GCTF
GLOBAL COUNTERTERRORISM FORUM

www.theGCTF.org

Recommandations d'Abuja sur la collecte, l'utilisation et l'échange d'éléments de preuve aux fins des poursuites pénales de terroristes présumés

Introduction

Les Recommandations d'Abuja présentées dans ce document ont été élaborées lors d'une réunion d'experts tenue à La Haye puis d'une réunion d'examen tenue à Abuja, et en prenant en compte des résultats recueillis au moyen de questionnaires et d'entretiens structurés avec des Membres du GCTF et des experts dans ce domaine. À travers ces Recommandations, le GCTF vise à soutenir et à compléter les travaux et les initiatives existantes menées par d'autres organisations internationales et régionales, à savoir les Nations Unies (ONU) et d'autres parties prenantes pertinentes œuvrant dans ce domaine.

Les Recommandations d'Abuja s'inspirent, en les prolongeant, des documents du GCTF suivants : *Mémorandum de Rabat sur les bonnes pratiques pour des actions efficaces de lutte contre le terrorisme dans le secteur de la justice pénale* (Mémorandum de Rabat), *Mémorandum de La Haye sur les bonnes pratiques du système judiciaire pour juger les actes terroristes* et *Recommandations sur l'utilisation et la protection du renseignement lors d'enquêtes et de poursuites menées par le secteur de la justice pénale et fondées sur l'état de droit*.

Leur objectif est de fournir des recommandations aux enquêteurs et procureurs traitant d'affaires de terrorisme afin de les aider à instruire des dossiers solides basés sur des preuves tangibles et admissibles. Les Recommandations d'Abuja s'adressent aux responsables chargés de l'élaboration de politiques, aux agents de détection et de répression et aux procureurs.

La dimension transnationale par essence des réseaux terroristes et des terroristes eux-mêmes va croissant. Les combattants terroristes étrangers franchissent les frontières pour rejoindre des organisations terroristes dans d'autres pays, pour gagner de nouvelles zones de conflit, pour chercher un refuge ou pour retourner dans leur pays de résidence. En outre, les organisations terroristes ont souvent des membres et des cellules dans plusieurs pays et se servent des médias sociaux et de l'internet pour organiser leurs activités et communiquer à leur propos, pour transférer d'un pays à l'autre des ressources financières et autres actifs en soutien de leurs activités ; elles mobilisent également les réseaux du trafic criminel international pour lever des fonds et/ou se procurer des armes, de l'expertise et des explosifs.

La complexité croissante des affaires de terrorisme rend la réussite des poursuites plus difficile et contraignante. En général, le succès des poursuites dans les affaires de terrorisme exige une intense coordination pendant la phase d'instruction pour tout ce qui concerne la collecte de preuves et l'utilisation des outils généraux ou spécifiques disponibles pour mener à bien les investigations.

Les preuves à traiter dans les affaires de terrorisme sont parfois imposantes de par leur volume et peuvent être cryptées, rédigées dans des langues étrangères, classées secrètes ou bien se trouver dans une zone de conflit, ou encore présenter une telle complexité technique qu'il est nécessaire de faire appel à des experts légistes ou à des spécialistes de la technologie considérée. D'autres difficultés identifiées au cours du premier séminaire à l'intention des praticiens organisé par la Direction exécutive du Comité contre le terrorisme (DECT) des Nations Unies (s/2001/240) avec pour thème « Traduire les terroristes en justice », concernent notamment les méthodes d'investigation, la

coopération internationale, la protection des témoins et les liens entre le terrorisme et d'autres formes de criminalité.

Il arrive souvent que la complexité des affaires de terrorisme et les contraintes liées à la collecte de preuves admissibles incitent à déployer plusieurs stratégies en matière de poursuite, par exemple en mettant en examen des terroristes présumés, y compris des combattants terroristes étrangers, pour des crimes pouvant couvrir les actes préparatoires, les crimes terroristes et/ou les crimes internationaux. Dans certaines circonstances, des crimes ordinaires perpétrés dans une situation de conflit armé peuvent être assimilés à des crimes de guerre.

Afin de traduire les terroristes en justice il est important d'exploiter des preuves admissibles dans toute la mesure du possible. Étant donné que les accusations d'actes de terrorisme – par exemple le fait d'apporter un soutien matériel à une organisation terroriste – ne reflètent pas *per se* tous les aspects des crimes perpétrés, les procureurs doivent avoir pour objectif que le jugement des personnes suspectées de terrorisme, y compris les combattants terroristes étrangers, se déroule de manière à exposer intégralement la gravité des faits. C'est ce qui contribue à rendre la justice et à restaurer la dignité des victimes, tout en permettant à ces dernières de tourner la page.

La Résolution 2242 (2015) du Conseil de sécurité des Nations Unies (RCSNU) exhorte les États membres à mener des travaux de recherche axés sur la problématique hommes-femmes et de collecter des données sur les facteurs de radicalisation parmi les femmes et sur les effets des stratégies de lutte contre le terrorisme sur les droits fondamentaux des femmes. Il est important de prendre acte de la diversité des rôles que peuvent jouer respectivement les hommes et les femmes qui prennent part à des activités en lien avec le terrorisme. Les femmes comme les hommes peuvent perpétrer des attentats terroristes. Il est toutefois nécessaire d'adopter un point de vue davantage axé sur la dimension du genre dans l'approche de la justice pénale vis-à-vis du terrorisme, compte tenu de la complexité des situations que les femmes peuvent affronter en tant que victimes, en tant que témoins ou en tant qu'auteurs. Cela suppose par exemple de fournir des orientations sur les problématiques liées au genre pouvant se présenter au cours de l'arrestation, l'interrogatoire, la poursuite, le jugement ou la détention des femmes, ainsi que lors de leur réhabilitation et réinsertion. Comme le rappelle le *Mémorandum de Neuchâtel sur les bonnes pratiques de justice des mineurs dans le contexte de la lutte contre le terrorisme* du GCTF les garçons et les filles impliqués dans les affaires de terrorisme ont des besoins particuliers et doivent bénéficier d'un soutien approprié tout au long de la procédure de justice pénale.

Les Recommandations d'Abuja devront être mises en œuvre en se conformant à la législation nationale en vigueur et au droit international, en particulier le droit international des droits de l'homme, le droit international des réfugiés et le droit international humanitaire.

Recommandations

I. Recommandations en matière de coopération policière et judiciaire

Compte tenu de la nature transnationale et transrégionale de la menace que fait peser le terrorisme, le renforcement de la coopération policière et judiciaire entre les États est une nécessité vitale. Les possibilités de poursuivre avec succès des individus soupçonnés de terrorisme sont compromises lorsque certains actes criminels en lien avec le terrorisme ne sont pas érigés en crimes par le code pénal, lorsqu'il n'y a pas de fondement juridique permettant l'extradition ou l'entraide judiciaire ou encore lorsque les procédures de coopération policière ou judiciaire sont compliquées et excessivement longues. Les États sont encouragés, chaque fois que possible, à améliorer l'efficacité de leur coopération policière et judiciaire, à faire en sorte d'instaurer la confiance parmi les parties prenantes et à s'adapter aux différentes traditions juridiques existantes et aux terminologies

employées. Le respect des obligations dictées par le droit international – y compris le droit international des droits de l'homme et le droit international humanitaire, en particulier le droit à un procès équitable et public – contribuera à la confiance mutuelle et à la coopération entre les États tout en renforçant l'état de droit.

Recommandation 1 : Rationalisation de la coopération policière et judiciaire

Les modalités d'établissement de la juridiction pénale compétente varient d'un pays à l'autre en fonction de la législation nationale, qui dans tous les cas prend en compte les obligations internationales pertinentes auxquelles chaque État particulier doit se conformer. L'application des conventions internationales contre le terrorisme et des résolutions du Conseil de sécurité des Nations Unies contribue à la qualification des actes de terrorisme en crimes dans les législations nationales du monde entier et peut aider à établir le critère de double incrimination afin de faciliter les extraditions, ainsi que le recours à l'entraide judiciaire, si nécessaire. Les conventions internationales de lutte contre le terrorisme intègrent l'injonction *aut dedere aut judicare* (« extrader ou juger »), selon laquelle les États qui n'extradent pas une personne suspectée ont l'obligation de soumettre l'affaire aux autorités compétentes afin que des poursuites puissent être engagées à son encontre.

En fonction du code (de procédure pénale) de chaque pays, la coopération policière et judiciaire peut prendre différentes formes et se traduire par une coopération entre les services de police et entre les services judiciaires des pays participants, y compris entre les procureurs et les juges de ces pays. Cette coopération peut faire suite à la présentation d'une demande officielle ou se dérouler de manière informelle, y compris à travers un échange spontané d'informations. Plusieurs formes de coopération peuvent être envisagées, en particulier les interrogatoires de suspects et de témoins (par vidéoconférence ou par téléphone si la législation nationale le permet, ou en présentiel), le témoignage sous serment (devant le tribunal), la recherche et la saisie de données relatives à la communication, l'interception de communications en temps réel, la transmission de procédures et la continuité de la preuve. Afin de faciliter la coopération entre pays concernant les enquêtes et les poursuites portant sur des crimes en lien avec le terrorisme, il convient que les États dont l'autorité nationale est insuffisante pour engager une telle coopération ratifient les conventions qui apportent un fondement juridique à l'entraide judiciaire, suivant les besoins et s'il y a lieu. Outre la ratification des conventions internationales de lutte contre le terrorisme, les États peuvent également opérer sur une base bilatérale et se constituer parties contractantes de conventions internationales ou régionales d'entraide judiciaire telles que la Convention des Nations Unies contre la criminalité transnationale organisée, ou, à l'échelle régionale, la Convention européenne d'entraide judiciaire en matière pénale, le Mécanisme d'entraide judiciaire en matière pénale au sein du Commonwealth, la Convention de la CEDEAO relative à l'entraide en matière pénale, ou le Traité d'entraide judiciaire en matière pénale de l'ASEAN. Lorsque la législation nationale n'autorise pas explicitement l'entraide judiciaire en matière pénale ou en l'absence d'accords en la matière, les pays sont encouragés à s'apporter mutuellement toute l'assistance envisageable et juridiquement fondée, en se basant notamment sur le principe de réciprocité dès lors que celui-ci s'applique. Les organismes de coopération judiciaire tels qu'Eurojust peuvent être saisis afin de faciliter la coopération et de coordonner le déroulement des enquêtes et des poursuites dans les affaires de terrorisme transfrontalier.

Il est donc recommandé aux États de qualifier en crimes les actes de terrorisme en appliquant les conventions internationales de lutte contre le terrorisme, de ratifier les accords d'entraide judiciaire existants et de les transposer dans la législation nationale afin de faciliter la coopération policière et judiciaire chaque fois que possible, ou bien, le cas échéant, de conclure des accords bilatéraux. Les divers projets de traités types rédigés jusqu'à présent peuvent être instructifs à cet égard. Le Traité type d'entraide judiciaire en matière pénale des Nations Unies en est un exemple.

Recommandation 2 : Renforcer les autorités centrales aux fins de l'entraide judiciaire

Les autorités centrales désignées aux fins de l'entraide judiciaire remplissent une fonction importante car elles permettent d'accélérer les demandes d'entraide judiciaire par le simple fait d'intervenir en tant que point focal auprès des autorités étrangères à qui est adressée la demande. Les autorités centrales ont la possibilité de constituer un réseau mondial, avec l'aide de l'Office des Nations Unies contre la drogue et le crime (ONUDC). En outre, elles peuvent transmettre les demandes d'entraide judiciaire aux autorités compétentes et aider l'autorité requérante à rédiger sa demande conformément aux critères d'application.

Aux fins de l'entraide judiciaire, les États sont donc encouragés à désigner l'autorité centrale compétente, qui devra être dotée de personnels qualifiés et en effectifs suffisants et aura pour tâche de faciliter la coopération et la communication efficaces entre les agents de détection et de répression, les juges d'instruction et les procureurs de différents pays.

