dessous.

391. L'identification d'un expert compétent, en particulier dans des domaines très spécialisés, peut constituer un défi important dans les juridictions moins développées. Les procureurs, en collaboration avec les enquêteurs, devraient adopter une démarche proactive et prudente, étudier toutes les voies pour engager (dans la mesure du possible) un témoin qualifié au niveau national mais, en cas de nécessité, prendre des mesures pour assurer la présence d'un témoin compétent à l'échelle internationale.

c) Vérification que l'expert utilise des moyens recevables

392. Il est primordial que les témoins de l'accusation respectent et appliquent les bonnes pratiques reconnues lorsqu'ils effectuent des examens ou des analyses dans le domaine sur lequel ils sont appelés à témoigner. C'est particulièrement le cas des analyses criminalistiques spécialisées qu'ils réalisent aux fins d'établir les avis qui seront produits à titre de preuves par l'accusation. Dès que possible, les enquêteurs et les procureurs devraient déterminer s'ils ont besoin de témoignages d'experts sur certains aspects spécialisés des arguments de l'accusation et, dans l'affirmative, consulter et engager les experts compétents au plus tôt pour faire en sorte que les preuves utilisées lors des témoignages d'experts ultérieurs soient préservées de façon recevable.

393. Dans certaines instances, en particulier celles qui concernent les technologies informatiques, les preuves sont parfois complexes sur le plan technique. Les procureurs et les témoins experts doivent donc envisager des façons novatrices de les présenter aux juges, aux jurys ou aux autres personnes chargées d'établir les faits, d'une manière qui soit claire, facilement compréhensible et incontestable. Par exemple, une description visuelle de la conception d'un système ou d'un trafic de données, à la place d'une simple déposition verbale, pourrait aider les personnes chargées d'établir les faits à

[171] Office des Nations Unies contre la drogue et le crime, *Recueil de cas sur les affaires de terrorisme*, par. 194.

mieux comprendre les aspects techniques des systèmes informatiques ou de communication. Évidemment, il importe également que le procureur ait une bonne connaissance pratique du domaine concerné de façon à présenter les termes et concepts pertinents au juge, au jury ou au tribunal, et à exposer ses arguments avec efficacité.

394. Dans l'affaire canadienne *Namouh*, un témoignage d'expert sur les questions de preuves numériques (fourni par un expert de la Gendarmerie royale du Canada en matière de criminalistique numérique) s'est avéré très utile. Ce témoignage portait principalement sur la prétendue utilisation par l'accusé d'un ordinateur (saisi à son domicile) et de l'Internet lorsqu'il participait à des forums de discussion en ligne, téléchargeait du matériel sur les sites Web et communiquait avec un complice situé en Autriche. Ce témoignage détaillé s'est avéré nécessaire pour convaincre le tribunal que c'était bien l'accusé qui avait utilisé l'ordinateur à partir duquel les messages compromettants avaient été envoyés, ainsi que pour décrire l'idéologie et les méthodes du GIMF, le groupe terroriste mondial auquel l'accusé participait activement.

395. La défense de Namouh a en partie consisté à décrédibiliser cet aspect de l'accusation. L'avocat a soutenu que, compte tenu du caractère fondamentalement faillible de l'Internet, le témoin expert ne pouvait l'utiliser de manière fiable comme source d'information pour émettre un avis sur l'activité du GIMF et d'autres groupes terroristes. En particulier, la défense a soutenu que le témoin expert ne pouvait établir avec certitude si les messages publiés sur les forums de discussion, et autres formes de communications électroniques, avaient été rédigés par les terroristes présumés ou étaient imputables à des fonctionnaires agissant comme agents provocateurs. Dans cette affaire, un expert de l'accusation a effectué un témoignage qui a suffi à convaincre le tribunal de la fiabilité des méthodes et des matériels Internet invoqués, et à attribuer la valeur correspondante à ce témoignage.

396. Il convient de noter que ces communications électroniques se sont déroulées en arabe et ont été traduites en français, l'accusation ayant déposé au tribunal la traduction française accompagnée de la transcription originale en arabe. Cet aspect souligne également la prudence requise lorsque les autorités cherchent à produire des traductions de conversations ou de documents dans d'autres langues, et notamment des transcriptions de communications interceptées.

397. Outre la question des preuves numériques déterminantes, l'accusation a appelé des experts à témoigner sur les activités et les objectifs du GIMF, sur ses méthodes de coordination et de recrutement de nouveaux membres, de propagation d'idéologie radicale et d'entraînement militaire, et sur ses modes de communication via l'Internet. L'accusation a produit les rapports écrits de deux experts sur ces points, l'un des experts étant cité à la barre pour confirmer les conclusions du rapport. Lors de la réunion du groupe d'experts, le spécialiste canadien a souligné qu'il était important que les procureurs puissent faire appel à plusieurs témoins experts sur les questions essentielles, en guise à la fois de confirmation et de plan de secours.

398. La valeur de ce type de témoignage concernant les chefs d'accusation relatifs au soutien d'une organisation terroriste est illustrée dans la déclaration suivante du juge

du procès, se rapportant aux "actions réelles encouragées par le GIMF", qui faisaient l'objet du témoignage de l'expert de l'accusation:

> "L'avocat de la défense a invité le Tribunal à considérer les différents messages véhiculés par le GIMF comme devant être pris au figuré. Le Tribunal n'a aucun doute à ce sujet. Le contexte de ces messages fait clairement référence à des *actions réelles encouragées par le GIMF*. La mort et la destruction sont partout. *Le Jihad dont le GIMF fait la promotion est de nature violente* [non souligné dans le texte]. Cette promotion constitue nettement un encouragement et parfois une menace d'activités terroristes. De ce fait, cette activité s'inscrit clairement dans la définition d'activité terroriste au sens de l'article 83.01 C.cr[172]."

H. Autres questions

1. La nécessité d'un plan de secours et de continuité

399. Compte tenu de la complexité des poursuites relatives au terrorisme, et particulièrement de celles qui impliquent une coopération internationale ou des éléments extrêmement techniques, il est très souhaitable qu'une équipe de procureurs soit chargée de l'affaire, et que chaque procureur en soit informé et, si nécessaire, soit capable de continuer si un membre de l'équipe se trouve subitement empêché. Cette précaution garantira une procédure de qualité et limitera le risque d'échec. Les affaires *Namouh* (Canada) et *Gelowicz, Yilmaz, Schneider et Selek* (Allemagne) constituent deux exemples de poursuites complexes et de grande ampleur qui nécessitent une équipe, et l'implication d'au moins un procureur tout au long de l'affaire. Dans l'affaire jugée en Allemagne, le procès devait initialement durer deux ans. Il a été beaucoup plus court, puisque les accusés ont plaidé coupables, mais il a quand même duré trois mois.

2. La nécessité d'un renforcement de la formation et des capacités

400. Afin de garantir une approche intégrée fondée sur l'état de droit et de préserver l'intégrité des réponses de justice pénale au terrorisme, les pays doivent disposer de processus solides et constants visant à renforcer la capacité des procureurs à appliquer la législation nationale de lutte contre le terrorisme et les obligations de coopération internationale connexes. Du fait de la nature de la législation et des enquêtes antiterroristes et de la rapidité, de la complexité et du caractère transfrontalier de l'activité menée sur Internet, les équipes d'enquête, dont les procureurs, doivent prendre dans des délais très courts de nombreuses décisions concernant différents aspects de l'espèce. Il est important qu'ils soient suffisamment formés et compétents pour s'acquitter de leurs principales fonctions dans les affaires de terrorisme.

401. Dans les pays où le risque d'activité terroriste est élevé et où les capacités institutionnelles au sein des services chargés des poursuites et des autres organismes de

[172] *Justice* c. *Leblond*, 1er octobre 2009.

justice pénale sont limitées, il convient de privilégier le développement de capacités spécialisées au sein de ces services, tant en termes de poursuites que concernant les mécanismes connexes de coopération internationale.

VII. Coopération du secteur privé

A. Rôle des acteurs du secteur privé

402. Si la responsabilité de la lutte contre l'utilisation d'Internet à des fins terroristes incombe *in fine* aux États Membres, la coopération des principaux acteurs du secteur privé est essentielle en termes d'efficacité. Les infrastructures de réseau des services Internet appartiennent souvent, en totalité ou en partie, à des entités privées. De même, des entreprises privées possèdent généralement les plates-formes de média social, qui facilitent la diffusion de contenus générés par les utilisateurs à un vaste public, tout comme les moteurs de recherche courants, qui filtrent les contenus en fonction de critères fournis par les utilisateurs.

403. L'efficacité de l'utilisation d'Internet pour diffuser des contenus relatifs aux actes de terrorisme dépend à la fois de l'émetteur de la communication et du public ayant accès aux technologies Internet. Dès lors, pour limiter les effets de ces communications, le mieux est de contrôler l'accès à l'infrastructure de réseau, de censurer les contenus ou de mettre en œuvre une combinaison des deux méthodes[173]. Le niveau de réglementation d'Internet varie beaucoup selon les États Membres, mais en l'absence d'autorité mondiale et centralisée responsable de cette réglementation, les acteurs du secteur privé tels que les prestataires de services, les sites Web hébergeant des contenus générés par les utilisateurs et les moteurs de recherche Internet continuent de jouer un rôle important en matière de contrôle de l'existence de contenus relatifs au terrorisme diffusés sur l'Internet. L'autorégulation des acteurs du secteur privé peut aussi contribuer à contrer les activités de communication, d'incitation, de radicalisation et d'entraînement menées au moyen d'Internet. Les services de contrôle privés jouent également un rôle dans l'identification en temps utile de l'activité susceptible de promouvoir des actes de terrorisme sur Internet.

