Pratiques comparées concernant l'utilisation d'informations recueillies dans des zones de conflit comme preuves dans le cadre de procédures pénales

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Pratiques comparées concernant l'utilisation d'informations recueillies dans des zones de conflit comme preuves dans le cadre de procédures pénales

Conseil de l'Europe

La présente publication est le fruit d'une collaboration entre le Comité de lutte contre le terrorisme du Conseil de l'Europe (CDCT) et l'Institut International pour la Justice et L'Etat de Droit (IIJ), avec le soutien du Département d'Etat des Etats-Unis. Elle reflète les pratiques à partir d'informations recueillies dans les zones de conflit des Etats membres et observateurs du Conseil de l'Europe, informations qui ont été aimablement fournies par les autorités nationales.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Édition anglaise :
Comparative Practices on the Use of Information Collected in Conflict Zones as Evidence in Criminal Proceedings

Les points de vue exprimés dans cet ouvrage n'engagent que le ou les auteurs et ne reflètent pas nécessairement la ligne officielle du Conseil de l'Europe.

Toute autre correspondance relative à ce document doit être adressée Direction générale droits humains et Etat de droit, Division pour la lutte contre le terrorisme, Conseil de l'Europe, F-67075 Strasbourg Cedex France.

E-mail: DGI-CDCT@coe.int

Conception de la couverture et mise en page : Service de la production des documents et des publications (SPDP), Conseil de l'Europe

Photos: Shutterstock

Cette publication n'a pas fait l'objet d'une relecture typographique et grammaticale de l'Unité éditoriale de la DPDP.

Table des matières

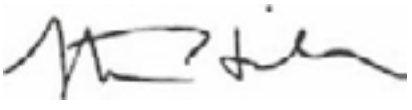
Avant-propos

Cet ensemble de Pratiques comparatives a été élaboré dans le cadre d'un partenariat entre le Comité du Conseil de l'Europe de lutte contre le terrorisme (CDCT) et l'Institut international pour la Justice et l'État de droit (IIJ), avec le soutien des États-Unis d'Amérique. Notre objectif était de fournir des conseils pratiques aux praticiens pour les aider dans les enquêtes et les poursuites des crimes de terrorisme et d'autres crimes, y compris les violations du droit international humanitaire commises dans le contexte des conflits armés. En tirant parti de l'expertise unique et du rayonnement du Conseil de l'Europe et de l'IIJ, nous avons cherché à atteindre cet objectif en rassemblant les nombreuses ressources existantes sur l'utilisation des informations collectées dans les zones de conflit afin de fournir des orientations actuelles basées sur des exemples de cas pour faire progresser de manière significative la responsabilité et la justice.

Dans les Pratiques comparatives, les praticiens trouveront des réponses à des questions importantes, telles que le type d'informations qui peuvent être disponibles dans de tels cas, où l'on peut chercher des informations à la fois au niveau national et international, et comment ces informations devraient être vérifiées et ensuite présentées au tribunal. En décrivant ces implications très pratiques de l'utilisation des informations collectées par certains acteurs du secteur non lié à la justice pénale, tels que l'armée, les Pratiques comparatives fournissent également une feuille de route pour toute considération de politique publique qui pourrait être justifiée dans certaines juridictions.

Nous tenons à exprimer notre profonde gratitude aux contributeurs qui ont partagé leur expérience de l'utilisation d'informations collectées dans des zones de conflit, à nos équipes respectives pour leurs efforts inlassables et au Bureau de la lutte contre le terrorisme du Département d'État des États-Unis pour le soutien apporté à ce projet.

M. Carlo Chiaromonte
Coordinateur du Conseil de l'Europe
de lutte contre le terrorisme



M. Steven Hill
Secrétaire exécutif de l'IIJ

Résumé

Identifier, récupérer et partager des informations recueillies dans des zones de conflit pour les utiliser comme preuves dans des affaires de terrorisme : en la matière, plusieurs États membres du Comité du Conseil de l'Europe de lutte contre le terrorisme (CDCT) ont acquis une grande expérience. Les Pratiques comparées présentées ici sont le fruit du travail du Secrétariat du CDCT et de l'Institut international pour la justice et l'État de droit (IIJ), qui ont œuvré en partenariat à rassembler les méthodes et les pratiques des États membres en une seule ressource à l'attention des praticiens, des décideurs et de toutes les personnes intéressées.

Les Pratiques comparées se fondent sur la Recommandation CM/Rec(2022)8 du Comité des Ministres aux États membres sur l'utilisation d'informations recueillies dans des zones de conflit comme preuves dans le cadre de procédures pénales relatives à des infractions terroristes. Elles offrent des orientations pratiques sur l'utilisation des informations recueillies dans des zones de conflit comme preuves dans des procédures pénales, au service de la justice et de la lutte contre l'impunité et dans le respect de l'État de droit et du droit international et national, notamment celui des droits humains.

Ce résumé offre un aperçu des principales considérations détaillées dans le document. En outre, l'annexe Questions fréquemment posées par les praticiens (FAQ) répond à un certain nombre de questions générales que les praticiens peuvent se poser sur les informations provenant des zones de conflit.