Recommandation 3 : Améliorer l'efficacité de la coopération et de l'échange d'informations officiels

Tous les acteurs intervenant dans le secteur de la justice pénale n'ont pas nécessairement connaissance des procédures d'entraide judiciaire qui régissent la coopération internationale en matière pénale. Il est donc recommandé de sensibiliser l'ensemble des acteurs du secteur sur cette question et de leur proposer des formations en vue de les aider à maîtriser ce type de procédures. Ces formations devront également faire ressortir les différences à prendre en compte entre systèmes juridiques.

Enfin, elles devront aborder également la question du partage d'informations avec les organisations internationales et régionales de coopération policière telles qu'Interpol, qui ont élaboré des bases de données dans leur domaine, ainsi qu'avec les organisations de coopération judiciaire. En outre, les agents de détection et de répressions et les procureurs doivent avoir une connaissance encore plus précise des exigences dictées par les droits de l'homme quant à l'utilisation de ces bases de données, en particulier l'obligation inscrite dans le droit international de s'abstenir de porter atteinte arbitrairement ou illégalement à la vie privée des personnes.

Il est donc recommandé aux pays de s'investir dans la sensibilisation et la formation concernant les avantages apportés par l'entraide judiciaire, les procédures d'échange d'informations, l'utilisation des informations accessibles à travers les instruments et bases de données pertinentes créés par les organisations internationales et régionales de coopération policière et judiciaire, y compris pour ce qui concerne les exigences découlant du droit international des droits de l'homme et les particularités des différents systèmes juridiques.

D'autre part, afin d'accélérer l'entraide judiciaire, il est recommandé aux pays d'uniformiser autant que possible les protocoles de demande d'entraide judiciaire, en particulier au sein d'une même région. Cela peut passer par l'élaboration de demandes-types pour les requêtes d'assistance judiciaire. Le recours à des formulaires électroniques pour transmettre les demandes pourrait accélérer encore plus la procédure au niveau des autorités centrales ou d'autres autorités de la justice pénale. Quelques exemples fructueux de modèles standardisés ont été élaborés par l'Union européenne et le Conseil de l'Europe, notamment. En outre, des programmes de renforcement des compétences mis en œuvre entre autres par l'ONUDC proposent également plusieurs modules couvrant différentes tâches communes aux systèmes du droit civil et du *Common Law*.

Il est recommandé aux autorités soumettant une demande d'entraide judiciaire de consulter leurs homologues dans le pays destinataire de la demande, notamment en leur présentant un premier

projet de cette demande avant l'envoi de la version officielle, de centrer la demande sur les éléments nécessaires au traitement du dossier, d'utiliser un langage simple et direct et de rédiger la demande dans la langue de l'État requis. Il est essentiel que les demandes d'entraide judiciaire ne portent que sur les points strictement nécessaires afin que l'entraide puisse être diligentée le plus rapidement possible.

Enfin, pour que les mesures juridiques puissent lutter efficacement contre le terrorisme, les pays sont encouragés à contribuer aux systèmes d'échange d'informations et à s'apporter le plus possible un soutien mutuel sous forme d'entraide judiciaire lors des enquêtes et des poursuites.

Recommandation 4 : Instaurer la confiance et s'investir dans des réseaux (informels)

L'information traitée durant les enquêtes et les poursuites judiciaires visant des individus suspectés de terrorisme comporte parfois des informations sensibles, éventuellement en lien avec la sécurité nationale du pays. Les enquêtes visant les personnes suspectées de terrorisme et les poursuites de ces suspects doivent être conduites dans un cadre respectueux de l'état de droit et en conformité avec le droit international, y compris le droit international des droits de l'homme et le droit international humanitaire, en particulier le droit à un procès équitable. Les informations effectivement partagées doivent toutefois être soumises aux exigences juridiques liées à la continuité de la preuve, et les sources ayant permis de les obtenir doivent faire l'objet d'une protection appropriée. Ces impératifs s'appliquent également aux informations et aux preuves obtenues dans le cadre de l'entraide judiciaire. Compte tenu du nombre accru d'affaires en lien avec le terrorisme qui comportent une dimension transfrontalière ou transrégionale, l'échange d'informations et la coopération avec les acteurs de la justice pénale d'autres pays sont devenus des aspects déterminants d'une réponse efficace de la justice pénale. À la lumière de ces défis, il est donc recommandé aux États de s'investir dans l'instauration d'un climat de confiance avec les acteurs de la justice pénale d'autres pays.

Le premier aspect d'une confiance instaurée est que chacun s'efforce de se familiariser avec ses homologues directs dans l'autre pays. La mise en place de réseaux (informels) par les autorités policières ou les procureurs peut se révéler utile. Des réseaux régionaux sont déjà opérationnels, par exemple le Réseau judiciaire européen. Les réseaux informels parviennent souvent à de fructueux échanges d'informations et d'expériences. En particulier, lors des échanges préparatoires avec un homologue direct avant la soumission d'une demande officielle d'entraide judiciaire, il sera utile de présenter une demande préalable non officielle afin d'identifier précisément le destinataire de la demande et d'examiner les exigences à remplir, ou simplement pour annoncer que la demande est en voie d'être présentée, afin d'accélérer la procédure. Le partage informel d'informations peut également être déterminant lors des phases préliminaires de l'instruction, ainsi que pour définir le motif valable requis dans certains cadres juridiques pour délivrer un mandat d'arrêt, même si ces informations ne sont pas nécessairement utilisées en tant que preuves lors du procès à un stade ultérieur de la procédure. Il est donc recommandé aux pays d'adopter une attitude proactive au regard du partage d'informations et de la mobilisation des réseaux (informels). L'Association internationale des procureurs a élaboré une série de bonnes pratiques en la matière. Il est toutefois important de signaler que le recours à des réseaux informels ne saurait en aucun cas se substituer à la demande officielle ni aux garanties juridiques liées à la continuité de la preuve et au respect du droit à un procès équitable, qui font tous partie du déroulement officiel de la procédure. Des séminaires peuvent être organisés dans le cadre de ces réseaux pour une mise en commun des expériences acquises, des difficultés rencontrées et des bonnes pratiques mises en œuvre.

Une autre possibilité pour accélérer les procédures d'entraide judiciaire ou plus généralement la coopération policière et judiciaire bilatérale ou multilatérale consiste à désigner des agents de liaison

nationaux affectés en poste dans un autre pays ou au sein d'une organisation internationale de coopération policière ou judiciaire.

Recommandation 5 : Promouvoir une coordination efficace des enquêtes judiciaires

Étant donné que les terroristes se déplacent et opèrent au sein d'organisations et de réseaux terroristes, les enquêtes sur les actes en lien avec le terrorisme qu'ils sont soupçonnés d'avoir perpétrés ne peuvent généralement pas être conduites dans les limites de la juridiction d'un seul État. Un attentat terroriste peut avoir été préparé dans un pays déterminé, tandis que les explosifs et les armes sont obtenus par contrebande à partir d'un deuxième pays, que les instructions proviennent d'un troisième pays et enfin que l'attentat lui-même est perpétré dans un quatrième pays. Au minimum, il faudra que les agents de détection et de répression et les enquêteurs judiciaires se mettent en relation avec leurs homologues des autres pays et/ou sollicitent leur aide, et qu'ils fassent une demande d'assistance accélérée sur la base d'une entraide informelle directe entre autorités policières aux fins d'enquêtes sur des actes criminels perpétrés sur leur territoire. Cette coopération peut ensuite déboucher sur une demande d'entraide judiciaire dès lors que les preuves réunies sont susceptibles d'être utilisées pour les poursuites de crimes en lien avec le terrorisme.

Par ailleurs, les organisations internationales ou régionales de coopération policière et judiciaire telles qu'Interpol, Europol et Eurojust ont institué des mécanismes d'enquête en temps réel lorsque des composantes transfrontalières ou transrégionales sont en jeu. Cela permet en particulier d'accélérer l'échange d'informations et de faciliter l'élucidation des connexions entre différents points au sein des réseaux d'organisations terroristes, souvent fort complexes.

Dans certaines situations, une autre bonne pratique consiste à mettre en place une modalité encore plus étroite de coopération en instituant des équipes communes d'enquête, dotées d'un objectif spécifique avec une échéance prédéfinie à des fins d'enquête judiciaire dans un ou plusieurs pays participants. Les équipes communes d'enquête sont constituées de membres des autorités compétentes nationales des pays participant à des enquêtes transfrontalières complexes exigeant une coordination d'activités. Le Réseau d'équipes communes d'enquête a élaboré avec la collaboration d'Eurojust, d'Europol et de l'Office européen de lutte contre la fraude (OLAF) un Guide pratique destiné à fournir aux praticiens des informations, des orientations et des conseils concernant la mise en place et le fonctionnement d'une équipe commune d'enquête. Des guides similaires ont été élaborés par d'autres pays. Le Modèle d'accord pour la création d'une équipe commune d'enquête (disponible dans toutes les langues de l'UE) constitue une référence commune non contraignante que les praticiens peuvent adapter aux nécessités de l'affaire qui les intéresse. Néanmoins, les règles régissant respectivement la communication et l'admissibilité des éléments de preuve n'étant pas toujours identiques d'un pays à l'autre, il conviendra que l'accord de création d'une équipe commune d'enquête précise clairement les modalités à mettre en œuvre en la matière.

Il est donc recommandé aux États de s'apporter mutuellement toute l'assistance nécessaire dans le respect du droit national et international, lors des enquêtes visant des crimes en lien avec le terrorisme comportant une dimension transfrontalière ou transrégionale, et de mettre également en place un mécanisme de coordination entre leurs propres agences nationales d'enquêtes judiciaires et celles des autres pays au cours de ces investigations. Il est également conseillé aux pays de recourir aux organisations de coordination existantes dans le cadre des mécanismes internationaux ou régionaux de coopération policière et judiciaire lorsqu'ils ont à traiter d'enquêtes complexes concernant des crimes en lien avec le terrorisme. Enfin, les pays peuvent envisager de convoquer des équipes communes d'enquête pour les enquêtes judiciaires extrêmement complexes et qui concernent au moins deux pays, ce qui exige une coordination rapprochée du processus d'investigation.

II. Recommandations relatives à la collecte, à l'utilisation et à la communication de preuves médico-légales et criminalistiques

Les preuves médico-légales et criminalistiques (c'est-à-dire les éléments de preuve obtenus par les méthodes criminalistiques modernes reconnues scientifiquement, en conformité avec le droit national et international, y compris le droit international des droits de l'homme) constituent souvent des outils précieux pour les enquêtes et les poursuites visant des crimes en lien avec le terrorisme, comme le précise la bonne pratique 10 du *Mémorandum de Rabat.*

La criminalistique peut contribuer à prouver la commission d'un crime (établissement de la réalité du fait), à identifier les victimes et les auteurs d'un crime (établissement de la source) ou à décrire la manière dont un crime a été perpétré (établissement du mode opératoire). La criminalistique peut être utilisée pour les besoins des enquêtes et des poursuites visant des actes en lien avec le terrorisme ainsi que pour prévenir des crimes terroristes.

Les données criminalistiques peuvent être obtenues sur les lieux du crime, immédiatement après un attentat terroriste et/ou sur le champ de bataille ou dans d'autres sites susceptibles de contenir des indices. Les types de preuves recueillies vont des empreintes digitales aux engins explosifs improvisés (EEI) non explosés, en passant par les composantes chimiques de bombes ou les données numériques extraites d'ordinateurs, de téléphones portables, de clés USB ou de caméras numériques. Les données criminalistiques peuvent être consignées et analysées sur la scène même du crime – lorsqu'on dispose d'un laboratoire mobile – ou expédiées à un laboratoire pour analyse.