1. Fournisseurs d'accès à l'Internet

404. Dans de nombreux États Membres, l'accès à l'Internet est contrôlé par des acteurs non étatiques, tels que les prestataires de télécommunications du secteur privé, qui possèdent ou gèrent l'infrastructure de réseau. Ces prestataires de services sont parfois bien placés pour aider à recueillir les données relatives aux communications ou pour divulguer ces données, selon le cas[174], dans le cadre d'une enquête menée par les services de détection, de répression, de justice pénale et de renseignement à propos

[173] Conway, "Terrorism and Internet governance: core issues", p. 26.

[174] Sous réserve des garanties et des réglementations relatives à la vie privée applicables.

d'une éventuelle activité terroriste. Les données relatives aux communications détenues par les FAI peuvent constituer des preuves déterminantes contre les auteurs d'infractions, ou permettre d'établir des liens vers d'autres preuves ou collaborateurs utiles à l'enquête.

405. À titre d'exemple, les FAI demandent parfois aux utilisateurs de s'identifier avant d'accéder à des contenus et services Internet. La collecte et la préservation des informations d'identification associées aux données Internet, et la divulgation de ces informations, sous réserve des garanties appropriées, pourraient grandement faciliter les enquêtes et les poursuites. En particulier, le fait de demander aux clients de s'enregistrer pour utiliser un réseau Wi-Fi ou pour se connecter dans un cybercafé pourrait fournir une source de données importante pour les enquêtes criminelles. Certains pays, comme l'Égypte, ont mis en œuvre une législation contraignant les FAI à identifier les utilisateurs avant de les autoriser à accéder à l'Internet, mais les FAI peuvent prendre spontanément ce type de mesures.

a) Coopération avec les autorités gouvernementales

406. Compte tenu du caractère délicat des affaires de terrorisme, les acteurs du secteur privé peuvent être incités à coopérer avec les autorités de détection et de répression par l'impact positif de cette coopération sur leur réputation, lorsque toutes les précautions sont prises pour assurer le respect des droits de l'homme fondamentaux, tels que la liberté d'expression, le respect de la vie privée, du domicile et de la correspondance, et le droit à la protection des données. Le fait d'éviter les conséquences préjudiciables découlant d'un défaut de coopération peut également constituer un facteur de motivation. Par exemple, il est possible que les FAI coopèrent parce qu'ils s'inquiètent des connotations négatives que pourrait avoir le fait d'être associés au soutien d'une activité terroriste. Les craintes liées à la responsabilité relative à l'hébergement de certains types de contenu Internet peuvent également influencer le niveau de coopération des entités du secteur privé.

407. L'expert égyptien a indiqué que l'on observait dans son pays une réponse concertée des acteurs pertinents du secteur privé aux demandes raisonnables des autorités gouvernementales d'interruption de l'accès aux contenus Internet relatifs au terrorisme. En outre, les FAI égyptiens seraient notamment incités à collaborer par la reconnaissance de la concordance de leurs intérêts avec ceux des autorités gouvernementales qui cherchent à prévenir et à poursuivre les actes de terrorisme, puisqu'ils risquent d'être eux-mêmes victimes d'une attaque terroriste.

408. Si les acteurs du secteur privé affichent parfois une volonté de supprimer volontairement des contenus illégaux, la législation nationale peut également les contraindre à le faire. Au Royaume-Uni, par exemple, l'article 3 de la loi de 2006 contre le terrorisme dispose que les autorités de détection et de répression peuvent délivrer des avis de "retrait" aux FAI (voir par. 172 et suivants ci-dessus). Ces avis sont utilisés pour informer les hébergeurs de contenus que certains matériels sont considérés par les agents des services de détection et de répression comme illégaux et liés au terrorisme. Les FAI auxquels un avis de retrait a été délivré doivent supprimer les contenus

concernés dans un délai de deux jours ouvrés. D'autres pays ont également recours à des avis de retrait pour certaines infractions, mais ils concernent plus fréquemment les cas de violation de droit d'auteur ou de contenus sexuellement explicites.

409. L'État d'Israël a souligné ses succès en matière de coopération des représentants étrangers du secteur privé sur son territoire. Par exemple, dans plusieurs enquêtes concernant des infractions informatiques, des demandes ont été présentées aux représentants de Microsoft et de Google en Israël. Dès réception d'une ordonnance judiciaire dûment signifiée, ces représentants ont fourni les informations demandées par les autorités chargées de l'enquête. Dans certains cas où il était nécessaire d'adresser des demandes à des représentants du secteur privé implantés aux États-Unis, les autorités ont généralement eu recours aux processus formels de demande d'entraide judiciaire par l'intermédiaire des autorités gouvernementales, tout en adressant occasionnellement des demandes directes de données d'identification aux entreprises étrangères du secteur privé, et ce avec succès.

b) Conservation des données

410. Plusieurs États Membres ont récemment adopté ou proposé l'adoption d'une législation exigeant des prestataires de services de télécommunications qu'ils enregistrent et archivent systématiquement les données relatives aux communications de leurs utilisateurs. En 2006, incitée en partie par les attaques terroristes de Madrid en 2004 et de Londres en 2005[175], l'Union européenne a adopté une directive sur la conservation obligatoire des données de communications relatives au trafic (directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE)[176]. La directive 2006/24/CE reconnaît les difficultés posées par les disparités juridiques et techniques existant entre les dispositions nationales pour ce qui est des types de données à conserver, ainsi que des conditions et des délais de conservation[177]. Elle tente donc d'harmoniser les obligations minimales de conservation des données incombant aux prestataires de services de communications électroniques qui opèrent dans les États membres de l'Union européenne aux fins de prévention, de recherche, de détection et de poursuite des infractions pénales.

411. La directive 2006/24/CE impose aux États membres d'adopter une législation[178] contraignant les fournisseurs de télécommunications à conserver certaines données

[175] Commission européenne, "Rapport de la Commission au Conseil et au Parlement européen: rapport d'évaluation concernant la directive sur la conservation des données (directive 2006/24/CE)", document COM(2011) 225 (Bruxelles, 18 avril 2011), sect. 3.2.

[176] *Journal officiel de l'Union européenne*, L 105, 13 avril 2006.

[177] Ibid., préambule, par. 6.

[178] En avril 2011, la législation de transposition était entrée en vigueur dans 22 États membres de l'Union européenne.

relatives au trafic se rapportant aux communications électroniques[179] pendant une durée comprise entre six mois et deux ans. Ces données relatives au trafic comprennent les informations nécessaires à l'identification de l'expéditeur et du destinataire des courriers électroniques et des communications de téléphonie sur Internet, ainsi que les informations concernant la date, l'heure et la durée de ces communications. Toutefois, l'obligation ne s'étend pas au contenu des communications électroniques[180]. Ces données doivent être communiquées, dans le contexte de la recherche, la détection et la poursuite des infractions graves, aux autorités nationales de détection et de répression et, par le biais des autorités nationales[181], à leurs homologues des autres États membres de l'Union européenne, conformément aux exigences de leurs droits internes respectifs.

412. Par exemple, une fois la directive transposée dans le droit interne, et sous réserve des obligations procédurales applicables, les autorités nationales de détection et de répression pourraient demander aux prestataires de services un accès à leurs données pour identifier les abonnés utilisant une adresse IP spécifique et les individus avec lesquels cette personne a été en contact pendant une période donnée[182]. En outre, les enquêtes sur les actes terroristes pourraient s'appuyer sur les données conservées par les prestataires de services, qui reflètent le temps consacré à la préparation de ces infractions, pour définir les types de comportements délictueux et les liens entre les complices d'une infraction, et pour établir l'intention délictueuse[183]. Des États membres de l'Union européenne[184] ont indiqué que la conservation des données était le seul moyen d'enquêter sur certaines infractions impliquant des communications sur Internet comme les messages publiés sur les forums de discussion, qui ne peuvent être retrouvés que par le biais des données relatives au trafic[185]. Plusieurs États membres de l'Union européenne[186] ont également signalé utiliser les données conservées par les prestataires de services pour innocenter des personnes soupçonnées d'infraction sans avoir besoin d'avoir recours à des méthodes de surveillance plus intrusives comme l'interception ou la perquisition de domicile. Les données de localisation sont également importantes pour exclure certains suspects de scènes de crime et vérifier les alibis. Les données conservées conformément à la loi de transposition de la directive permettent également l'établissement d'un faisceau de preuves aboutissant à un acte de terrorisme, notamment en facilitant l'identification ou la corroboration d'autres formes de preuves concernant les activités et les liens entre les suspects[187].

[179] Cela comprend les données générées ou traitées par les prestataires de services dans le cadre de leurs activités, par exemple aux fins de transmission de communication, de facturation, d'interconnexion, de paiement, de commercialisation et d'autres services à valeur ajoutée.

[180] *Journal officiel de l'Union européenne*, L 105, 13 avril 2006, art. 5.

[181] Ibid., art. 4.

[182] Commission européenne, "Rapport de la Commission au Conseil et au Parlement européen: rapport d'évaluation concernant la directive sur la conservation des données (directive 2006/24/CE)", sect. 5.2.

[183] Ibid., sect. 3.1 et 5.2.

[184] Belgique, Irlande et Royaume-Uni.

[185] Commission européenne, "Rapport de la Commission au Conseil et au Parlement européen: rapport d'évaluation concernant la directive sur la conservation des données (directive 2006/24/CE)", sect. 5.4.

[186] Allemagne, Pologne, Royaume-Uni et Slovénie.

[187] Commission européenne, "Rapport de la Commission au Conseil et au Parlement européen: rapport d'évaluation concernant la directive sur la conservation des données (directive 2006/24/CE)", sect. 5.4.

2. *Sites Web et autres plates-formes hébergeant des contenus générés par les utilisateurs*

413. Les contenus relatifs au terrorisme hébergés sur les sites Web très prisés qui comportent des éléments générés par les utilisateurs risquent d'atteindre un public beaucoup plus large que les contenus affichés sur les sites Web spécialisés traditionnels, les tableaux d'affichage électroniques et les forums, qui s'adressent généralement à un groupe d'individus auto-sélectionnés. D'après le site de partage YouTube, 48 heures de vidéos générées par les utilisateurs sont téléchargées sur son site chaque minute, ce qui équivaut à près de huit ans de contenus téléchargés chaque jour[188]. L'offre mensuelle de contenus aux huit millions d'utilisateurs uniques estimés de YouTube restreint significativement les obstacles à l'accès aux contenus relatifs au terroriste. Depuis quelques années, la popularité croissante des contenus générés par les utilisateurs accroît les difficultés logistiques de contrôle des contenus relatifs au terrorisme. En outre, les utilisateurs de sites Web hébergeant de la vidéo peuvent tomber par inadvertance sur des contenus relatifs au terrorisme en recherchant ou consultant des matériels plus modérés, compte tenu des mécanismes intégrés qui suggèrent automatiquement des contenus connexes.

Affaire *Filiz G.*

Dans cette affaire intervenue en Allemagne, Filiz G. a été déclarée coupable de recrutement de membres ou de sympathisants d'organisations terroristes étrangères (Al-Qaida, Union du Jihad islamique et Deutsche Taliban Mujahideen) et de fourniture d'un soutien à ces organisations.

En mars 2009, Filiz G. a rejoint un forum Internet et a commencé à publier des traductions en allemand de communiqués d'organisations terroristes dénonçant des crimes qui auraient été commis par les forces armées internationales en Iraq et en Afghanistan, et appelant les utilisateurs à rejoindre ou à soutenir le djihad. En tant qu'épouse d'un terroriste allemand incarcéré, Filiz G. s'est rapidement vu attribuer des droits d'administrateur sur le forum Internet. Au moment de son arrestation en février 2010, elle avait publié plus de 1 000 contributions et commentaires, tant dans la partie accessible au public du forum que dans une section fermée, visible des seuls membres enregistrés. Elle avait ouvert neuf canaux vidéo sur le portail YouTube et posté 101 vidéos, dont des publications de groupes terroristes tels qu'Al-Qaida et l'Union du Jihad islamique et des vidéos qu'elle avait produites elle-même. L'accusée coopérait très étroitement avec M., l'"interlocuteur média" de l'Union du Jihad islamique. M. l'avait contactée par Internet et lui avait d'abord demandé de traduire du turc à l'allemand des textes à caractère religieux. Par la suite, il lui a donné des liens vers des vidéos, que l'accusée a publiées sur YouTube, et lui a demandé de l'aider à recueillir des dons.

Dans un cas, Filiz G. a traduit en allemand des matériels publiés sur une page Web en langue turque et les a publiés sur une page Web allemande. Ces matériels appelaient les donateurs à soutenir les "familles des moudjahidin en Afghanistan qui résistent aux attaques

[188] Statistiques de YouTube disponibles à l'adresse: www.youtube.com/t/press_statistics.

cruelles des nations en croisade". Le texte était accompagné de sept photos, dont l'une montrait divers produits alimentaires, et les six autres des enfants équipés de fusils d'assaut et d'autres armes.

Outre la publication de matériel de collecte de fonds, Filiz G. intervenait de manière effective dans cette collecte. Pour préserver l'anonymat des donateurs, elle avait ouvert une boîte postale, à laquelle ceux-ci adressaient des enveloppes indiquant leur nom d'utilisateur Internet et contenant des espèces (généralement quelques centaines d'euros). Elle utilisait alors Western Union Financial Services pour transférer les fonds à un intermédiaire en Turquie, qui les transmettait à M. au Waziristan. Elle publiait également des vidéos sur Internet pour remercier les donateurs (qui, à cette fin, se voyaient attribuer des surnoms liés à leur nom d'utilisateur Internet) et les informer des avancées de la campagne de collecte de fonds.

Au procès, en mars 2011, l'accusée a reconnu les charges retenues à son encontre et a été condamnée à une peine de deux ans et demi d'emprisonnement. Dans sa décision, le tribunal a jugé qu'elle était pleinement consciente du fait que le matériel de propagande qu'elle diffusait provenait d'organisations terroristes et que les fonds qu'elle collectait et transférait étaient destinés à acheter, outre des biens humanitaires, des armes et des munitions pour ces organisations. En relevant que les infractions s'étaient principalement déroulées sur Internet, le juge a fait l'observation suivante:

"[…] le Tribunal attribue un poids particulier à la forte dangerosité de la diffusion de propagande djihadiste via l'Internet. Une fois téléchargés sur l'Internet, les matériels ne peuvent quasiment plus être contrôlés ou supprimés du Web, puisque d'autres utilisateurs peuvent les télécharger, les utiliser et les rediffuser. Compte tenu de son usage quasi mondial et de son nombre considérable et toujours plus grand d'utilisateurs, l'Internet est une plate-forme de plus en plus utilisée par les groupes terroristes pour diffuser leurs objectifs et leur propagande et susciter un climat mondial de craintes de menaces terroristes omniprésentes. La diffusion de contributions comme celles qui sont publiées par l'accusée représente donc un 'incendie criminel intellectuel'. Ses effets sont infiniment plus durables et elle est donc plus dangereuse que, par exemple, la diffusion de propagande au moyen de brochures ou d'autres médias imprimés."

414. L'affaire *R.* c. *Roshanara Choudhry*, jugée au Royaume-Uni, offre l'exemple d'une autodidacte, M^me^ Choudhry, qui s'est radicalisée pour commettre un acte violent au seul moyen de matériels trouvés sur Internet et, en particulier, de sites d'hébergement de vidéos. Cette instance a attiré l'attention de la communauté internationale sur la facilité avec laquelle M^me^ Choudhry avait pu, grâce aux plates-formes de partage de vidéos contenant des contenus générés par les utilisateurs, trouver et consulter des vidéos à contenu islamique extrémiste, et sur le processus par lequel la consultation permanente de ces contenus sur plusieurs mois avait forgé sa détermination à commettre un acte de terrorisme.

415. En 2010, après des discussions avec le Gouvernement du Royaume-Uni, menées par la cellule de détection et de répression Counter Terrorism Internet Referral Unit, et avec le Gouvernement des États-Unis, pays où se trouvent les serveurs de YouTube, la société mère de YouTube, Google Inc., a volontairement mis en place un système permettant aux utilisateurs de ce site de signaler les éventuels contenus terroristes. Ce mécanisme représente un outil important pour identifier de manière proactive les contenus susceptibles de promouvoir les actes de terrorisme.

416. Certains sites Web et plates-formes de réseau social incluent également dans leurs conditions d'utilisation des dispositions qui interdisent l'utilisation de leurs services pour promouvoir, entre autres, des activités terroristes. Par exemple, les conditions d'utilisation de Twitter[189], un réseau d'information en temps réel, interdisent d'utiliser ce service pour publier des menaces directes et spécifiques de violence envers d'autres personnes, à des fins illicites ou pour poursuivre des activités illégales[190]. En cas de non-respect de ces conditions, le prestataire de services se réserve le droit (mais n'a pas l'obligation) de supprimer ou de refuser de diffuser le contenu offensant ou de résilier le service. En outre, les utilisateurs de Twitter se limitent aux personnes qui ont le droit de bénéficier de prestations de services en vertu des lois des États-Unis ou d'autres pays compétents, ce qui exclut l'utilisation de ces services par les organisations terroristes désignées. Néanmoins, même si de telles conditions ont été mises en place, leur application peut poser des difficultés, en raison notamment du grand nombre d'utilisateurs et donc de l'importance des volumes de contenus à contrôler.

417. Des informations récemment parues dans la presse indiquent que, en cas de contrefaçon de droit d'auteur, Google supprime généralement les contenus ou liens illégaux dans un délai de six heures après la réception de la demande, bien que l'entreprise ait été inondée de plus de cinq millions de demandes de ce type en 2011[191]. La combinaison d'un mécanisme de signalement de contenus et d'une réponse tout aussi diligente et opportune aux contenus que l'on soupçonne liés au terrorisme constituerait une étape très positive dans la lutte contre l'utilisation d'Internet pour recruter, radicaliser et entraîner des terroristes, et pour faire l'apologie et inciter à commettre des actes de terrorisme.

418. Les contenus diffusés par les organisations terroristes portent souvent des signes distinctifs que l'on sait associés à une organisation donnée[192]. Le contrôle et la suppression de ces contenus facilement identifiables par les sites Web qui les hébergent pourraient présenter de gros avantages en matière de lutte contre la diffusion de propagande terroriste illégale. En outre, l'utilisation usuelle de mécanismes de signalement similaires à ceux qui sont mis en œuvre sur YouTube, sur les autres médias de réseau social et les moteurs de recherche Internet pourrait améliorer la probabilité de suppression en temps voulu de la propagande visant à servir les objectifs terroristes. Des mesures accrues d'identification des contenus relatifs au terrorisme, combinées avec des partenariats renforcés de partage d'informations formels et informels entre l'État et les acteurs privés, pourraient considérablement contribuer à identifier et contrer l'activité terroriste impliquant l'utilisation d'Internet.

[189] Disponible à l'adresse: https://twitter.com/tos.

[190] Voir http://support.twitter.com/articles/75576-reglement-de-twitter#.

[191] Jenna Wortham, "A political coming of age for the tech industry", *The New York Times*, 17 janvier 2012. Disponible à l'adresse: www.nytimes.com/2012/01/18/technology/web-wide-protest-over-two-antipiracy-bills.html?hp.

[192] "Jihadist use of social media: how to prevent terrorism and preserve innovation", témoignage d'A. Aaron Weisburd, Directeur, Society for Internet Research, devant le Comité sur la sécurité du territoire de la Chambre des représentants des États-Unis, Sous-comité sur la lutte contre le terrorisme et le renseignement, 6 décembre 2011.