La criminalistique est une discipline scientifique qui recouvre plusieurs méthodologies, dont l'analyse balistique et l'examen des armes à feu, l'expertise textile, la chimie criminalistique et les technologies biométriques. En particulier, l'analyse biométrique, qui fait appel à l'identification semi-automatisée des personnes basée sur des caractéristiques morphologiques spécifiques révélées par reconnaissance faciale, relevé d'empreintes digitales, examen de l'iris, reconnaissance vocale, analyse de l'ADN ou analyse dentaire, est largement utilisée. Les techniques criminalistiques connaissent actuellement des avancées très rapides, notamment pour ce qui concerne la biométrique et l'analyse de l'ADN. Les pays qui en ont les moyens techniques et financiers pourraient investir dans la recherche criminalistique, mettre au point des techniques plus sophistiquées et fiables au service des enquêtes visant les crimes en lien avec le terrorisme et contribuer à renforcer les capacités criminalistiques d'autres pays.

La collecte, l'analyse, l'archivage et l'échange de données criminalistiques peuvent avoir une incidence en matière de protection de la vie privée mais peuvent aussi affecter le droit à un procès équitable. La protection de la vie privée n'est pas un droit absolu, mais constitue néanmoins un droit de l'homme reconnu dans l'article 17 du Pacte international relatif aux droits civils et politiques (PIDCP).

Aux termes de la RCSNU 2396 (2017), les États Membres doivent élaborer et mettre en œuvre des systèmes de collecte de données biométriques pour identifier de manière responsable les terroristes, y compris les combattants terroristes étrangers, dans le respect du droit interne et du droit international des droits de l'homme. Il convient de tenir compte de ces contraintes juridiques, y compris le respect du droit à la protection de la vie privée, afin d'amplifier l'utilisation de la criminalistique dans les affaires en lien avec le terrorisme. Les pays doivent investir dans le renforcement de leurs capacités criminalistiques, ce qui recouvre la recherche scientifique, la technologie, les équipements, l'expertise et la formation et nécessite également que des efforts soient consacrés à s'assurer que le système en place est à même de s'adapter aux nouvelles évolutions scientifiques, notamment le renseignement criminalistique. Grâce à la création de nouvelles applications, à l'adoption de normes acceptées au plan international ou fondées sur la science pour

l'archivage, l'analyse et l'échange des données criminalistiques, et au renforcement de la coopération en matière de preuves médico-légales entre les différentes parties prenantes, la science criminalistique peut jouer un rôle vital dans la prévention et la lutte contre le terrorisme.

Recommandation 6 : Promouvoir l'application de normes internationalement reconnues ou fondées sur la science en matière d'extraction, d'analyse et de consignation des données criminalistiques

L'un des aspects des enquêtes menées sur les lieux d'un crime porte sur l'extraction des données criminalistiques pertinentes afin que celles-ci puissent être traitées et analysées par un laboratoire (mobile ou non). Si les méthodes de collecte, d'analyse et de stockage des données sont conformes aux normes adoptées au plan international ou fondées sur la science et qu'elles sont bien documentées, les données criminalistiques peuvent apporter des informations essentielles susceptibles d'être présentées comme preuves devant un tribunal. S'il s'agit de crimes sexuels à visée terroriste, la collecte de données criminalistiques doit de surcroît se faire selon des méthodes respectueuses de la dimension du genre. La généralisation de l'utilisation et de l'échange de données criminalistiques renforce la nécessité d'élaborer des normes nationales et internationales et de s'y conformer. Ces normes concernent notamment l'accréditation des laboratoires de police scientifique, les méthodes d'analyse des données criminalistiques normalisées et fondées sur la science dans les différentes disciplines criminalistiques et la certification des experts légistes et judiciaires. Cela contribuera à une utilisation plus équitable, plus efficace et plus fiable des preuves médico-légales dans les affaires en lien avec le terrorisme.

Les laboratoires médico-légaux peuvent être institués en tant qu'organismes publics indépendants, en tant que structures privées ou en tant qu'entités liées à une organisation d'application de la loi. L'accréditation permet d'établir la fiabilité des laboratoires d'analyses médico-légales en garantissant que leurs activités sont menées conformément aux normes en vigueur. Concernant l'accréditation des laboratoires médico-légaux, la norme révisée ISO/IEC 17025 : 2017 Exigences générales concernant la compétence des laboratoires d'étalonnages et d'essais fournit des orientations précieuses pour mettre en œuvre un système qualité basé sur une méthodologie scientifique. En outre, l'International Laboratory Accreditation Cooperation (ILAC) a publié un guide (ILAC G-19:08/2014 on Modules in a Forensic Science Process) fournissant des orientations plus détaillées sur les procédures d'expertise médico-légale depuis la scène du crime jusqu'au tribunal. Il est donc recommandé aux pays de procéder à l'accréditation de leurs laboratoires d'analyses médico-légales conformément aux normes adoptées au plan international ou basées sur la science. En outre, il est conseillé aux pays de veiller à l'assurance qualité de ces laboratoires en organisant à intervalles réguliers des tests comparatifs inter-laboratoires. Les États devraient en même temps se tenir prêts à s'adapter aux innovations technologiques susceptibles de faire avancer telle ou telle technique d'enquête particulière.

Nombre d'organisations nationales et internationales ont élaboré des normes validées scientifiquement pour toute une gamme de techniques criminalistiques dont l'analyse des empreintes digitales, l'expertise balistique, les preuves numériques et les prélèvements d'ADN. À l'échelle régionale, en particulier au sein de l'UE, des efforts sont déployés pour s'assurer que la collecte, l'analyse et l'utilisation des données criminalistiques sont conformes aux normes minimales en matière criminalistique. Il est donc recommandé aux pays d'élaborer des normes nationales en s'alignant sur les normes internationales et régionales, ce qui pourrait contribuer à la solidité des preuves médico-légales présentées devant les tribunaux tout en renforçant la confiance du public dans la science criminalistique.

Enfin, les pays pourraient veiller à la mise en place d'un système de certification approprié des experts légistes afin de garantir la fiabilité et les compétences des personnes chargées d'analyser les données criminalistiques.

Recommandation 7 : La collecte et le stockage des données criminalistiques

Les données criminalistiques peuvent jouer un rôle vital dans la prévention des crimes en lien avec le terrorisme, ainsi que dans les enquêtes et les poursuites relatives à ces crimes. Les technologies d'analyse de l'ADN se sont considérablement perfectionnées, certains pays s'étant dotés d'un fichier national d'empreintes génétiques. D'autres pays procèdent actuellement à la création de bases de données nationale pour les besoins de l'identification des personnes, du suivi sanitaire, des contrôles d'immigration ou des enquêtes pénales. Plusieurs types de fichiers ADN peuvent être créés par les pays pour y recourir dans leurs enquêtes pénales : enregistrement du profil génétique des individus condamnés, recherche de personnes disparues, ou base de données ADN « intervenants » à des fins d'exclusion (personnels de laboratoire et agents de détection et de répression en contact avec des données criminalistiques dans le cadre de leur travail). La décision d'un pays d'établir une base de données centralisée ou décentralisée peut influer sur l'interopérabilité et la sécurité des fichiers. Bien que plus vulnérables, les bases de données centralisées sont plus avantageuses en termes d'interopérabilité, tandis que les bases de données décentralisées ne facilitent pas toujours le partage de données compatibles avec d'autres bases de données mais ont un niveau de sécurité plus élevé. Les pays ou les organisations internationales telles qu'Interpol qui ont une expérience dans la création et l'entretien d'une base de données ADN aux fins des enquêtes pénales sont encouragés à partager leurs expériences avec d'autres pays.

Les pays devraient veiller à ce que les bases de données permettent de distinguer, parmi les données biométriques, celles qui sont rattachées à des acteurs représentant une menace avérée ou suspectée (auteurs d'actes criminels ou terroristes).

En outre, la collecte et le stockage de données biométriques peuvent constituer une atteinte au droit à la vie privée. Afin de protéger les données personnelles, les pays devront s'assurer que leurs bases de données offrent les garanties requises de robustesse et de sécurité. Pour éviter qu'une collecte et conservation incorrectes des données biométriques n'empiètent trop sur le droit à la vie privée, il est recommandé aux pays de procéder à la collecte et la conservation de données biométriques dans des buts spécifiques, transparents et légitimes. Les pays doivent formuler sous quelles conditions juridiques peuvent être prélevés des échantillons d'ADN sans le consentement de l'intéressé et définir les procédures permettant de prélever ces échantillons (par exemple sous présentation d'un mandat), la période de conservation des données, les modalités d'accès aux données biométriques et les voies de recours pour un accusé ainsi que les modalités d'effacement d'une empreinte génétique du fichier national. Il est donc recommandé aux pays d'adopter des garde-fous appropriés. La Résolution 45/95 de l'Assemblée générale des Nations Unies, Principes directeurs pour la réglementation des fichiers personnels informatisés (1990) contient de précieuses directives et orientations qui pourraient s'appliquer à la conservation des données biométriques.

Afin de protéger les droits des mineurs, il est conseillé aux pays d'instaurer des dispositions spécifiques relatives à la collecte, l'exploitation et la conservation des données criminalistiques portant sur des mineurs. Ces mesures peuvent inclure l'obtention du consentement des parents, la limitation de la durée de conservation des données biométriques ou la suppression définitive des données lorsqu'il s'agit de délits mineurs. En outre, afin de garantir le respect des obligations internationales en vigueur en matière de droits de l'homme, il est recommandé aux pays d'envisager d'introduire des mécanismes de contrôle adéquats.

Recommandation 8 : Échange des données criminalistiques et des preuves médico-légales : l'importance d'une coopération à l'échelle nationale et internationale

La coopération internationale des parties prenantes en matière de données criminalistiques peut prendre plusieurs formes. Il est impératif que les acteurs de la justice pénale connaissent davantage et apprécient la portée de la science criminalistique et de sa contribution aux poursuites visant les crimes en lien avec le terrorisme. Une coopération rapprochée à l'échelle nationale entre les laboratoires d'analyses médico-légales et les acteurs de la justice pénale doit être encouragée à travers la mise en place d'une plateforme permettant d'échanger les points de vue. Il est recommandé aux pays d'améliorer les connaissances des acteurs de la justice pénale en matière criminalistique (y compris concernant les limites et le potentiel inhérents à cette discipline), mais aussi d'affiner parmi les intervenants de la communauté médico-légale la perception de la valeur probante s'attachant aux données criminalistiques.

En mettant en place une coopération entre les laboratoires d'analyses médico-légales de différents pays, ces derniers peuvent s'apporter un soutien mutuel lors de la collecte ou l'analyse de données criminalistiques immédiatement après un attentat terroriste, mais aussi organiser des formations et partager leurs méthodologies afin de renforcer leurs capacités criminalistiques. Les pays pourraient envisager la bonne pratique consistant à réaliser à titre gracieux des analyses criminalistiques pour le compte de pays dépourvus de capacités dans le domaine médico-légal. Compte tenu des disparités des capacités technologiques et financières suivant les pays, il est recommandé à ces derniers de promouvoir la participation de leurs instituts de police scientifique aux réseaux internationaux et régionaux d'instituts homologues afin d'accroître les échanges d'expertise criminalistique, de renforcer leurs capacités techniques respectives et d'élaborer des normes communes.

Les agents de détection et de répression et les procureurs de différents pays peuvent partager leurs points de vue et expertise médico-légale dans le cadre de l'entraide judiciaire ou bien, dans certaines circonstances, d'une coopération entre services de police, afin de soutenir les enquêtes et les poursuites visant des crimes terroristes dans le respect des obligations relatives aux droits de l'homme. Un certain nombre de difficultés inhérentes à l'échange d'informations s'appliquent également à l'échange des données criminalistiques et à la communication des preuves médico-légales. Les agents de détection et de répression et les procureurs doivent avoir conscience des normes particulières d'admissibilité des preuves médico-légales s'appliquant dans chaque pays.

Enfin, une autre modalité de coopération criminalistique internationale est la communication à d'autres pays ou à des organisations internationales ou régionales de données criminalistiques extraites des bases de données nationales. La Convention de Prüm, par exemple, permet aux États membres de l'Union européenne de consulter et de comparer les profils ADN de leurs bases de données respectives de manière automatisée. En outre, il est recommandé aux pays de partager les profils génétiques de leurs bases de données avec le fichier ADN d'Interpol, dans le respect de leur législation nationale. Cette base de données applique des normes internationales conformes aux dispositions de la Convention de Prüm. Les pays qui partagent avec Interpol des profils génétiques conservent la propriété des fiches ADN qu'ils transmettent et déterminent le type d'information qu'ils acceptent de partager, ainsi que les pays avec lesquels ils partagent cette information. En outre, Interpol a mis en place un bureau de la protection des données destiné à garantir la protection des données, la transparence et la responsabilisation afin de faciliter et de consolider la confiance des pays à l'égard de l'échange de données criminalistiques avec Interpol.