419. Le partage d'informations est particulièrement important dans le contexte de la distinction entre les contenus en ligne contestables et ceux qui pourraient être illégaux (voir discussion à la section I.B.1). Par exemple, le système de signalement employé par YouTube peut aider à hiérarchiser l'examen de certains contenus, mais il faut ensuite déterminer si ces contenus atteignent le seuil nécessaire pour être supprimés ou bloqués. Un dialogue informel entre les FAI ou les sites Web hébergeant ces contenus d'une part, et les agents de justice pénale d'autre part, peut faciliter ce processus. À cette fin, les acteurs pertinents du secteur privé peuvent être encouragés à coopérer avec les autorités de détection et de répression en signalant les contenus contestables qui, selon les soupçons, sont liés à un utilisateur affilié à une organisation terroriste connue ou promeuvent les activités d'une telle organisation.

3. Moteurs de recherche Internet

420. Les moteurs de recherche constituent une passerelle entre les contenus Internet et l'utilisateur final. Les contenus qui en sont exclus ont un public nettement réduit. Certains de ces moteurs de recherche, tels Google et Yahoo, censurent volontairement les contenus jugés sensibles ou préjudiciables à leurs intérêts. Par exemple, après les attentats du 11 septembre 2001 aux États-Unis, de nombreux moteurs de recherche ont supprimé les résultats de recherche relatifs à de potentielles organisations terroristes[193]. Les dirigeants et les agents des services de détection et de répression de plusieurs États Membres ont encouragé des initiatives similaires pour rendre plus difficile l'accès via les moteurs de recherche aux contenus susceptibles de promouvoir des actes violents. La mise en œuvre spontanée d'un système de signalement des contenus relatifs au terrorisme, similaire à celui utilisé par YouTube, pourrait également être bénéfique.

4. Services de contrôle

421. Certains acteurs privés ont adopté une approche plus structurée pour contrer les activités terroristes sur Internet. Des services de contrôle tels que les organisations américaines Search for International Terrorist Entities (SITE) et Internet Haganah contrôlent et collectent les informations provenant de sources librement accessibles et se rapportant aux organisations terroristes[194]. L'organisation Search for International Terrorist Entities, qui collecte des renseignements, tire des revenus importants d'abonnements payants. Dès lors, cette organisation bénéficie, comme d'autres organismes similaires, d'un meilleur accès aux ressources permettant d'identifier rapidement et de traduire, le cas échéant, les activités Internet susceptibles de promouvoir les actes de terrorisme. Internet Haganah, en revanche, contrôle l'activité des groupes extrémistes islamistes sur Internet dans le but d'identifier les contenus relatifs au terrorisme et d'en interrompre l'accès. Internet Haganah est en partie financé par des dons et fonctionne principalement grâce à un réseau de bénévoles. Ce service de contrôle recherche et identifie de manière proactive les contenus Internet considérés comme liés au terrorisme ainsi que les sites Web les hébergeant. Il partage ces informations avec les autorités de

[193] Conway, "Terrorism and Internet governance: core issues", p. 30.

[194] Ibid, p. 31.

détection et de répression ou le public, ou les utilise pour contacter le site d'hébergement concerné et préconiser la suppression de ces contenus ou l'interruption de leur accès[195]. Les objectifs et le mode de fonctionnement de ces deux organisations diffèrent, mais leurs actions favorisent l'identification rapide de contenus relatifs au terrorisme, ce qui peut s'avérer utile en matière de renseignement, d'enquête et de poursuite de ces activités.

B. Partenariats public-privé

422. L'établissement de partenariats public-privé avec les acteurs intéressés présente de nombreux avantages dans la lutte contre l'utilisation d'Internet à des fins terroristes. En matière de cybercriminalité, l'absence de communication entre les services de détection et de répression et les prestataires de services à propos de la collecte des preuves, ainsi que les tensions existant entre le respect de la vie privée, d'une part, et la nécessité de conserver les données à des fins de détection et de répression, d'autre part, sont les obstacles souvent cités à la coopération public-privé. La création d'un lieu de dialogue formel et informel entre homologues du secteur public et du secteur privé pourrait fortement dissiper ces craintes. Outre les possibilités offertes par des réunions régulières entre les partenaires impliqués, des activités telles que des programmes de formation conjointe pourraient contribuer à surmonter les difficultés de communication et à renforcer la confiance entre les participants à ces partenariats[196].

423. Des progrès significatifs ont été réalisés en matière de création de partenariats public-privé sur les questions de sécurité liées à d'éventuelles attaques terroristes contre des cibles ou des infrastructures vulnérables, ou relatives à la prévention et à la poursuite de la cybercriminalité de manière générale. L'établissement de partenariats public-privé en matière de réglementation de l'utilisation d'Internet à des fins terroristes serait bénéfique. À titre d'exemple de partenariat fructueux, on peut citer l'Overseas Security Advisory Council (Conseil consultatif de sécurité à l'étranger), créé entre le Département d'État américain et les organisations américaines du secteur privé opérant à l'étranger. Cette assemblée offre un lieu d'échange des meilleures pratiques et une plate-forme de partage régulier et opportun d'informations entre le secteur privé et le Gouvernement américain à propos des évolutions observées en matière d'environnement de sécurité à l'étranger, et notamment de terrorisme, ainsi que des facteurs politiques, économiques et sociaux susceptibles d'avoir un impact sur l'environnement de sécurité à l'échelle mondiale et sur les pays individuels[197].

424. L'Indonesia Security Incident Response Team on Internet Infrastructure (équipe indonésienne d'intervention en cas d'incident lié à la sécurité de l'infrastructure Internet) offre un autre exemple d'initiative de partenariat public-privé axé sur la sécurité.

[195] Ariana Eunjung Cha, "Watchdogs seek out the web's bad side", *The Washington Post*, 25 avril 2005. Disponible à l'adresse: www.washingtonpost.com/wp-dyn/content/article/2005/04/24/AR2005042401473.html.

[196] Institut interrégional de recherche des Nations Unies sur la criminalité et la justice, "Public-private partnerships for the protection of vulnerable targets against terrorist attacks: review of activities and findings" (janvier 2009), par. 23.

[197] Ibid., par. 9.

Cette équipe rassemble des représentants des services postaux et des télécommunications, de la police nationale, du bureau de l'Attorney General, de Bank Indonesia, de l'Indonesian Internet Service Providers Association, de l'Indonesian Internet Café Association, de l'Indonesian Credit Card Association et de l'Indonesian ICT Society (MASTEL). Ses membres coopèrent pour, entre autres, mener des opérations de contrôle, de détection et de signalement précoce des menaces et perturbations sur les réseaux de télécommunications basés sur un protocole Internet, engager des activités de recherche et de développement, fournir des laboratoires de simulation et dispenser des formations sur la sécurité de l'utilisation des réseaux de télécommunications basés sur un protocole Internet, offrir des services consultatifs et une assistance technique aux organismes ou institutions stratégiques, et assurer la coordination entre les institutions ou organismes stratégiques pertinents, tant nationaux qu'internationaux[198].

425. En novembre 2006, le Forum mondial pour des partenariats public-privé dans la lutte contre le terrorisme a été organisé à Moscou. À la suite de ce forum, le Groupe des Huit[199] a adopté la Stratégie de partenariat public-privé pour la lutte contre le terrorisme[200], qui promeut notamment la coopération entre les fournisseurs d'accès à l'Internet ou autres entreprises et les autorités gouvernementales pour lutter contre l'utilisation abusive d'Internet par les terroristes et empêcher que soient ainsi franchis les derniers pas qui conduisent de l'extrémisme au terrorisme. En vertu de cette Stratégie, les gouvernements sont encouragés à établir des partenariats plus étroits et librement consentis avec les fournisseurs de services Internet, au niveau local comme à l'échelon international, afin de combattre l'utilisation d'Internet dans le cadre d'activités telles que le recrutement, l'entraînement et l'incitation à commettre des actes terroristes.

426. Parmi les autres initiatives pertinentes, on peut citer le groupe de travail du Conseil de l'Europe créé en 2007, avec des participants des services de détection et de répression, du secteur d'activité et des associations de prestataires de services, pour examiner les questions relatives à la cybercriminalité de manière générale. Cette initiative a pour but d'améliorer la coopération entre les autorités de détection et de répression et le secteur privé, et de lutter plus efficacement contre la cybercriminalité.

427. En 2010, la Commission européenne a approuvé et financé un projet qui implique une collaboration entre le monde universitaire, le secteur d'activité, et les services de détection et de répression, et qui vise à créer un réseau nommé Cybercrime Centres of Excellence Network for Training Research and Education (2CENTRE) en Europe. Ce réseau propose actuellement des formations par le biais de centres d'excellence nationaux situés en Irlande et en France. Chaque centre national est financé par un partenariat entre les représentants des services de détection et de répression, du monde universitaire et du secteur d'activité, qui collaborent pour élaborer les programmes et les outils de formation pertinents qui seront utilisés dans la lutte contre la cybercriminalité (voir la section IV.G).

[198] Soumission écrite de l'expert de l'Indonésie.

[199] Forum non officiel des chefs des pays industrialisés suivants: Allemagne, Canada, États-Unis, Fédération de Russie, France, Italie, Japon et Royaume-Uni.

[200] A/61/606-S/2006/936, annexe.

428. Les partenariats public-privé visant expressément l'utilisation d'Internet par des terroristes pourraient également offrir un moyen de promouvoir des lignes directrices claires concernant le partage d'informations entre le secteur privé et le secteur public, conformes à la réglementation applicable sur la protection des données. Les Lignes directrices pour la coopération entre organes de répression et fournisseurs de services Internet contre la cybercriminalité constituent une bonne base[201]. Ces lignes directrices portent principalement sur l'établissement de relations de confiance mutuelle et de coopération entre les acteurs du secteur public et ceux du secteur privé comme base de coopération. Elles mettent également l'accent sur la nécessité de promouvoir des procédures efficaces et rentables de coopération. Les forces de l'ordre et les fournisseurs de services Internet sont encouragés à s'engager dans des échanges d'informations visant à renforcer leur capacité à identifier et combattre la cybercriminalité par la tenue de réunions régulières, et à partager les bonnes pratiques et retours d'informations. Les lignes directrices encouragent également l'établissement de partenariats formels et de procédures écrites comme base de relations à long terme, avec, entre autres, les garanties appropriées de façon à ce que le partenariat n'enfreigne pas les droits des participants du secteur ou les pouvoirs légaux des forces de l'ordre[202].

429. Les mesures recommandées devant être prises par les forces de l'ordre conformément aux lignes directrices sont notamment les suivantes:

- Engager une coopération élargie et stratégique avec les fournisseurs de services Internet, notamment en conduisant régulièrement des séminaires de formation technique et juridique, ainsi qu'en faisant remonter les informations collectées à l'occasion des plaintes enregistrées ou des renseignements obtenus par les fournisseurs de services;
- Fournir des explications et de l'assistance aux fournisseurs de services Internet en matière de techniques d'investigation générales afin qu'ils puissent mieux comprendre comment la coopération des fournisseurs de services Internet débouchera sur des investigations plus efficaces;
- Définir les priorités dans les requêtes concernant de gros volumes de données tout en évitant de susciter des coûts inutiles et de perturber l'activité des fournisseurs de services[203].

430. Les mesures recommandées devant être prises par les fournisseurs de services Internet conformément aux lignes directrices sont notamment les suivantes:

- Coopération visant à réduire l'utilisation des services à des fins illicites;
- Dénonciation des activités criminelles aux autorités en charge des poursuites;
- Si possible, communication sur demande de la liste des types de données

[201] Conseil de l'Europe, Division du crime économique, "Lignes directrices pour la coopération entre organes de répression et fournisseurs de services Internet contre la cybercriminalité" (Strasbourg, 2 avril 2008). Disponibles à l'adresse: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/Reports-Presentations/567_prov-d-guidelines_provisional2_3April2008_fr.pdf.

[202] Ibid., par. 10 à 13.

[203] Ibid., par. 17, 29, 30 et 33.

pouvant être mis à disposition pour chaque service à la réception d'une requête de divulgation valide émanant des forces de l'ordre[204].

431. Les partenariats public-privé peuvent également fournir une structure permettant de promouvoir des normes minimales de conservation sécurisée des données par les acteurs du secteur privé et d'améliorer les canaux de communication des informations transmises par les acteurs du secteur privé à propos des activités suspectes.

[204] Ibid., par. 41, 42 et 50.

VIII. Conclusion

A. Utilisation d'Internet à des fins terroristes

432. Les premiers chapitres du présent document offrent un aperçu, élaboré selon des critères fonctionnels, de la façon dont l'Internet est souvent utilisé pour promouvoir et soutenir les actes de terrorisme, particulièrement en matière de propagande (notamment aux fins de recrutement, de radicalisation et d'incitation au terrorisme), d'entraînement, de financement, de planification et d'exécution de ces actes. Ces chapitres mettent également l'accent sur les possibilités offertes par cette technologie pour prévenir, détecter et décourager les actes de terrorisme. À ce titre, on peut citer la collecte de renseignements et d'autres activités visant à prévenir et contrer de tels actes, ainsi que le recueil de preuves pour les poursuivre.

433. Les contre-communications et autres communications stratégiques peuvent constituer des moyens efficaces d'interrompre le processus de radicalisation vers des idéaux extrémistes, qui peut à son tour se traduire par des actes de terrorisme. Il importe également de comprendre les origines plus générales de la radicalisation pour entamer un dialogue constructif avec les recrues potentielles d'une cause terroriste, et promouvoir les moyens légaux de réaliser leurs aspirations politiques, sociales ou religieuses légitimes.

434. Le respect des droits de l'homme et de l'état de droit fait partie intégrante de la lutte contre le terrorisme. Les États Membres ont en particulier réaffirmé ces obligations dans la Stratégie antiterroriste mondiale des Nations Unies, en reconnaissant "qu'une action efficace contre le terrorisme et la protection des droits de l'homme sont des objectifs non pas contradictoires mais complémentaires et synergiques". L'efficacité de la mise en œuvre d'une approche fondée sur l'état de droit pour contrer l'utilisation d'Internet à des fins terroristes doit être évaluée à toutes les étapes des initiatives de lutte contre le terrorisme, de la collecte préventive de renseignements à la garantie d'une procédure régulière lorsque des poursuites sont exercées contre un suspect.

B. Contexte international

435. Actuellement, il n'existe ni traité global des Nations Unies sur le terrorisme, ni définition officielle de ce terme. Néanmoins, les États Membres de l'Organisation des Nations Unies sont en train d'élaborer une convention générale sur le terrorisme international, qui viendra compléter le cadre juridique existant en matière de lutte contre le terrorisme. Ce cadre se compose de toute une série de sources, dont des résolutions de l'Assemblée générale et du Conseil de sécurité, des traités, de la jurisprudence et

du droit international coutumier. Plusieurs instruments régionaux et sous-régionaux offrent également des normes de fond et de procédure extrêmement utiles pour ériger en infractions pénales les actes de terrorisme perpétrés au moyen d'Internet.

436. Les États Membres ont décidé, conformément à la Stratégie antiterroriste mondiale, d'agir d'urgence pour prévenir et combattre le terrorisme sous toutes ses formes et dans toutes ses manifestations et, en particulier:

a) D'envisager de devenir parties sans plus tarder aux conventions et protocoles internationaux en vigueur relatifs à la lutte contre le terrorisme, d'appliquer ces instruments et de n'épargner aucun effort pour parvenir à un accord et conclure une convention générale sur le terrorisme international;

b) D'appliquer toutes les résolutions de l'Assemblée générale relatives aux mesures visant à éliminer le terrorisme international et les résolutions pertinentes de l'Assemblée qui ont trait à la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste;

c) D'appliquer toutes les résolutions du Conseil de sécurité relatives au terrorisme international et de coopérer pleinement avec les organes subsidiaires du Conseil chargés de la lutte antiterroriste dans l'accomplissement de leurs mandats.

C. Cadres politiques et législatifs

1. Politiques

437. Pour apporter des réponses de justice pénale efficaces aux menaces présentées par l'utilisation d'Internet par des terroristes, les gouvernements doivent élaborer des politiques et des lois nationales claires portant, entre autres, sur: *a)* l'incrimination des actes illégaux commis par des terroristes sur Internet ou sur des services connexes; *b)* l'octroi de pouvoirs d'investigation aux services de détection et de répression chargés de mener les enquêtes liées au terrorisme; *c)* la réglementation des services connexes à Internet (par exemple, FAI) et le contrôle des contenus; *d)* la facilitation de la coopération internationale; *e)* la mise au point de procédures spécialisées en matière judiciaire ou probatoire; et *f)* le maintien de normes internationales des droits de l'homme.

438. La classification globale des approches stratégiques proposée par le Groupe de travail sur la lutte contre l'utilisation d'Internet à des fins terroristes de l'Équipe spéciale de lutte contre le terrorisme, qui implique l'utilisation d'une législation générale sur la cybercriminalité, d'une législation générale (non spécifique à l'Internet) sur la lutte contre le terrorisme et d'une législation spécifique à Internet en la matière, fournit un cadre conceptuel utile aux dirigeants et aux législateurs. Actuellement, seuls quelques États ont élaboré une législation ciblant expressément les actes commis par des terroristes sur Internet. La plupart des pays ont recours aux lois pénales générales, à la législation sur la cybercriminalité et/ou à la législation sur la lutte contre le terrorisme pour incriminer et poursuivre ce type d'infractions.

2. Législation

439. Les terroristes utilisent l'Internet dans le cadre d'actions visant à commettre des infractions matérielles (par exemple, attentats à l'explosif), mais également pour mener d'autres activités de soutien (par exemple, diffusion de propagande ou recrutement et entraînement de membres). Les pays ont eu recours à différentes méthodes pour incriminer les actes illégaux associés au terrorisme et commis via l'Internet.

440. Dans sa résolution 1624 (2005), le Conseil de sécurité a, entre autres, appelé les États à incriminer l'incitation à commettre des actes terroristes. Les États sont tenus, aux termes de cette résolution et d'autres instruments internationaux, de s'assurer que les mesures visant les actes incitant au terrorisme sont pleinement conformes aux obligations internationales qui leur incombent en vertu du droit des droits de l'homme, du droit des réfugiés et du droit humanitaire.

441. L'élaboration et l'application de lois incriminant l'incitation à commettre des actes de terrorisme tout en protégeant pleinement les droits de l'homme (par exemple, le droit à la liberté d'expression) constituent des défis permanents pour les dirigeants, les législateurs, les services de détection et de répression et les procureurs de tous les pays. Les États ont adopté différentes méthodes pour incriminer les actes d'incitation au terrorisme. Certains ont expressément érigé en infractions pénales les actes d'incitation ou d'apologie des actes terroristes, tandis que d'autres se fondent sur des infractions telles que l'incitation ou l'entente criminelle.

442. Les enquêtes sur les affaires de terrorisme impliquant l'utilisation d'Internet ou d'autres services connexes par les suspects nécessitent souvent l'utilisation de pouvoirs d'enquête spécialisés par les services de détection et de répression. La plupart des gouvernements ont adopté une législation permettant à ces services de mener de telles activités dans ce type d'enquêtes. Ces techniques devraient être dûment autorisées en vertu des lois nationales et mises en œuvre de manière à assurer le respect des droits de l'homme fondamentaux protégés par le droit international des droits de l'homme.