Recommandation 9 : Consolider l'exploitation des preuves médico-légales devant les tribunaux

L'évaluation et l'interprétation des constatations criminalistiques constituent ce qu'on appelle l'expertise médico-légale, destinée à fournir des éléments susceptibles d'être présentés en tant que preuves médico-légales devant les tribunaux. Afin de pouvoir exploiter les preuves médico-légales devant les tribunaux, il est crucial de consigner avec soin les méthodes d'obtention des données criminalistiques, le moment de leur collecte, les méthodes utilisées pour leur extraction et analyse et le nombre de personnes ayant participé à leur traitement. Les procureurs doivent s'assurer de l'authenticité et de l'intégrité des preuves médico-légales. Il est donc recommandé aux agents de police et aux procureurs de consigner avec soin la manière dont les données criminalistiques ont été obtenues et analysées afin de faciliter leur utilisation en tant que preuves devant les tribunaux.

En outre, les preuves médico-légales doivent être présentées devant les tribunaux par des experts légistes qualifiés. Afin de s'assurer que les constatations criminalistiques sont interprétées et évaluées de manière systématique et professionnelle, le Comité technique ISO/TC 272 sur la criminalistique travaille actuellement à l'élaboration d'une norme portant sur la détection et le prélèvement des preuves médico-légales, l'analyse et l'interprétation subséquentes de ces preuves, ainsi que la communication des résultats et conclusions, qui devrait permettre d'améliorer les normes et les procédures en la matière. Il est recommandé aux pays d'investir dans la formation et le recrutement d'experts légistes qualifiés, d'établir une liste d'experts légistes certifiés, d'utiliser une terminologie normalisée et d'élaborer des rapports-types relatifs à l'interprétation et à la communication des constatations criminalistiques à des fins d'enquêtes et de poursuites.

Afin de garantir un procès équitable et le respect de principe de l'égalité des armes, les avocats de la défense doivent pouvoir contester la validité des preuves criminalistiques présentées à charge. Cela signifie que les preuves médico-légales doivent pouvoir être consultées par la défense – pour autant que l'enquête le permette – suffisamment tôt pour que l'avocat puisse examiner les données criminalistiques ou les soumettre à un expert légiste en vue d'une contre-expertise des données ou d'une interprétation contradictoire des constatations criminalistiques. Compte tenu des coûts induits par l'examen des preuves médico-légales, il est recommandé aux pays de faire en sorte que la défense puisse recourir à la criminalistique en intégrant l'accès à cette expertise dans les dispositifs d'aide juridique.

III. Recommandations relative à la collecte, à l'utilisation et à la communication des preuves numériques

Si les progrès des technologies de l'information et de la communication apportent de nombreux avantages, les terroristes et les organisations terroristes utilisent également l'internet à des fins de terrorisme, en particulier pour le recrutement, le financement, la formation, la planification et la commission d'attentats terroristes, attaques cybernétiques incluses. La forte dépendance des terroristes à l'égard de l'internet signifie également qu'ils laissent des traces numériques, ce qui ouvre des perspectives en termes d'enquêtes judiciaires et de poursuites. L'utilisation croissante des preuves numériques dans les affaires en lien avec le terrorisme s'accompagne néanmoins de difficultés nouvelles, qu'il convient de traiter.

Les informations obtenues à partir de l'internet peuvent être classées en trois catégories : renseignements de base sur les abonnés, données liées au trafic et données liées aux contenus, chacune de ces informations pouvant constituer une preuve électronique. Il existe plusieurs méthodes permettant aux agents de détection et de répression et aux procureurs d'obtenir ces informations afin de les saisir en tant que preuves électroniques. Il convient de distinguer la « sécurisation des

données » de la « conservation des données ». La sécurisation des données désigne le fait de garder sur une durée longue des données qui sont déjà archivées d'une manière ou d'une autre, en les protégeant de tout risque de détérioration de leur qualité ou d'altération de leur support matériel. La sécurisation des données désigne l'activité consistant à garder sous une forme sécurisée et protégée des données préalablement archivées, tandis que la conservation des données désigne le processus d'archivage lui-même. La conservation des données fait référence à la période durant laquelle sont stockées les données relatives au trafic, à la localisation et aux informations de base d'un abonné. Les agents de détection et de répression et les procureurs peuvent demander d'accéder non seulement aux informations stockées, mais aussi à des informations en temps réel, qui peuvent porter aussi bien sur le trafic que sur le contenu.

Les preuves électroniques sont instables, facilement modifiées, endommagées ou détruites, elles ne résistent pas au temps et ne sont pas liées à une juridiction territoriale. L'évolution rapide des technologies de la communication, le recours à la technologie du chiffrement, aux méthodes d'anonymisation et à l'informatique en nuage imposent aux pays d'adapter leurs capacités en conséquence. Les outils d'investigation classiques peuvent se révéler inadéquats pour la collecte et l'obtention de preuves électroniques, qui exigent des outils plus spécifiquement « cybernétiques », comme cela a été souligné dans la bonne pratique 4 du *Mémorandum de Rabat*.

La coopération avec les fournisseurs de services est cruciale pour conserver et obtenir les preuves électroniques. Le fait que les données soient mobiles en permanence et puissent être stockées dans des juridictions multiples ou étrangères constitue un problème pour les agents de détection et de répression et les procureurs qui envisagent de présenter une demande d'entraide judiciaire et doivent donc savoir à quel pays adresser leur demande. La collecte de preuves électroniques et les règles afférentes à la conservation des données peuvent avoir des conséquences sur le droit à la vie privée et sur d'autres droits de l'homme. Conformément à l'alinéa 2 de la RCSNU 1373 (2001), réaffirmé par les RCSNU 2178 (2014), 2322 (2016) et 2396 (2017), les pays sont tenus de s'apporter mutuellement toute l'assistance possible lors des poursuites à l'encontre d'auteurs présumés d'actes terroristes.

Recommandation 10 : Améliorer l'utilisation tant des outils classiques que de ceux spécifiquement cybernétiques afin d'obtenir des preuves électroniques

L'exploitation des preuves électroniques est un aspect qui prend une importance grandissante dans les poursuites à l'encontre des terroristes présumés. Les agents de détection et de répression peuvent recourir à des techniques d'instruction classiques ou spécialisées afin d'obtenir des preuves électroniques, ou faire appel à des outils de nature plus spécifiquement cybernétique.

S'il y a lieu, il est recommandé aux agents de détection et de répression et aux procureurs de tenter d'obtenir le consentement de l'utilisateur ou d'un de ses proches parents à la collecte des données le concernant. Le terme d'utilisateur est défini par les fournisseurs de service et se réfère généralement à la personne ayant créé un compte ; il est parfois utilisé de manière interchangeable avec celui d'abonné, qui désigne la personne qui s'est inscrite afin d'avoir accès à un service en ligne. Cela peut présenter une certaine utilité lorsqu'une technique cryptographique a été mise en œuvre. D'autres outils tels que les enquêtes en sources ouvertes – terme désignant les données accessibles au public – peuvent contribuer à localiser un utilisateur ou un fournisseur de services ou à déterminer si une activité criminelle a été effectivement perpétrée. Les agents de détection et de répression peuvent recourir aux outils en sources ouvertes pour obtenir des données électroniques pertinentes. Il convient d'envisager une définition étroite des « sources ouvertes » afin de se prémunir contre toute atteinte aux droits de l'homme, en particulier le droit à la liberté d'expression. En outre, il est recommandé aux agents de détection et de répression et aux procureurs de consigner les sources des

informations recueillies afin de s'assurer que celles-ci puissent être ensuite utilisées en tant que preuves devant un tribunal.

Dans les situations où les autorités en charge de l'instruction ne disposent manifestement pas des capacités nécessaires pour obtenir des preuves numériques relatives à des crimes en lien avec le terrorisme, il est recommandé aux pays d'envisager l'introduction d'une législation portant spécifiquement sur le domaine cybernétique, notamment pour garantir la sécurisation des données informatiques et/ou pour ratifier des conventions multilatérales ou régionales cyber-spécifiques. En outre, il est recommandé aux pays d'investir dans le renforcement des capacités des agents de détection et de répression en organisant des formations et en encourageant l'utilisation de manuels de bonnes pratiques en matière d'obtention des preuves électroniques, tels que les guides de l'ONUDC ou du Conseil de l'Europe.

Les pays devraient déterminer si la législation en vigueur prend en compte les nouvelles technologies et si elle contient des dispositions relatives à la conservation et à l'obtention de preuves électroniques, par exemple l'obligation pour les fournisseurs d'accès à l'internet de conserver certaines informations ou de permettre aux agents de détection et de répression d'accéder aux données en temps réel ou de procéder à des fouilles dans les disques durs d'ordinateurs.

Recommandation 11 : Localisation et sécurisation des preuves électroniques

Les terroristes et les réseaux terroristes ont souvent recours à des logiciels et à d'autres techniques permettant de dissimuler tant leur identité que leur localisation et de stocker leurs propres informations. Une fois les données localisées ou le fournisseur d'accès hébergeant ces données identifié, les agents de détection et de répression ou les procureurs devraient tenter de sécuriser ces données le plus rapidement possible afin de contrer toute tentative de modification ou de suppression de celles-ci. Suivant les juridictions, les agents de détection et de répression ou les procureurs peuvent adresser une injonction de sécurisation des données directement au fournisseur d'accès à Internet, faire appel à la coopération informelle (par exemple la coopération entre services de police) ou adresser une demande d'entraide judiciaire visant la sécurisation des données en cause. Lorsque cela est possible, les demandes de sécurisation des données seront présentées par les agents de détection et de répression et par les procureurs via les réseaux de veille permanente.

L'informatique en nuage rend la localisation des sites de stockage des données de plus en plus difficile, les données étant parfois stockées dans des juridictions étrangères, ou bien en des lieux multiples ou inconnus ce qui se traduit par une « perte de localisation ». En outre, l'informatique en nuage pose des problèmes particuliers concernant la législation applicable et la juridiction compétente. Les critères appliqués par les pays pour déterminer la compétence d'une juridiction varient suivant les objectifs visés. En effet, les facteurs de rattachement utilisés pour déterminer la juridiction compétente et la législation applicable dépendent du motif pour lequel les données sont recherchées, à savoir la protection des données, la fiscalité, la propriété intellectuelle ou l'engagement de poursuites. Il est recommandé aux pays d'étudier la question de savoir s'il leur faut adopter des mesures législatives afin d'empêcher la perte de données et de garantir l'exploitation de ces dernières à des fins d'enquêtes et de poursuites dans les affaires en lien avec le terrorisme.

Recommandation 12 : Encourager une coopération effective avec les fournisseurs de services

Un fournisseur de services a pour tâche de transférer des informations par voie électronique ; le terme désigne aussi bien les entreprises de télécommunications (lignes terrestres et téléphonie sans fil), les serveurs de données, les câblo-opérateurs, les fournisseurs de réseaux, les sociétés de transmission par satellite et les fournisseurs d'accès Internet. Les fournisseurs de services sont soumis aux diverses

réglementations nationales ; par ailleurs, ils ont souvent élaboré leurs propres politiques et normes internes. Le stockage des données coûte cher, de sorte que le fait qu'un fournisseur de services conserve ou non des données dépend de la législation nationale du pays dont il relève. Dans certains pays il n'existe aucune obligation en la matière, tandis que d'autres imposent aux fournisseurs de services de conserver les données pendant une durée limitée dans le temps.