443. Les autorités ont besoin de la coopération des opérateurs de télécommunications lorsqu'elles mettent en œuvre un contrôle électronique, procèdent à des mises sur écoute ou utilisent des techniques d'enquête électroniques similaires. Il est souhaitable que les gouvernements donnent un fondement juridique clair aux obligations imposées aux parties du secteur privé, et précisent notamment les spécifications techniques requises de leurs réseaux et les modes de prise en charge des frais de mise à disposition de ces capacités.

444. Il apparaît que des terroristes ont utilisé des cybercafés pour mener leurs activités, mais l'ampleur du problème reste inconnue. Certains gouvernements ont imposé des obligations spécifiques aux opérateurs de cybercafés à des fins de détection et de répression (notamment antiterroristes) concernant l'obtention, la conservation et, sur demande, la communication aux services compétents de l'identification photographique, de l'adresse et des données d'usage/de connexion des clients. On n'évalue pas très bien l'utilité d'appliquer ces mesures aux seuls cybercafés alors que d'autres formes d'accès

public à Internet (par exemple, aéroports, bibliothèques et points d'accès public sans fil) offrent aux criminels (terroristes inclus) les mêmes possibilités et ne sont pas réglementées.

445. La mesure dans laquelle les gouvernements devraient réglementer les contenus relatifs au terrorisme sur l'Internet est une question complexe, qui nécessite de concilier les considérations de détection et de répression et celles ayant trait aux droits de l'homme (par exemple, le droit à la liberté d'expression). Les manières de procéder sont variables, certains États appliquant des contrôles réglementaires stricts aux FAI et autres prestataires de services connexes, et utilisant parfois des technologies destinées à filtrer ou bloquer l'accès à certains contenus. D'autres États adoptent une approche plus légère, et s'appuient dans une plus grande mesure sur l'autorégulation du secteur de l'information. La plupart des FAI, des sociétés d'hébergement Web, des sites de partage de fichiers et de réseau social ont des conditions d'utilisation qui interdisent certains contenus; certains contenus relatifs au terrorisme pourraient enfreindre ces restrictions contractuelles.

D. Enquêtes et collecte de renseignements

446. En matière d'Internet, les enquêtes efficaces s'appuient sur une combinaison de méthodes classiques, de connaissance des outils permettant de mener une activité illicite via l'Internet et d'élaboration de pratiques visant à identifier, appréhender et poursuivre les auteurs de tels actes. Une approche proactive des stratégies d'enquête et des outils spécialisés connexes qui tirent parti des ressources en constante évolution d'Internet favorise l'identification efficace des données et des services les plus utiles à l'enquête.

447. Les enquêteurs dotés des compétences techniques appropriées disposent de toute une gamme d'utilitaires et de matériels informatiques spécialisés. Si possible, il convient de veiller, dans les affaires impliquant l'obtention de preuves numériques, à mettre en place des procédures normalisées de récupération de données facilitant l'extraction du maximum de preuves disponibles ainsi que la préservation de l'intégrité de la source des données et de la chaîne de conservation, pour assurer leur recevabilité dans une procédure judiciaire. En raison de la fragilité des preuves numériques, leur évaluation, leur obtention et leur examen sont plus efficaces lorsque des experts en criminalistique spécialement formés s'en chargent.

E. Coopération internationale

448. Dans de nombreuses affaires liées au terrorisme, notamment celles qui impliquent certains aspects d'utilisation d'Internet par les délinquants, une coopération internationale efficace constitue un facteur important des poursuites. Les États sont tenus, en vertu de nombreux instruments internationaux, régionaux, multilatéraux et bilatéraux relatifs au terrorisme et à la criminalité transnationale organisée, d'établir des politiques et des cadres législatifs pour faciliter la coopération internationale en matière d'enquête

et de poursuite concernant des actes de terrorisme ou des infractions graves connexes. Actuellement, il n'existe pas d'instrument universel relatif à la cybercriminalité ou au terrorisme qui impose aux États des obligations spécifiques en matière de coopération internationale. Cette situation constitue un obstacle à l'efficacité de la coopération internationale dans certaines enquêtes et poursuites liées au terrorisme.

449. Les canaux formels de coopération internationale restent essentiels, mais en pratique, les voies informelles deviennent tout aussi importantes. Quel que soit le mode de coopération, la confiance entre les autorités nationales respectives est, dans de nombreux cas, un élément clef d'une coopération internationale efficace. Indépendamment des mécanismes prévus par les traités formels ou les instruments juridiques similaires, les initiatives régionales ou sous-régionales ne reposant pas sur des traités et visant à renforcer la coopération en matière de détection et de répression sont également importantes. Les pays ayant des intérêts communs dans certains domaines thématiques relatifs à la sécurité pourraient conclure des arrangements collectifs prévoyant l'échange d'informations et le partage de renseignements.

450. L'existence d'un cadre législatif national prévoyant une coopération internationale efficace est fondamentale pour faciliter cette coopération dans les enquêtes et les poursuites concernant des affaires de terrorisme. Cette législation devrait incorporer dans le droit interne d'un pays les principes relatifs à la coopération et à la criminalité transnationale organisée pertinente énoncés dans les instruments universels contre le terrorisme.

451. La législation est une composante fondamentale d'un régime efficace de coopération internationale, mais elle ne suffit pas. L'existence d'une autorité centrale dotée de moyens suffisants, intervenant en amont et capable, en utilisant toutes les voies disponibles, de faciliter l'entraide judiciaire est également essentielle. Enfin, il est important d'établir et de maintenir des relations de confiance avec les homologues étrangers intervenant dans la coopération en matière d'enquêtes criminelles transfrontalières.

452. En sus des voies formelles, les autorités doivent développer et utiliser les canaux informels de coopération bilatérale. De nombreux services de détection et de répression nationaux gèrent un réseau de postes de liaison internationaux, qui facilite considérablement les demandes de coopération internationale. Les instruments universels de lutte contre le terrorisme ne mentionnent pas expressément les équipes d'enquête conjointe, mais cette stratégie de coopération est parfaitement conforme aux principes sous-jacents et à l'esprit des dispositions de ces instruments ayant trait à la coopération internationale. Certains pays, en particulier européens, ont adopté cette méthode avec succès dans un certain nombre d'enquêtes liées au terrorisme.

453. En dépit des améliorations, les procédures formelles d'entraide judiciaire en matière pénale restent des processus de longue haleine, qui nécessitent un travail administratif considérable. Dans les affaires impliquant la préservation de données détenues par un FAI d'un autre pays, les autorités devraient pouvoir coopérer directement et de manière informelle avec ce FAI pour préserver ces données aux fins d'enquêtes ou de poursuites relatives à une infraction pénale. Dans d'autres situations, l'exercice d'un

pouvoir coercitif et l'obtention d'une autorisation judiciaire peuvent s'avérer nécessaires concernant, par exemple, la préservation, la recherche et la saisie de données relatives à Internet pour les produire et les utiliser à titre de preuves dans une procédure pénale.

454. Les enquêteurs et les procureurs devraient être pleinement conscients de l'importance potentielle de ces données et de la nécessité de prendre le plus rapidement possible des mesures pour les préserver, d'une manière qui garantisse leur recevabilité à titre de preuves lors d'une procédure judiciaire ultérieure. Dans la mesure du possible, les services nationaux de détection et de répression devraient élaborer, soit directement avec les FAI, soit avec les organismes équivalents d'autres pays, des procédures claires, comportant des éléments tant formels qu'informels, visant à assurer le plus rapidement possible la conservation et la production des données d'usage Internet requises dans une enquête criminelle.

455. Lors de la réunion du groupe d'experts, certains spécialistes ont souligné que la nécessité, pour les autorités nationales, de protéger le matériel de renseignement sensible constituait souvent un obstacle au partage d'informations.

456. Lorsqu'elles envisagent de mener dans d'autres pays des actions impliquant la collecte de preuves numériques, les autorités devraient être attentives aux implications que ces actions pourraient avoir en termes de souveraineté sur d'autres États. Dans la mesure du possible, les autorités envisageant des mesures d'enquête relatives à des personnes ou des objets qui se trouvent dans un autre pays devraient en informer leurs homologues du pays concerné et coordonner leurs actions avec elles.

457. Les données relatives à Internet (par exemple, données d'usage des clients) constituent des preuves importantes dans de nombreuses affaires de terrorisme. Dans ces instances, les autorités devraient veiller à ce que les données pertinentes soient préservées pour être ultérieurement utilisées à titre de preuves dans la procédure. À cet égard, il importe de relever la distinction entre la notion de "conservation" des données (données conservées par un FAI en vertu d'une obligation réglementaire) et celle de "préservation" des données (données préservées en vertu d'une ordonnance ou d'une autorisation judiciaire). Dans de nombreux pays, la loi contraint les FAI à conserver certains types de données relatives aux communications pendant une période spécifiée. Néanmoins, malgré les efforts accomplis (par exemple, au niveau régional en Europe), il n'existe pas d'accord international sur le type de données qui devraient être conservées par les FAI ou sur la durée de cette conservation. Dès lors, il existe à l'échelle internationale une forte disparité sur ces deux points. Cela peut poser problème lorsque les autorités ont besoin d'obtenir des données relatives aux communications situées dans un pays pour s'en servir à titre de preuves dans le cadre d'une procédure pénale engagée dans un autre pays.

458. L'élaboration d'un cadre réglementaire universellement accepté imposant des obligations cohérentes à tous les FAI en matière de type et de durée de conservation des données d'usage des clients, serait extrêmement utile aux services de détection, de répression et de renseignement qui enquêtent sur les affaires de terrorisme. En l'absence d'un tel cadre, les autorités devraient déterminer le plus tôt possible s'il existe des

données pertinentes dans le cadre de l'enquête et l'endroit où elles se trouvent, et prendre sans délai des mesures pour les préserver afin qu'elles puissent être utilisées à titre de preuves.