Les demandes de retrait d'un contenu particulier doivent être adressées aux fournisseurs de services dans le respect du droit international des droits de l'homme, tout en prenant en compte le fait que le contenu en question est susceptible d'intéresser les agents de détection et de répression ainsi que les procureurs. Les *Recommandations de Zurich-Londres sur la prévention et la lutte contre l'extrémisme violent et le terrorisme en ligne* du GCTF offrent d'utiles orientations sur le sujet.

Suivant la juridiction dont ils relèvent, les fournisseurs de services peuvent conserver les données, les communiquer ou bien répondre à une demande urgente sur une base volontaire, conformément à leurs propres normes en matière d'application de la loi et à la législation nationale du pays où ils sont établis. Les normes en matière d'application de la loi décrivent la procédure à suivre pour présenter une demande de conservation ou de communication de données, le type de données susceptibles d'être demandées, les modalités de présentation de ces demandes, les possibilités d'extension du délai d'une injonction de conservation et la décision d'informer ou non l'utilisateur de cette injonction. Plusieurs fournisseurs majeurs de services communiquent leurs données en cas d'urgence.

Le caractère pléthorique des réglementations officielles et des normes privées crée un environnement complexe qui impose aux agents de détection et de répression et aux procureurs de se familiariser avec les normes légales applicables aux fournisseurs de services ainsi qu'avec les différentes règles en matière de conservation des données dans les pays où sont établis des fournisseurs de services.

Si un fournisseur de services n'a mis en place aucune procédure spécifique, il est recommandé aux agents de détection et de répression de s'adresser aux organisations internationales ou régionales chargées de l'application de la loi ou de faire appel à la coopération policière auprès des agents de détection et de répression du pays où est établi le fournisseur de services, afin de solliciter leur aide dans l'obtention de preuves électroniques. Néanmoins, les procédures de coopération actuellement en vigueur entre autorités judiciaires pour obtenir des preuves électroniques dans un contexte transfrontalier sont excessivement lentes si on les compare à la vitesse à laquelle les données peuvent être modifiées ou supprimées. La coopération informelle permet d'assouplir la procédure et d'obtenir directement des preuves électroniques auprès des fournisseurs de services, mais également d'accélérer une demande officielle de communication de données. La mise en place de réseaux informels entre agents de détection et de répression, procureurs, fournisseurs de services et autres parties prenantes peut également contribuer à promouvoir une meilleure compréhension mutuelle et à créer un climat de confiance.

Les pays devraient encourager les fournisseurs de services à rechercher une meilleure cohérence et normalisation des processus appliqués pour la conservation, l'obtention et le transfert de données, y compris en réponse à des demandes urgentes, et à désigner des représentants officiels au niveau national afin de faciliter la réception et le traitement des demandes de transmission de preuves électroniques.

Recommandation 13 : Obtenir des preuves électroniques situées à l'étranger

Il arrive souvent que les preuves électroniques se trouvent dans une juridiction autre que celle où se déroule la procédure pénale. Bien que les demandes d'entraide judiciaire soient chronophages et complexes, les pays continuent à recourir en priorité aux formes classiques et officielles de

coopération judiciaire internationale. Les pays qui ont besoin d'obtenir des preuves électroniques provenant d'autres pays peuvent faire appel aux conventions multilatérales telles que la Convention des Nations Unies contre la criminalité transnationale organisée, aux traités régionaux ou bilatéraux d'entraide judiciaire ainsi qu'à leur législation nationale, ou encore aux dispositions pertinentes de certaines conventions internationales ou régionales relatives à la lutte contre le terrorisme. En outre, les pays peuvent se prévaloir des conventions internationales cyber-spécifiques telles que la Convention du Conseil de l'Europe sur la cybercriminalité adoptée à Budapest, afin d'obtenir des preuves électroniques se trouvant dans d'autres pays. Afin d'accélérer la procédure d'entraide judiciaire, les agents de détection et de répression et les procureurs sont encouragés à indiquer précisément le type de données requises, à s'assurer que le critère de double incrimination est rempli et à envisager de se servir soit de formulaires-types internationaux ou nationaux de demandes d'entraide judiciaire, soit de l'instrument de demande d'entraide judiciaire de l'ONUDC. Un contact informel de leur part avec les pays requis avant l'émission de la demande officielle peut se révéler fructueux. Une autre bonne pratique consiste à transmettre informellement le projet de demande d'entraide judiciaire avant de la présenter par la voie officielle. Plusieurs formes de coopération informelle peuvent être envisagées, telles que la coopération entre services de police ou le recours au réseau de veille permanente des Bureaux centraux nationaux d'Interpol. D'autres réseaux informels de coopération, par exemple le réseau de veille permanente sous l'égide de la Convention du Conseil de l'Europe sur la cybercriminalité ou le Sous-groupe du G8 sur la criminalité liée aux technologies de pointe, peuvent également être saisis pour préparer les demandes d'entraide judiciaire et pour les soutenir.

La coopération informelle fonctionne souvent de manière plus rapide ce qui la rend très utile pour la collecte de preuves électroniques, en particulier lorsque les informations recherchées sont destinées aux services de renseignement. Un suivi peut être effectué à l'occasion de la demande officielle subséquente, dès lors que l'information a pour vocation de servir de preuve. Les agents de détection et de répression, les procureurs et les diverses autorités compétentes pourraient utilement consulter le Guide pratique sur la requête et la collecte transfrontalière des preuves électroniques rédigé par la DECT, l'ONUDC et l'Association internationale des procureurs (IAP).

Sachant que les preuves obtenues par le biais d'une collaboration informelle ou bien directement auprès des fournisseurs de services risquent de ne pas être admissibles devant les tribunaux, la collaboration officielle reste une modalité incontournable pour obtenir des preuves électroniques à partir d'un pays étranger. Il est recommandé aux pays de s'appuyer sur le cadre juridique existant pour activer l'entraide judiciaire afin d'obtenir des preuves électroniques à partir de pays étrangers, ou bien, le cas échéant, d'utiliser les mécanismes de coopération informelle, préalablement ou en complément de la coopération officielle, et de se baser sur la législation nationale ou sur le fondement juridique de la réciprocité pour que les pays concernés s'apportent mutuellement une entraide judiciaire dans les affaires en lien avec le terrorisme.

Recommandation 14 : Le respect des droits de l'homme dans le domaine des preuves électroniques

Le recours à des outils classiques ou cyber-spécifiques et les règles sur la conservation de données peuvent avoir une incidence sur le droit à la vie privée – et constituer de ce fait une violation de l'article 17 du PIDCP – ainsi que sur la protection des données personnelles. La protection des données personnelles est étroitement liée au droit à la vie privée mais les systèmes juridiques n'établissent pas toujours une distinction entre ces deux droits. La protection des données personnelles n'a pas un ancrage aussi solide dans les instruments internationaux contraignants, mais de très nombreux pays introduisent actuellement des dispositions sur cette question dans leur législation nationale.

La surveillance et la conservation légales des données à des fins de lutte contre le terrorisme sont des objectifs légitimes mais dont la nécessité et le caractère proportionnel doivent néanmoins, dans certaines juridictions, être établis afin d'éviter une application arbitraire. Certes, la plupart des pays sont dotés de dispositions protégeant la vie privée, mais les modalités de cette protection peuvent varier substantiellement d'un pays à l'autre : ainsi, dans certains pays le droit à la vie privée est garanti par la constitution, tandis que dans d'autres la protection de la vie privée fait l'objet de textes législatifs spécifiques. La protection de la vie privée peut également être assurée par autorégulation : ainsi, certains fournisseurs de services ont adopté des mesures relatives à la protection de la vie privée et ont parfois souscrit à des principes communs en la matière. Les garde-fous les plus fréquents visent notamment à restreindre les types de données concernées (renseignements sur l'abonné, sur le trafic ou sur le contenu), à limiter la durée d'activation des outils d'investigation, à fournir des garanties effectives contre l'utilisation abusive et à introduire des mécanismes de contrôle indépendants. À la lumière de l'évolution actuelle des technologies, il est recommandé aux pays de déterminer si la législation nationale sur la protection des données et de la vie privée prend suffisamment en compte la nécessité, pour les autorités chargées de l'application de la loi procédant à l'instruction ou à des poursuites relatives à des crimes en lien avec le terrorisme, de faire appel à des outils d'investigation, tout en respectant le droit à la vie privée et les droits de l'homme.

Recommandation 15 : Renforcer l'exploitation des preuves électroniques devant les tribunaux

Les preuves électroniques se modifient ou se dégradent facilement, ce qui constitue un défi au moment de les présenter devant les tribunaux. Les procureurs doivent s'assurer de l'authenticité et de l'intégrité des preuves électroniques présentées. La criminalistique numérique, qui consiste à extraire, analyser et décrire les données récupérées à partir d'ordinateurs, de téléphones portables ou d'autres supports, joue un rôle crucial pour la présentation des preuves électroniques devant les tribunaux. Lorsque les preuves électroniques proviennent directement des fournisseurs de services, les agents de détection et de répression ou les procureurs peuvent demander au fournisseur concerné de présenter un document expliquant les garanties juridiques liées à la possession et à la communication de données ou une déclaration indiquant que la preuve électronique fait l'objet d'une authentification automatisée. Il est recommandé aux pays d'investir dans le renforcement des capacités en criminalistique numérique, ce qui recouvre les équipements mais aussi la formation du personnel au décryptage et à l'évaluation de la fiabilité des preuves électroniques.

Les preuves électroniques sont difficiles à traiter dans les affaires en lien avec le terrorisme en raison de la multiplicité de formats de fichiers, de systèmes d'exploitation et de logiciels utilisés par les acteurs de la justice pénale et par les fournisseurs de services dans un même pays ou d'un pays à l'autre. Il est donc recommandé aux pays d'élaborer des normes internationales afin d'améliorer l'interopérabilité des données électroniques quel que soit le système juridique, et d'améliorer l'utilisation des preuves électroniques dans les enquêtes et les poursuites en lien avec le terrorisme.

Dans la plupart des pays, les preuves électroniques sont admissibles devant les tribunaux. Les preuves électroniques peuvent être présentées de différentes manières, en recourant à des témoignages ou à des rapports d'experts mais aussi sous forme d'équipements informatiques. Les preuves électroniques peuvent atteindre un tel degré de complexité technique qu'il est parfois nécessaire de convoquer un expert spécialisé dans la criminalistique numérique afin d'expliquer à la cour la pertinence des preuves électroniques présentées dans une affaire particulière. Il est recommandé aux pays d'améliorer les capacités techniques des procureurs en organisant régulièrement à leur intention des formations en informatique dédiées plus particulièrement aux différents aspects de l'extraction, du stockage et de l'utilisation des preuves électroniques devant les tribunaux.

IV. Recommandations sur la collecte, l'utilisation et le partage du renseignement aux fins d'enquêtes et de poursuites pénales

Les services de renseignement tant civils que militaires disposent d'informations pertinentes sur les terroristes et leurs réseaux, qui sont obtenues aussi bien sur le champ de bataille qu'en dehors de celui-ci. En particulier, là où les canaux habituels de la coopération policière et judiciaire entre les différents acteurs du secteur de la justice pénale n'opèrent plus, par exemple dans les situations de conflit, les services de renseignement peuvent jouer un rôle crucial pour réunir des renseignements aux fins d'enquêtes et de poursuites pénales. Cela s'applique également au cas des combattants terroristes étrangers qui ont quitté une zone de combat pour retourner dans leur pays ou se rendre dans un pays tiers. Afin d'optimiser le potentiel probant du renseignement devant les tribunaux, il est essentiel de veiller à l'efficacité de la coordination, la coopération et la communication entre les services de renseignement et des services de police, aussi bien à l'échelle nationale qu'entre différents pays. Il faut également tenir compte de la difficulté liée, d'une part à l'objectif escompté d'utiliser effectivement le renseignement comme élément de preuve devant les tribunaux, ce qui va au-delà d'une l'utilisation de cette information en tant que simple élément permettant d'ouvrir une enquête ; et d'autre part à la nécessité de garantir que la procédure en place permette de présenter cette information devant les tribunaux tout en respectant le droit à un procès équitable et en protégeant les sources et les méthodes d'obtention de cette information.