459. Dans la mesure du possible, les autorités devraient établir des relations ou conclure des accords informels avec les FAI (tant nationaux qu'étrangers) susceptibles de détenir des données pertinentes à des fins de détection et de répression, concernant les procédures de communication de ces données au cours des enquêtes. En l'absence de procédures informelles, les autorités devraient collaborer dès que possible avec leurs homologues étrangères, si nécessaire via les canaux formels et les autorisations judiciaires appropriées, à propos de la préservation de ces données.

460. En matière de preuves, les affaires de terrorisme nécessitant des investigations transfrontalières ajoutent une étape supplémentaire à la tâche déjà complexe des enquêteurs et des procureurs, en les contraignant à faire en sorte que les méthodes utilisées pour recueillir des preuves (éventuellement dans plusieurs pays) et les produire lors de poursuites exercées dans une autre juridiction soient pleinement conformes aux lois et aux principes applicables dans tous les pays pertinents.

461. L'exigence de double incrimination (le fait que les actes auxquels l'extradition et l'entraide judiciaire se rapportent constituent des infractions dans les deux États), visée dans de nombreux instruments bilatéraux et multilatéraux relatifs au terrorisme et à la criminalité transnationale organisée, peut présenter des difficultés dans les affaires pénales, dont celles relatives au terrorisme, qui comportent un élément quelconque de coopération internationale.

462. Les affaires de terrorisme dans lesquelles les actes constitutifs d'infraction sont commis sur Internet soulèvent parfois des questions complexes de compétence, en particulier lorsqu'un suspect se trouve dans un pays et utilise des sites Internet ou des services hébergés par des FAI situés dans un autre pays. Ce type d'affaire a déjà concerné des personnes qui résidaient dans un pays et qui créaient et administraient des sites Web en vue de promouvoir le djihad et d'autres actes violents relatifs au terrorisme.

463. Le droit international ne prévoit pas de règle contraignante régissant la manière dont les États devraient gérer les situations dans lesquelles plusieurs d'entre eux pourraient faire valoir leur compétence pour connaître d'une infraction impliquant le même suspect. Généralement, les autorités nationales mettent en balance ou évaluent les facteurs pertinents, notamment le degré de connectivité existant entre les divers pays et l'infraction alléguée, pour déterminer si elles doivent déclarer et exercer leur compétence dans une instance donnée. En cas de revendications de compétence concurrente, il est important que les autorités centrales pertinentes (généralement, les organismes nationaux chargés des poursuites) communiquent immédiatement et collaborent pour résoudre ces questions.

464. La législation nationale relative à la protection des données ou à la vie privée restreint souvent la capacité des services de détection, de répression et de renseignement

à partager des informations avec leurs homologues nationaux et étrangers. La conciliation du droit humain à la vie privée et de l'intérêt légitime de l'État à enquêter et à poursuivre avec efficacité les infractions constitue un défi permanent pour les gouvernements et, dans certains cas (notamment en matière de réponses au terrorisme), une source de préoccupation.

F. Poursuites

465. Un élément essentiel du cadre juridique universel contre le terrorisme, la Stratégie antiterroriste mondiale des Nations Unies, concerne l'obligation faite aux États de refuser l'asile aux auteurs d'actes terroristes, et de les traduire en justice quel que soit l'endroit où ces actes se produisent. En sus du cadre législatif nécessaire, la capacité institutionnelle des organismes nationaux chargés des poursuites à respecter l'état de droit dans les affaires de terrorisme, conformément aux droits de l'homme des suspects et des accusés définis par le droit international des droits de l'homme, fait partie intégrante d'une réponse de justice pénale efficace au terrorisme.

466. Il est fréquent que les procureurs n'interviennent pas seulement dans la phase de poursuites des affaires de terrorisme, mais qu'ils aient également un rôle direct dans la phase d'enquête, en fournissant des conseils juridiques et stratégiques sur des questions qui auront une influence sur l'issue des poursuites. Ils joueront probablement ce rôle dans le cadre d'une équipe multidisciplinaire et plurijuridictionnelle. Le haut niveau de confiance, de coordination et de communication qui est essentiel à une coopération internationale efficace, doit également exister entre les services nationaux de détection, de répression, de renseignement et chargés des poursuites.

467. Les nouvelles techniques d'enquête offrent aux autorités des possibilités accrues de cibler les activités terroristes sur l'Internet, mais elles comportent également des risques juridiques auxquels les procureurs doivent rester vigilants. Compte tenu des disparités existant entre les droits nationaux en matière de collecte et de recevabilité des preuves, ces risques sont plus élevés lorsque les actes à l'origine des preuves ne se sont pas déroulés dans le pays où le procès a lieu.

468. Dans la plupart des pays, les procureurs disposent d'un large pouvoir discrétionnaire pour décider s'ils doivent engager une procédure pénale, et sur quels chefs d'accusation. Ces décisions sont souvent prises conformément aux lignes directrices ou aux codes qui visent à assurer l'exercice juste, transparent et cohérent de cet important pouvoir discrétionnaire, et qui prévoient souvent des seuils fondés sur la suffisance des preuves et l'intérêt public.

469. Les enquêtes liées au terrorisme ont pour objectif principal la sécurité publique. Dans certains cas, les autorités doivent intervenir pour empêcher la commission d'actes terroristes avant d'avoir obtenu suffisamment de preuves pour engager des poursuites au titre des actes terroristes qu'elles estiment en cours de planification.

470. Dans ces situations, les autorités doivent parfois s'appuyer sur d'autres infractions pénales pour fonder juridiquement leurs actions, notamment sur des infractions telles

que l'incitation, l'entente criminelle, l'association de malfaiteurs ou le fait de fournir un soutien matériel aux terroristes, et non sur des infractions matérielles relatives aux actes terroristes dont la planification est en cours. Les autorités peuvent utiliser d'autres dispositions pénales générales relatives à la fraude ou à la possession ou l'utilisation d'objets illégaux (par exemple, faux documents d'identité ou de voyage, armes) pour interrompre ou compromettre les activités des groupes terroristes avant l'exécution des attaques ou des activités planifiées.

471. Dans de nombreuses affaires de terrorisme, les preuves utilisées par l'accusation sont fondées sur le renseignement. L'intégration des activités de renseignement dans les systèmes de justice pénale reste un problème fondamental en matière de lutte contre le terrorisme. Comment les autorités peuvent-elles protéger le matériel sensible étayant les preuves tout en respectant l'obligation de garantir aux accusés un procès équitable et une défense effective, et notamment de communiquer à la défense tous les arguments pertinents de l'accusation?

472. Dans les affaires de terrorisme impliquant l'utilisation d'ordinateurs ou d'Internet, les preuves numériques constituent une partie importante de l'accusation. L'utilisation de ce type de preuves soulève inéluctablement des questions relatives à leur recevabilité. Il est essentiel de veiller, tout au long de l'enquête et des poursuites, à la parfaite conformité des méthodes de collecte, de préservation, d'analyse et de production des éléments aux règles probatoires ou procédurales pertinentes, et au respect des bonnes pratiques établies.

473. Les autorités chargées des poursuites devront convaincre un tribunal de la fiabilité des preuves numériques, et notamment des méthodes utilisées pour les recueillir, les analyser et les produire. On nomme les procédures de préservation de l'intégrité des preuves la "chaîne de conservation" ou la "chaîne de preuves". Lorsque ces preuves sont collectées dans un pays pour être utilisées au cours d'un procès se déroulant dans un autre, la situation est beaucoup plus compliquée et nécessite une attention particulière de la part des enquêteurs et des procureurs. Dans les affaires où les autorités déterminent qu'il existe des preuves pertinentes et les localisent, elles devraient étudier les moyens (informels et formels) de les obtenir et de les préserver. Il faut que le mode opératoire choisi garantisse la recevabilité des preuves dans le pays où le procès aura lieu.

474. Les principes et processus juridiques relatifs à la collecte et à la recevabilité des preuves en matière pénale diffèrent selon les pays. Dans les enquêtes transfrontalières, une part significative du travail des autorités concerne la "transmission" des différents éléments de preuve. Le processus est parfois complexe et chronophage, mais constitue un facteur essentiel de succès. Les avocats de la défense invoqueront presque certainement toutes les failles juridiques des méthodes de collecte, de préservation, de transmission ou de production des preuves utilisées au procès.

475. Dans les affaires de terrorisme, le procureur est souvent tenu de produire des témoignages d'experts pour prouver certains aspects spécialisés de son argumentation. Parmi les domaines dans lesquels un témoignage d'expert est fréquemment nécessaire, on peut citer la technologie et la communication, ainsi que l'idéologie, les activités et

la structure organisationnelle des groupes terroristes. Il est très possible que les procureurs aient besoin de plusieurs témoins experts. Lorsque l'intervention d'un témoin expert est requise, trois phases ou étapes se présentent généralement: *a)* détermination claire des questions qui nécessitent un avis d'expert (et de leur objet); *b)* identification d'un expert qualifié; et *c)* vérification du fait que cet expert utilise des moyens recevables.

476. Dès que possible, les procureurs devraient déterminer les questions qui nécessiteront probablement des témoignages d'experts et charger les experts d'entreprendre l'analyse requise, en leur fournissant si nécessaire des conseils précis sur les principales règles de procédure ou de preuve. Lorsqu'ils choisissent les témoins experts, les procureurs doivent se demander s'il convient de faire appel à des experts gouvernementaux ou non. Le recours aux experts gouvernementaux offre certains avantages, mais n'est pas nécessairement souhaitable si des sources ou des méthodes de renseignement sensibles étayent les preuves. L'identification d'un expert compétent, en particulier dans des domaines très spécialisés, peut constituer un défi important dans les juridictions moins développées. Dans la mesure du possible, les témoins experts devraient respecter et appliquer les bonnes pratiques reconnues du domaine sur lequel ils sont appelés à témoigner. En raison de la complexité de certains témoignages d'experts, il convient d'envisager des façons novatrices de présenter ces preuves complexes aux juges, aux jurys ou aux autres personnes chargées d'établir les faits, d'une manière qui soit facilement compréhensible. Il importe que le procureur ait une bonne connaissance pratique du domaine concerné.