En particulier, les pays devraient se doter de mécanismes et de procédures permettant aux services de renseignement de partager avec les agents de détection et de répression autorisés les informations relatives aux menaces terroristes, chaque fois que nécessaire. La mise en place de ces procédures devra tenir compte à la fois des préoccupations du gouvernement en matière de sécurité nationale et du droit de l'accusé à bénéficier d'un procès équitable. Dans un souci de protection des victimes et des informateurs et de préservation des sources et des méthodes, et afin de pérenniser le potentiel des techniques sensibles d'investigation, il conviendra que les gouvernements puissent soustraire certaines catégories d'informations et de techniques à toute diffusion publique, y compris lors du déroulement de la procédure pénale.

Les recommandations suivantes complètent et prolongent la Résolution 2396 (2017) du Conseil de sécurité des Nations Unies ainsi qu'un certain nombre de bonnes pratiques et recommandations existantes du GCTF, en particulier les bonnes pratiques 6 et 9 du *Mémorandum de Rabat*, la bonne pratique 6 du *Mémorandum de La Haye sur les bonnes pratiques du système judiciaire pour juger les actes terroristes* et les recommandations 1, 2, 3, 4, 5 et 6 des *Recommandations du GCTF sur l'utilisation et la protection du renseignement lors d'enquêtes et de poursuites menées par le secteur de la justice pénale et fondées sur l'état de droit*.

Recommandation 16 : Promouvoir une coordination, une coopération et une communication efficaces

L'intensification de la coordination et de la coopération, par exemple par le biais des centres de fusion du renseignement (mais aussi d'autres mécanismes de coopération plus informels) aboutira à une meilleure compréhension des rôles et des besoins respectifs des deux communautés. L'information requise est souvent là, mais elle doit être rendue disponible pour ceux qui en ont besoin, pour autant que la législation nationale le permette ; elle doit être accessible en premier lieu aux intervenants concernés. Par exemple, les agents des services de renseignement disposent parfois d'informations qui ne sont pas pertinentes pour leur propre travail, mais qui peuvent être d'une importance capitale pour un procureur à la recherche de la dernière pièce du puzzle qui lui permettra d'engager des poursuites à l'encontre d'un terroriste présumé. Lorsqu'un élément d'information particulier a joué un rôle déterminant dans la condamnation d'un terroriste, il est important de le signaler aux services

qui ont les premiers fourni cette information (il peut s'agir du service de renseignement d'un pays étranger), afin de faciliter la mise en place d'une chaîne vertueuse de remontée des informations.

Il est donc recommandé aux pays de continuer à s'investir dans la mise en place de mécanismes de coordination et de coopération entre les services de renseignement, les autorités policières et le secteur judiciaire à l'échelle nationale. Comme cela a déjà été préconisé dans les *Recommandations du GCTF sur l'utilisation et la protection du renseignement lors d'enquêtes et de poursuites menées par le secteur de la justice pénale et fondées sur l'état de droit*, il est souhaitable que les pays mettent en place des mécanismes et des procédures permettant aux agences de renseignement de prendre pleinement connaissance des normes relatives aux règles de la preuve qui s'appliquent dans les procédures judiciaires du pays concerné.

Recommandation 17 : Améliorer le partage du renseignement aux fins d'enquêtes et de poursuites pénales à l'échelle internationale

Les pays peuvent procéder à un partage tant bilatéral que multilatéral du renseignement aux fins d'enquêtes et de poursuites pénales, par exemple via Interpol ou Europol. Le partage du renseignement est d'autant plus fructueux que les droits de l'homme ont été respectés aussi bien lors de la collecte des données que lors de leur traitement et utilisation dans le cadre des procédures pénales. Les pays sont davantage disposés à souscrire au partage du renseignement lorsque des garanties ont été apportées quant au caractère conforme aux droits de l'homme des procédures de collecte et de partage des données.

Il est évident que les pays vont réserver le partage avancé de données du renseignement aux seuls pays dont les services concernés leur inspirent confiance, c'est-à-dire ceux dont le système juridique leur paraît fiable (car respectueux des droits de l'homme). Certains pays, en vertu de leur législation et réglementations nationales ne peuvent partager de renseignements avec des services étrangers que si ces derniers se conforment à un certain nombre d'exigences en matière de droits de l'homme. Il est recommandé aux pays ayant d'authentiques doutes sur la manière dont l'information sera utilisée par un autre pays de ne partager ses informations que sous réserve d'avoir reçu de l'autre pays des garanties sérieuses que l'information fournie ne donnera pas lieu à une violation des droits de l'homme.

Par ailleurs, il est recommandé aux pays de renforcer le partage du renseignement aux fins d'enquêtes et de poursuites pénales en recourant aux organisations internationales. Le terrorisme (en particulier dans ses aspects en lien avec le phénomène des combattants terroristes étrangers) est doté d'une dimension transfrontalière ou transrégionale qui exige une réponse véritablement internationale. Comme c'est le cas au niveau national, il est essentiel au niveau international que les informations pertinentes soient communiquées aux acteurs qui en ont le plus besoin. Des organisations telles qu'Interpol et Europol peuvent jouer un rôle crucial à cet égard. Dans chaque situation, qu'il s'agisse d'un partage bilatéral ou multilatéral, il est recommandé aux pays de ne fournir aux organisations telles qu'Interpol et Europol, aux fins d'enquêtes et de poursuites pénales, que des informations obtenues en pleine conformité avec les exigences des droits de l'homme.

Cela renforcera les probabilités que l'information soit jugée admissible au cas où elle serait présentée en tant que preuve devant les tribunaux.

Recommandation 18 : Renforcer l'exploitation du renseignement en tant que preuve devant les tribunaux

Les services de renseignements sont généralement réticents à rendre publiques les sources et les méthodes d'obtention de leurs informations. Toutefois, pour que cette information puisse être jugée admissible en tant que preuve devant les tribunaux, il est important, suivant la législation nationale en vigueur, que l'origine, et donc la fiabilité des informations puissent être établies aussi bien par le procureur que par le juge. En général, afin d'éviter autant que possible de recourir à des procédures de déclassification, il est recommandé aux États de ne pas surclassifier les données du renseignement.

En outre, dans certains pays, les données du renseignement sont parfois examinées par une tierce partie, ayant à la fois un pied dans la communauté du renseignement et un autre dans la communauté de l'application de la loi, par exemple une commission indépendante ou un procureur spécialisé dans le renseignement, qui détermine à l'issue de cet examen si certaines informations peuvent être déclassifiées et versées aux dossiers. Toutefois, dans d'autres pays, surtout ceux de *Common Law*, les agents de détection et de répression collaborent avec ceux des services de renseignement afin de déterminer quelles informations sont pertinentes pour l'affaire en cours. Par la suite, le procureur décidera avec ces entités de la manière appropriée de transmettre ces informations au tribunal et/ou à la défense. Il est recommandé aux pays d'envisager la mise en place de mécanismes de ce type qui permettent d'exploiter le renseignement en tant que preuve recevable, compte tenu des spécificités du système juridique.

Recommandation 19 : Respecter le droit international et les droits de l'homme

En vertu du droit relatif aux droits de l'homme, tout accusé a le droit de contester les éléments de preuve présentés contre lui. En même temps, une certaine souplesse peut se révéler nécessaire si l'on veut prendre en compte les préoccupations légitimes sur la sécurité qui se manifestent lors de l'utilisation d'informations classifiées ou sensibles issues des services de renseignement, du moins lorsqu'il apparaît que cette information est destinée à être utilisée en tant que preuve lors d'une procédure pénale. Il s'agit de situations où il faut savoir sortir des anciens cadres conceptuels et recourir à des méthodes innovantes. On peut, par exemple, protéger l'identité des témoins en les faisant témoigner sous pseudonyme, derrière un écran de protection ou sous des formes déguisées (avec l'autorisation de la cour).

En ce qui concerne la question de savoir ce qu'il convient de faire en cas de violation du droit international lors de la phase d'instruction : dans la plupart des systèmes juridiques, les juges ont le pouvoir discrétionnaire de décider, au cas par cas, des mesures à prendre en cas de violation d'un droit, mais tous les juges n'ont pas le même niveau de qualification concernant les normes du droit international (par opposition au droit national), et tous les pays n'ont pas le même niveau de transposition de ces normes en droit national. Tout en soulignant l'autonomie et l'indépendance du pouvoir judiciaire, et conformément aux pratiques et cadres juridiques applicables et pertinents, les pays pourraient élaborer des lignes directrices en la matière, dont les juges pourraient tenir compte lorsqu'ils évaluent certaines violations des droits de l'homme et/ou du droit international survenues avant le procès ou dans le cadre de celui-ci. Les mesures les plus graves sont l'exclusion des preuves obtenues illégalement ou l'exclusion de l'argument de ces preuves. En effet, la gravité de certaines violations des droits est telle – par exemple le recours à la torture pour obtenir des éléments d'information – que la preuve sera toujours déclarée inadmissible par le tribunal afin d'éviter de compromettre l'intégrité de la procédure judiciaire, et ce quel que soit l'auteur responsable. Dans de telles situations, les agents des services concernés devraient également déterminer s'il convient ou non de partager ce type d'information « douteuse », que ce soit sur un mode bilatéral ou multilatéral. Pour les violations moins graves des droits, d'autres mesures peuvent être envisagées, telles qu'une

réduction de peine, une indemnisation financière ou, s'il s'agit d'une violation strictement procédurale sans impact substantiel sur les droits du suspect, l'énoncé du non-respect de certaines règles de procédure.

V. Recommandations relatives à la collecte, à l'utilisation et au partage des éléments de preuve par les forces armées

Les enquêtes et les poursuites visant des crimes en lien avec le terrorisme se limitent rarement aux actes commis sur le territoire d'un seul pays. Les terroristes et les organisations terroristes opèrent souvent à l'étranger et ont désormais une dimension transfrontalière ou transrégionale. La collecte d'informations et d'éléments de preuve concernant les crimes en lien avec le terrorisme exige souvent de coopérer avec d'autres pays en activant l'entraide judiciaire. Néanmoins, en situation de conflit ou de post-conflit, une telle coopération n'est pas toujours efficace ni même envisageable. Cela est dû au contexte souvent chaotique et instable dans lequel se trouve l'information, ce qui rend très difficile le recours aux accords existants d'entraide judiciaire, ou bien au fait que les accords d'entraide judiciaire n'existent pas et que la coopération judiciaire basée sur la simple réciprocité est impossible dans le pays où se trouvent ces preuves. Le risque qui se pose dans ces cas de figure est celui de l'impunité, en raison de la probabilité que des crimes en lien avec le terrorisme effectivement commis dans ces situations de conflit ou de post-conflit ne fassent pas l'objet de poursuites, par manque d'éléments de preuve. Dans un tel scénario, les procureurs de certains pays ont adopté une stratégie d'accusation un peu différente, axée sur une poursuite des auteurs de ces crimes pour tentative de quitter le territoire, conspiration en vue d'un attentat terroriste, ou appartenance à une organisation terroriste. Ces situations soulèvent la question du risque d'impunité ainsi que celle du droit des victimes à la justice, qui sont toutes deux à prendre en compte.

D'autre part, une situation chaotique consécutive par exemple à un conflit armé peut également survenir sur le territoire du pays ayant engagé des poursuites contre un suspect. Dans un tel contexte il peut aussi se révéler très difficile pour l'accusation d'apporter la preuve de la commission de crimes terroristes, y compris des crimes connexes tels que les violences sexuelles exercées par des membres d'organisations terroristes.

Les difficultés auxquelles sont confrontés les agents de détection et de répression et les procureurs lors de la collecte d'éléments de preuve pertinents sont exacerbées par la menace croissante posée par les combattants terroristes étrangers et par le retour dans leur pays de ces combattants, ainsi que par l'ambition des procureurs de poursuivre des citoyens ou des résidents de leur propre pays. Les nombreuses informations susceptibles d'être récupérées dans un contexte de conflit ou de post-conflit peuvent se révéler intéressantes dans une perspective de poursuites pénales. Il s'agit notamment de données du renseignement, de données criminalistiques comme les empreintes digitales relevées sur des engins explosifs improvisés saisis sur le champ de bataille, d'information et de preuves recueillies dans divers sites, dont les fosses communes, et d'informations sur l'appartenance de certains individus à des organisations terroristes et sur la portée des réseaux au sein desquels ils opèrent. Ce type d'information et de preuves peut apporter des pièces déterminantes au puzzle à compléter pour cerner le modus operandi des organisations terroristes et déterminer qui sont les auteurs respectifs des divers crimes en lien avec le terrorisme.

Dans la plupart des cas, les opérations militaires n'ont pas pour principal objet de recueillir des informations susceptibles d'être utilisées en tant qu'éléments de preuve. Néanmoins, du fait de leur présence sur le champ de bataille, les militaires sont susceptibles de contribuer à la collecte d'informations pertinentes qui pourraient être utilisées en tant qu'éléments de preuve devant les tribunaux. De telles activités doivent être réalisées dans le respect du droit international.

Si les circonstances s'y prêtent et en coordination avec les forces armées, les commissions d'enquête internationales ou d'autres mécanismes dûment autorisés par le Conseil de sécurité des Nations Unies peuvent également prélever des informations pertinentes sur le champ de bataille, en vue de leur utilisation dans les poursuites visant des crimes en lien avec le terrorisme. Clairement, le scénario où les forces armées contribuent à faciliter la collecte d'informations et d'éléments de preuve doit être considéré comme un événement exceptionnel.

Toutefois, dans cette situation les agents de détection et de répression et les procureurs sont confrontés à la difficulté particulière de devoir s'assurer que l'information obtenue par les militaires et par d'autres acteurs reconnus dans des situations de conflit ou de post-conflit répond aux exigences légales minimales permettant par la suite d'accepter cette information comme élément probant dans le cadre d'une procédure pénale, quel que soit le système juridique du pays. Les conditions juridiques strictes prévues dans les codes de procédures pénales nationaux, notamment celles portant sur l'admissibilité des preuves, sur les garanties juridiques liées à la possession et à la communication d'éléments de preuve et sur le droit à un procès équitable devront être remplies.

Cette difficulté a été prise en compte dans les Principes directeurs de Madrid (S/2015/939, 23 décembre 2015) et mentionnée également dans la RCSNU 2396 (2017). En outre, le Sixième rapport du Secrétaire général sur la menace que représente l'État islamique d'Iraq et du Levant (*Da'esh*) (S/2018/80 du 31 janvier 2018) souligne que rares sont les États en mesure de recueillir des éléments de preuve dans les zones de conflit, de sorte que les efforts en la matière doivent être renforcés.

Plusieurs initiatives internationales sont en cours d'élaboration pour soutenir le rôle des militaires, leur fournir des principes directeurs et clarifier le mandat dans lequel ils doivent s'inscrire ainsi que les modalités applicables. Dans un contexte onusien, les « Lignes directrices des Nations Unies visant à faciliter l'utilisation et la recevabilité en tant que preuves des informations sauvegardées, recueillies et partagées par les militaires » permettront de fournir de telles orientations.

Recommandation 20 : Renforcer l'utilisation des informations recueillies par les forces armées en tant qu'éléments de preuve devant les tribunaux

Étant donné que dans les situations exceptionnelles telles que les situations de conflit ou à haut risque, les agents de détection et de répression ne sont pas toujours en mesure de mener à bien les enquêtes sur des crimes en lien avec le terrorisme, il est recommandé aux pays de faire en sorte que l'information recueillie par les militaires puisse être utilisée en tant qu'élément probant dans les affaires de terrorisme, conformément au droit pénal national et, si nécessaire, d'amender leur législation nationale afin de rendre possible cette utilisation, ou de donner les instructions nécessaires pour que cela puisse être fait. En outre, il est recommandé aux pays de s'assurer que le droit à un procès équitable, l'absence de torture et de traitements inhumains et dégradants, le principe du contradictoire et l'admission équitable des preuves sont respectés lorsqu'ils autorisent l'utilisation d'informations de ce type recueillies par les forces armées.

Dans certaines situations, les agents de détection et de répression et les procureurs peuvent jouer un rôle encore plus proactif en communiquant clairement aux acteurs militaires leurs besoins spécifiques en matière de preuves, par exemple lors de la phase préparatoire d'une mission militaire.

Certains États ont acquis une certaine expérience dans la collecte d'informations sur le champ de bataille en vue de leur utilisation en tant qu'éléments de preuve dans des procédures pénales et trouvé un compromis entre, d'une part, la nécessité de sécuriser les garanties juridiques liées à la possession et à la communication d'éléments d'information dans un contexte parfois chaotique et dangereux et, d'autre part, le droit à un procès équitable, ce qui recouvre mais sans s'y limiter,

l'absence de torture et de traitements inhumains et dégradants, le respect du principe du contradictoire et le respect de l'admission équitable des preuves. Il est donc recommandé aux États d'échanger sur ces expériences afin de réunir un compendium de bonnes pratiques.

Recommandation 21 : Veiller aux garanties juridiques liées à la continuité de la preuve et respecter l'intégrité des procédures pénales

La sauvegarde des garanties juridiques liées à la continuité de la preuve est une condition fondamentale pour pouvoir présenter une information de quelque type que ce soit en tant qu'élément de preuve dans une procédure pénale. Il est parfois difficile de veiller aux garanties juridiques liées à la continuité de la preuve lorsque ces informations sont recueillies sur un champ de bataille et utilisées lors d'une procédure pénale, indépendamment du type de preuves dont il s'agit (matérielles, électroniques ou médico-légales). En effet, dans le contexte chaotique et fortement instable d'un champ de bataille, il n'est pas toujours possible de suivre la procédure consistant à protéger les preuves dans des pochettes étiquetées sur la scène même du crime, maintenue sous scellés. Néanmoins, les militaires et d'autres acteurs autorisés à recueillir des informations sur un champ de bataille peuvent, dans la mesure du possible, assurer la traçabilité de l'information dès qu'ils ont gagné une position sécurisée et consigner le nom de la personne ayant recueilli l'information, le lieu, la date et l'heure, ainsi que les circonstances de cette collecte et le nom de tous ceux qui ont manipulé la preuve et du destinataire final. L'existence de failles dans les garanties juridiques liées à la continuité de la preuve ne devrait toutefois pas entraîner l'exclusion systématique de la preuve. Nonobstant ces difficultés et compte tenu du potentiel existant, il est recommandé aux pays de sensibiliser les acteurs de la justice pénale sur les limites et les possibilités liées à la collecte d'informations et d'éléments de preuve sur le champ de bataille, en tenant compte des impératifs de l'efficacité opérationnelle.

Au cours du procès, un certain nombre de difficultés peuvent se présenter et influer sur l'admissibilité de l'information en tant qu'élément de preuve devant le tribunal. Ces difficultés portent sur l'interrogatoire ou contre-interrogatoire du témoin ou du militaire ayant recueilli l'information et sur son niveau d'expertise et de compétences au regard de la procédure à suivre pour disposer les éléments de preuve dans des pochettes étiquetées.

La défense doit être en mesure de vérifier la fiabilité et la crédibilité des éléments de preuve présentés. Pour des raisons de sécurité nationale, l'identité de l'individu ayant recueilli l'information ou prélevé l'élément de preuve sur le champ de bataille doit parfois rester secrète (qu'il s'agisse d'un militaire ou d'un autre acteur). Afin de produire malgré tout un témoignage sur la manière dont cette information ou élément de preuve a été recueilli tout en garantissant dans toute la mesure du possible le droit à un procès équitable, des solutions innovantes ou non conventionnelles devront être recherchées afin que la défense puisse exercer son droit à un contre-interrogatoire. Il peut s'agir de dispositifs vidéo ou de la présentation d'une déclaration écrite sous serment, sous réserve du droit national de la preuve.

Se pose aussi la question du niveau d'expertise et de compétences des différents acteurs en présence sur le champ de bataille concernant la manière de traiter les informations ou de manipuler les éléments de preuve qui doivent être présentés devant un tribunal. Par exemple, on peut supposer que les unités de la police militaire (lorsqu'elles existent) ou les enquêteurs intégrés (par exemple, détachés par le ministère de la Justice auprès du commandement militaire) auront reçu une formation sur le traitement des preuves. En fonction du niveau d'expertise et de compétences des acteurs militaires concernés, l'intérêt des preuves présentées peut compenser d'éventuelles irrégularités dans les garanties juridiques liées à la continuité de la preuve. En dernière instance, il appartiendra à la cour de se prononcer sur l'admissibilité des preuves.

Il est donc recommandé aux pays d'envisager l'élaboration de principes directeurs rédigés en conformité avec les règles nationales de procédure pénale et avec les obligations qui leur incombent en vertu du droit international des droits de l'homme, afin d'aider les acteurs de la justice pénale à définir le compromis à trouver entre la prise en compte des circonstances dans lesquelles a été obtenue une information ou une preuve et le respect des garanties juridiques liées à la continuité de la preuve, ainsi que l'intégrité de la procédure pénale, en particulier le plein exercice des droits de la défense.

Recommandation 22 : Promouvoir l'efficacité de la coopération, la coordination, l'entraide judiciaire et la communication avec les acteurs concernés

Il est recommandé aux agents de détection et de répression ainsi qu'aux procureurs qui requièrent, dans des affaires en lien avec le terrorisme, de recourir à des éléments de preuve collectés sur le champ de bataille, de faire tout ce qui est en leur pouvoir pour établir des relations de travail avec les autorités de la justice pénale du pays dans lequel la preuve a été collectée, afin de faciliter l'entraide judiciaire. Toutefois, dans les situations dans lesquelles il semble impossible d'établir de telles relations, il est recommandé aux agents de détection et de répression ainsi qu'aux procureurs d'établir, aussitôt que possible dans la procédure, des relations de travail et des canaux de communication avec les acteurs concernés sur le champ de bataille qui pourront apporter une assistance dans la collecte des informations susceptibles d'être présentées comme éléments de preuve.

Recommandation 23 : Renforcer le caractère pluridisciplinaire de l'information recueillie par les forces armées et la déclassification du renseignement militaire

En maintes occasions, dans le cadre des activités habituelles des forces armées durant une opération, il arrive que du renseignement soit recueilli à des fins opérationnelles. Ces données du renseignement sont susceptibles de contenir des informations importantes concernant la commission de crimes en lien avec le terrorisme, les réseaux terroristes et les individus impliqués. De toute évidence, les enquêtes et poursuites pénales gagneraient à obtenir ces informations. De manière générale, il est conseillé de ne classifier l'information qu'en cas de stricte nécessité. Lorsque le renseignement a été classifié mais est susceptible d'être ultérieurement déclassifié en raison de sa pertinence aux fins de l'instruction d'une affaire ou d'une poursuite pénale, la question de son admissibilité devant un tribunal demeure entière.

Dans certaines situations, l'information recueillie par les forces armées peut être traitée dans le cadre de filières parallèles et avec une double finalité. Ainsi, outre son traitement par la filière du renseignement, confidentielle, l'information pourrait en même temps être traitée dans le but de poursuites judiciaires, en veillant à garantir la continuité de la preuve et le droit à un procès équitable. Le cas échéant, il est conseillé aux agents de détection et de répression ainsi qu'aux procureurs de communiquer aux acteurs concernés quels sont leurs besoins dans le cadre d'une enquête aux fins des poursuites judiciaires, faisant ainsi en sorte que toutes les possibilités de traitement de l'information soient envisagées.

Il existe des bonnes pratiques sur la manière de concilier la nécessité de respecter la confidentialité des sources avec la nécessité de transparence dans les procédures pénales, tout en respectant les garanties d'un procès équitable. Il est par conséquent conseillé aux pays de prendre en considération les recommandations et bonnes pratiques déjà existantes et figurant dans les documents suivants du GCTF : *Mémorandum de Rabat*, *Mémorandum de La Haye sur les bonnes pratiques pour juger les actes terroristes*, et *Recommandations sur l'utilisation et la protection du renseignement lors d'enquêtes et de poursuites menées par le secteur de la justice pénale et fondées sur l'état de droit*.