477. Compte tenu de la complexité des poursuites relatives au terrorisme, et particulièrement de celles qui impliquent une coopération internationale ou des éléments extrêmement techniques, il est extrêmement souhaitable qu'une équipe de procureurs soit chargée de l'affaire. Afin de garantir une approche intégrée fondée sur l'état de droit et de préserver l'intégrité des réponses de justice pénale au terrorisme, les pays doivent disposer de processus solides et constants visant à renforcer la capacité des procureurs à appliquer la législation nationale de lutte contre le terrorisme et les obligations de coopération internationale connexes. Dans les pays où le risque d'activité terroriste est élevé et où les capacités institutionnelles au sein des services chargés des poursuites et des autres organismes de justice pénale sont limitées, il convient de privilégier le développement de capacités spécialisées au sein de ces services, tant en termes de poursuites que concernant les mécanismes connexes de coopération internationale.

G. Coopération du secteur privé

478. Si la responsabilité de la lutte contre l'utilisation d'Internet à des fins terroristes incombe *in fine* aux États Membres, la coopération des principaux acteurs du secteur privé est essentielle en termes d'efficacité. Un dialogue proactif avec les acteurs du secteur privé tels que les prestataires de services, les sites Web hébergeant des contenus générés par les utilisateurs et les moteurs de recherche Internet continue de jouer un rôle important en matière de contrôle de l'existence de contenus relatifs au terrorisme diffusés sur Internet.

479. L'établissement de partenariats public-privé relativement à la réglementation de l'utilisation d'Internet à des fins terroristes serait bénéfique. Des initiatives similaires ont été élaborées avec succès concernant d'autres domaines de la lutte contre le terrorisme, et pour combattre la cybercriminalité de manière générale. Ces initiatives fournissent un lieu de dialogue formel et informel entre homologues du secteur public et du secteur privé. Elles favorisent également des activités telles que les programmes de formation conjointe qui pourraient contribuer à surmonter les obstacles de communication et à renforcer la confiance, la compréhension et l'élaboration de pratiques harmonisées entre les participants à ces partenariats.

Annexe

Liste des contributeurs

Algérie

M. Bachir Said
Commissaire de police
Direction générale de la sûreté nationale

Allemagne

M. Christian Monka
Procureur principal

Dr Uwe E. Kemmesies
Chef de l'Unité de recherche sur le terrorisme/l'extrémisme
Office fédéral de police criminelle

M. Florian Thurner
Mission permanente de l'Allemagne, Vienne

Autriche

M. David Blum
Ministère fédéral de l'intérieur
Administration fédérale pour la protection de la Constitution et la lutte contre le terrorisme

M. Hannes Schneider

Brésil

M. Romulo Dantas
Directeur du Département de lutte contre le terrorisme
Cabinet de la sécurité internationale/Service de renseignement brésilien

Canada

M. Dominique Dudemaine
Avocat-conseil
Service des poursuites pénales du Canada

Chine

M. Bin Hu
Conseiller
Mission permanente de la Chine, Vienne

Mme Xuena Lu
Directrice de division adjointe
Bureau de la sécurité des réseaux, Ministère de la sécurité publique

Colombie

Capitaine Luis Fernando Atuesta Zárate
Groupe des enquêtes technologiques
Direction des enquêtes criminelles et Organisation internationale de police criminelle (INTERPOL)
Police nationale

Lieutenant Nadres Bernardo Molina Vivas
Groupe des enquêtes technologiques
Direction des enquêtes criminelles et INTERPOL
Police nationale

M. Mauricio Aguirre Patiño
Procureur spécialisé
Cellule nationale de poursuite du terrorisme

Égypte

Dr Ehab Maher Elsonbaty
Juge principal

Espagne

M. Alfonso Estévez Ochoa
Inspecteur chef au Bureau général de l'information
Police nationale espagnole

M. Ismael Romero Ramos
Capitaine
Chef, Bureau de l'information
Garde civile

M. Sergio De Frutos Pariente
Bureau général de l'information
Ministère de l'intérieur

États-Unis

M. Michael Mullaney
Directeur de la section antiterroriste
Ministère de la justice

M. Michael Keegan
Directeur adjoint de la section antiterroriste
Ministère de la justice

Fédération de Russie

M. Alexey Yudintsev
Directeur adjoint du Département des menaces et défis naissants
Ministère des affaires étrangères

M. Alexey Dronov
Chef de section, Conseiller principal
Mission permanente de la Fédération de Russie auprès des organisations internationales sises à Vienne

M. Andrey Vasilenko
Deuxième secrétaire
Mission permanente de la Fédération de Russie auprès des organisations internationales sises à Vienne

France

M. Olivier Christen

Vice-procureur
Chef de la Section C1 — Antiterrorisme et atteintes à la sûreté de l'État

M. Guillaume Portenseigne
Vice-Procureur

Inde

Dr Ravi Shankar Ayyanar
National Investigation Agency, Hyderabad

M. Abhijit Hadler
Conseiller
Mission permanente de l'Inde, Vienne

Indonésie

M. Petrus Golose
Directeur des opérations
Agence nationale de lutte contre le terrorisme

M. Aris Munandar
Conseiller
Mission permanente de l'Indonésie, Vienne

Israël

M. Haim Wismonsky
Superviseur national, loi et technologie
Bureau du Procureur israélien

Italie

M. Giorgio Ruggieri
Groupe des opérations spéciales du Corps des Carabinieri
Département des enquêtes techniques

Japon

M. Masao Kuwahara
Commissaire de police
Division de la lutte contre le terrorisme, Département des affaires étrangères et du renseignement
Bureau de la sécurité, Agence de police nationale

M. Satoshi Hanashima
Inspecteur de police
Division de la lutte contre le terrorisme, Département des affaires étrangères et du renseignement
Bureau de la sécurité, Agence de police nationale

M. Masao Sumita
Inspecteur de police adjoint
Division de la lutte contre le terrorisme, Département des affaires étrangères et du renseignement
Bureau de la sécurité, Agence de police nationale

Malaisie

M. Thomas Koruth Samuel
Directeur de la recherche et des publications
Centre régional d'Asie du Sud-Est pour la lutte contre le terrorisme
Ministère des affaires étrangères

Maroc

M. Abderrahim Hanine
Chef du Département des affaires pénales spéciales
Ministère de la justice

Nigéria

M. Akin Akintewe
Directeur adjoint du ministère public
Ministère de la justice

Pakistan

M. Yasir Mahmood
Directeur adjoint
Ministère des affaires étrangères

République de Corée

M. Minwoo Yun
Professeur adjoint
Département de techniques policières, Université Hansei

Roumanie

M. Razvan Avramescu
Service de renseignement roumain

Royaume-Uni

M^me^ Moira Macmillan
Juriste spécialisée dans la lutte contre le terrorisme
Service des poursuites de la Couronne

Conseil de l'Europe

M^me^ Gertraude Kabelka
Représentante de l'Autriche
Conseil de l'Europe, Comité d'experts sur le terrorisme
Direction exécutive du Comité contre le terrorisme

M^me^ Norha Restrepo
Responsable de l'information

Équipe spéciale de lutte contre le terrorisme

M. Kasper Ege
Département des affaires politiques

Eurojust

M^me^ María García Escomel
Groupe de travail chargé de la lutte contre le terrorisme

Organisation pour la sécurité et la coopération en Europe

M. Ben Hiller
Administrateur de programme adjoint
Direction des menaces transnationales/Unité d'action contre le terrorisme de l'OSCE

M. Nemanja Malisevic
Responsable de la cybersécurité
Direction des menaces transnationales, Cellule de coordination

PricewaterhouseCoopers

M. Neal Pollard

University College Dublin

Professeur Joe Carthy
Directeur du Centre de cybersécurité et d'enquête sur la cybercriminalité de l'University College Dublin

Haut-Commissariat aux droits de l'homme

M^me^ Lisa Oldring
Groupe de l'état de droit et de la démocratie

Office des Nations Unies contre la drogue et le crime[205]

M^me^ Marta Requena
Chef du Service de la prévention du terrorisme

M^me^ Gillian Murray
Chef de la Section de l'appui à la Conférence
Service de la criminalité organisée et du trafic illicite

M. Mauro Miedico
Chef du Groupe spécialisé dans la prévention du terrorisme
Service de la prévention du terrorisme

M. Philip Divett
Administrateur de programme, Groupe spécialisé dans la prévention du terrorisme
Service de la prévention du terrorisme

[205] L'Office des Nations Unies contre la drogue et le crime souhaiterait exprimer ses remerciements à ses collaborateurs qui ont contribué à l'élaboration de la présente publication: Tome Lingurovski, Luciana Neagoe, André Peña Torres et Stanislau Tsepliakou.

M. Steven Malby
Spécialiste du contrôle des drogues et de la prévention du crime, Section de l'appui à la Conférence
Service de la criminalité organisée et du trafic illicite

M. Eugene Gallagher
Consultant
Service de la prévention du terrorisme

M^me^ Kerry Dalip
Consultant
Service de la prévention du terrorisme

UNODC

United Nations Office on Drugs and Crime

Vienna International Centre, PO Box 500, 1400 Vienna, Austria
Tel.: (+43-1) 26060-0, Fax: (+43-1) 26060-5866, www.unodc.org

V.12-57353