VI. Recommandations sur l'audition des témoins et l'utilisation des témoignages

Les témoignages ont toujours été précieux, et continuent de l'être, dans le cadre des enquêtes et de la poursuite des crimes, notamment de crimes en lien avec le terrorisme. Nombreux sont les témoins dont la déposition peut être retenue, par exemple les victimes, les informateurs et les collaborateurs de la justice/repentis.

En raison précisément du rôle crucial dévolu aux témoins dans les enquêtes et poursuites de crimes graves, nombre d'entre eux peuvent faire l'objet d'intimidations ou de menaces, phénomène particulièrement notoire dans les affaires en lien avec le terrorisme. Dans le contexte des combattants terroristes étrangers, il arrive que des membres de la famille d'un combattant terroriste apportent un témoignage pour ensuite se rétracter ou modifier leur témoignage du fait des intimidations reçues. Cela soulève des problématiques relatives à la fois à la vulnérabilité et à la crédibilité de ces témoins. C'est pourquoi il est d'une importance majeure de protéger les témoins (au tribunal et à l'extérieur) mais en même temps de garantir le droit du défendant à un procès équitable conformément à l'article 14 du PIDCP.

L'on peut s'attendre à une augmentation du recours aux dépositions de ce type de témoins dans les poursuites relatives à des affaires de terrorisme, notamment celles des témoins experts. En effet, les affaires de terrorisme gagnent sans cesse en complexité, compte tenu de la nature parfois technique, voire scientifique, des éléments de preuve tels que la preuve électronique ou médico-légale. Par conséquent, ce sont les témoins experts qui doivent détailler la nature et la pertinence de ces éléments de preuve à l'intention des procureurs, des avocats de la défense et des juges.

Les recommandations suivantes viendront compléter et prolonger les bonnes pratiques et recommandations du GCTF déjà existantes, notamment : la bonne pratique 4 du *Mémorandum de La Haye sur les bonnes pratiques du système judiciaire pour juger les actes terroristes*, la bonne pratique 1 du *Mémorandum de Rabat* et les recommandations 1, 5 et 7 des *Recommandations sur l'utilisation et la protection du renseignement lors d'enquêtes et de poursuites menées par le secteur de la justice pénale et fondées sur l'état de droit*. En outre, le manuel de l'Office des Nations Unies contre la drogue et le crime intitulé Bonnes pratiques de protection des témoins dans les procédures pénales afférentes à la criminalité organisée (en abrégé le Manuel de l'ONUDC) est tout aussi pertinent dans le contexte des affaires de terrorisme et doit donc être pris en compte.

Recommandation 24 : Autoriser le recours à des mesures procédurales de protection

En vue de veiller à ce que les témoins, dans la plus grande mesure possible, puissent témoigner sans se sentir intimidés ou menacés, diverses mesures procédurales de protection sont envisageables. Parmi elles, l'utilisation de déclarations faites pendant l'instruction (qu'il s'agisse de dépositions écrites ou d'enregistrements vidéo ou audio) au lieu de témoignages apportés devant le tribunal ; caviardage/noircissement du nom et de l'adresse d'un témoin dans les déclarations écrites ; témoignage entendu au moyen d'un circuit fermé de télévision ou d'une connexion audiovisuelle, par exemple sous forme de visioconférence, en utilisant un pseudonyme, un léger déguisement, un dispositif d'altération de la voix, ou en installant le témoin derrière un rideau ou un écran protecteur ; ou en faisant sortir le public de la salle d'audience (séance à huis clos). Il est recommandé aux pays de se pencher sur la diversité des mesures procédurales utilisées dans d'autres pays ou par les tribunaux en vue de protéger les témoins dans les affaires ici traitées, et d'adopter le cas échéant des mesures qui respectent leurs obligations internationales ainsi que celles découlant de leurs cadres et systèmes juridiques. Cela implique notamment de déterminer si de telles mesures procédurales de protection sont permises au regard de la législation en vigueur, et si elles sont réalisables technologiquement.

Ces mesures pourraient avoir une incidence sur les droits de la défense « à interroger ou faire interroger les témoins à charge et à obtenir la comparution et l'interrogatoire des témoins à décharge dans les mêmes conditions que les témoins à charge » en vertu de l'article 14, paragraphe 3 (e) du PIDCP. Les droits de la défense et la perception publique de la légitimité des institutions judiciaires sont mieux servis si le recours à des informations classifiées ou à des audiences en huis clos est limité. Par conséquent, une condamnation ne saurait reposer uniquement sur un témoignage classifié ou secret ni sur des preuves expurgées ou censurées.

Recommandation 25 : Adopter une approche adaptée, souple et globale encadrant les auditions des témoins ainsi que l'assistance et la protection qui leur sont fournies

Il est important d'adopter une approche adaptée, souple et globale lors de l'audition des témoins ou dans les mesures d'assistance et de protection à leur égard, afin d'obtenir des informations exactes et fiables sur les faits survenus. Lors de l'audition des témoins, tous les éléments pertinents doivent être pris en considération, tels que l'âge, le genre et les capacités mentales. Certaines circonstances exigent d'accorder une attention particulière à des individus ou des groupes donnés, par exemple les femmes, les personnes âgées ou les enfants. De plus, afin d'éviter tout traumatisme supplémentaire ou revictimisation, il convient de prêter spécialement attention aux victimes d'actes terroristes, dont les femmes ayant subi un crime sexuel commis par des organisations terroristes. Pour ces témoins particulièrement vulnérables, les mesures procédurales de protection évoquées plus haut, y compris le recours à la technologie vidéo ou à une assistance psychologique au tribunal, peuvent être encore plus pertinentes que pour les autres témoins. Dans le contexte de l'assistance aux victimes, qu'il convient de distinguer de la protection des victimes, il pourrait être utile de recourir à des ONG reconnues, évaluées et approuvées qui ont l'expérience du travail avec les personnes vulnérables. Lorsque, dans certaines circonstances, les preuves sont recueillies par les forces armées, les personnels militaires doivent avoir conscience que la personne qu'ils interrogent peut se sentir intimidée par eux, ce qui pourrait avoir des répercussions sur la fiabilité de la déposition du témoin. Il convient dès lors de tenir compte des sensibilités institutionnelles/culturelles, ou tout simplement de comprendre l'effet que l'on a sur autrui. Enfin, la protection des témoins doit être comprise dans son acception la plus ample et globale ; les mesures doivent être prises aussitôt que possible, et il convient de prendre en considération non seulement les menaces posées à l'intégrité physique ou à la sécurité des personnes, mais aussi à leur bien-être et dignité, y compris au stress émotionnel que peut induire le fait de comparaître devant un tribunal. Il est par conséquent recommandé aux pays de mettre au point une approche adaptée, souple et globale encadrant les auditions des témoins ainsi que l'assistance et la protection qui leur est fournie.

Recommandation 26 : Aider au témoignage des personnes en possession d'informations sensibles ou classifiées

Les personnes en possession d'informations sensibles ou classifiées (par exemple les agents du renseignement) peuvent se montrer réticentes à témoigner devant un tribunal, mais les mesures spécifiques de protection présentées dans la Recommandation 24 peuvent néanmoins, le cas échéant, faciliter de tels témoignages. Il a cependant été constaté que lorsque ces personnes apportent effectivement un témoignage, il arrive parfois que les juges mettent en cause la crédibilité de leur déposition, même lorsqu'il s'agit d'agents de services du renseignement d'un autre pays. Cela n'est pas dû à l'information (ou au manque d'information) détenue par ces personnes, mais à la manière dont celle-ci est présentée. Ainsi, si l'on veut éviter que des informations cruciales ne soient écartées par les juges pour ces raisons, il est recommandé aux pays d'investir davantage dans l'assistance aux personnes qui n'ont peut-être pas l'habitude de témoigner devant un tribunal (étranger), y compris aux agents du renseignement et à toute autre personne ayant des informations déterminantes dans une affaire. Si les pays investissent dans des activités permettant aux personnes de se familiariser avec la manière de présenter leur déposition, ou leur expliquant ce que signifie concrètement le

témoignage devant un tribunal, quel comportement adopter et comment s'adresser au juge, cela pourrait donner davantage de crédibilité à leur témoignage, ce qui pourrait dès lors contribuer à une conclusion plus rapide et satisfaisante de l'affaire.

Recommandation 27 : Mettre sur pied des programmes de protection des témoins

Aux côtés des mesures procédurales de protection qui s'appliquent dans les tribunaux, il est loisible aux pays de décider de mettre sur pied un programme de protection des témoins reposant sur une analyse qui tienne compte, entre autres, des ressources disponibles, de la volonté de poursuivre les crimes en lien avec le terrorisme sur la base de témoignages, ainsi que de la fréquence des actes de violence à l'encontre de témoins. Les programmes de protection des témoins prévoient parfois l'installation de témoins dans un pays étranger, éventuellement avec les membres de leur famille immédiate. Les programmes peuvent relever des forces de police ou d'autres organes, certains modèles faisant d'ailleurs intervenir un organisme multidisciplinaire. Quelle que soit l'approche adoptée, il est recommandé aux pays de veiller à établir une séparation nette entre ce qui relève de l'instruction et de la confidentialité de la procédure, d'une part, et ce qui relève des aspects opérationnels et de l'autonomie organisationnelle des forces de police, d'autre part. Dans ce contexte il est impératif de se doter de ressources dédiées et d'organiser une coordination rapprochée entre tous les acteurs compétents au niveau national. Il est en outre recommandé aux pays de proposer continuellement des formations multidisciplinaires qui contribueront à instaurer la confiance des autres pays en leur capacité de protéger les témoins, ce qui renforcera la coopération internationale en matière de réinstallation des témoins.

Recommandation 28 : Renforcer le recours à des témoins experts près les tribunaux

À la lumière de l'utilisation croissante d'éléments de preuve sous une forme chaque fois plus technique, comme la preuve électronique et la preuve médico-légale, les tribunaux vont probablement recourir de plus en plus à des témoins experts. Compte tenu du degré de technicité en jeu, il sera vraisemblablement difficile d'évaluer ce qui est réellement dit (sur le fond) et le niveau d'expertise du témoin entendu. Dans tous les cas où des témoins sont appelés à s'exprimer devant un tribunal dans une procédure pénale, tout se résumera en fait à la mesure dans laquelle un juge estimera que la déclaration du témoin entendu est fiable et convaincante ; en outre, les affirmations du témoin pourraient bien être contestées par un autre témoin (expert) appelé à comparaître par la défense. En vue de trancher, un juge doit pouvoir comprendre la déposition et de surcroît être convaincu que le témoin expert est véritablement un expert. Il est par conséquent conseillé aux experts de s'exprimer en utilisant des phrases claires et simples, et de répondre de manière compréhensible aux questions qui leur sont posées. Dans le but d'éviter des contentieux superflus et fastidieux concernant le niveau d'expertise présumé d'un témoin expert, il est recommandé aux pays de mettre au point des mécanismes qui contribuent à la rationalisation des procédures de recours aux experts témoins près les tribunaux. En dépit des difficultés que cela comporte, un exemple pourrait être la création d'une liste (inter)nationale de témoins experts accrédités et qualifiés dans un domaine donné. Outre l'accréditation et la certification des experts, il pourrait être utile de normaliser la manière dont certains types de preuves doivent être interprétés. Il est recommandé aux pays de coopérer avec l'ISO afin de déterminer pour quelles autres catégories de preuve à haut niveau de technicité il serait possible de procéder à une normalisation, par exemple les preuves médico-légales. Une autre pratique à promouvoir dans les affaires les plus complexes serait celle de procéder, avant l'ouverture du procès, à un échange des rapports d'expertise entre la défense et le ministère public. Cela permettrait de détecter et de débattre de tous les points de désaccord au préalable, et de ne les présenter au tribunal que plus tard. D'autant que lorsque les experts se rencontrent et sont en mesure de débattre des points de désaccord, ces derniers ont tendance à s'amoindrir, voire à disparaître complètement.