1. Sources et types d'informations

Beaucoup d'États, dans des procédures pénales concernant des infractions terroristes, ont déjà produit comme preuves des informations provenant de zones de conflit. Ces informations sont de nature très variée et proviennent de différentes sources.

Les **sources d'informations potentielles** sont les suivantes :

- **institutions nationales**, notamment l'armée, les services de renseignement et les acteurs de la justice pénale ordinaire ;
- **institutions étrangères et mécanismes intergouvernementaux** de conservation et de partage des informations (par exemple les bases de données d'Interpol, de l'Union européenne et d'Operation Gallant Phoenix) ;
- **acteurs multilatéraux** (par exemple les tribunaux internationaux et les mécanismes des Nations Unies) ;
- **acteurs non gouvernementaux** (organisations de la société civile, universitaires, chercheurs et experts, média d'information, entreprises privées, etc.).

La **typologie** est vaste, comprenant entre autres des informations :

- **matérielles** (armes, composants d'engins explosifs improvisés, téléphones portables, disques durs et autres supports de stockage, etc.) ;
- **numériques** (communications écrites, photos et vidéos, données de trafic et autres données électroniques telles que les informations sur les portefeuilles de cryptomonnaies) ;
- **sur papier** (documents manuscrits ou imprimés) ;
- **interceptées** depuis des communications téléphoniques ou autres – ou **générées** par imagerie **satellite** ou par **drones ;**
- **déclarations et témoignages** (par exemple les déclarations faites volontairement par les accusés ou par d'autres personnes interrogées ainsi que les témoignages, déclarations et autres informations fournies par des témoins, victimes, informateurs et autres personnes).

2. Mécanismes permettant d'accéder aux informations et de les partager

Pour accéder à des informations provenant de zones de conflit et les partager à des fins de justice pénale, les États ont déjà eu recours à différents mécanismes.

Ils cherchent, selon différentes modalités, **à se coordonner et à partager des informations au niveau national**.

- **Cadres juridiques nationaux :** certains services[1] militaires et de renseignement jouissent d'un large mandat qui leur permet de partager des informations avec l'autorité judiciaire, tandis que d'autres sont habilitées à le faire – et en ont même parfois l'obligation – en vertu de dispositions juridiques précises. Les services « à double casquette », assumant à la fois des fonctions répressives et de renseignement, peuvent faciliter la circulation des informations parmi les agences étatiques ou avec les partenaires internationaux.
- **Mécanismes de coordination interagences[2] :** les États ont désigné des chargés de liaison, mis en place des mécanismes permanents pour élargir la coordination entre agences, et/ou créé, lorsque cela s'avère nécessaire, des groupes de travail ponctuels.
- **Procédures de déclassification :** les États ont également adopté des procédures formelles permettant de déclassifier des informations à des fins de justice pénale.
  - Typiquement, l'entité qui a classifié les informations secrètes est réputée les « détenir » et c'est à elle que revient, en dernier ressort, la décision de les déclassifier. Certains États ont également mis en place des organes consultatifs, habilités à accéder aux informations et à livrer des avis sur l'opportunité de les déclassifier.
  - Face au problème, fréquemment pointé du doigt, de la confidentialité excessive, un État a décidé que les éléments et objets collectés par l'armée dans des zones de conflit devaient être présumés non classifiés – contrairement aux sources et aux méthodes de collecte sensibles, qui restent secrètes.

Les États suivent différentes **approches pour obtenir des informations de sources étrangères**.

- **Coordination informelle :** les praticiens commencent souvent par contacter de manière informelle leurs homologues à l'étranger.
- **Conditions à la communication d'informations :** les États appliquent généralement la « règle du tiers service » ou le « principe du contrôle par le détenteur », c'est-à-dire qu'une agence étatique ayant reçu des informations d'un État étranger s'abstient de les transmettre à un tiers ou de les divulguer sans l'autorisation de l'entité étrangère qui les a fournies.
- **Partage d'informations par les voies policières ou judiciaires officielles :** souvent, le partage d'informations avec des partenaires étrangers se fait initialement – et parfois exclusivement – via les canaux officiels entre services répressifs ou de renseignement. Lorsque ces canaux ne suffisent pas ou lorsque la législation nationale l'impose, les États recourent aux demandes formelles d'informations : les processus d'entraide judiciaire et la décision d'enquête européenne sont des outils éprouvés dans ce cadre. De nombreux États ont recours, parfois successivement, à l'ensemble des approches évoquées ci-dessus, en fonction de la nature et des nécessités du dossier.
- **Bases de données intergouvernementales :** les bases de données d'Interpol, les systèmes d'information Schengen et Europol (Union européenne) et l'Operation Gallant Phoenix se sont tous avérés des sources précieuses d'informations initialement recueillies dans des zones de conflit.
- **Coordination avec des acteurs multilatéraux :** plusieurs États ont pris l'initiative de se coordonner avec les acteurs multilatéraux présents sur les zones de conflit et susceptibles d'avoir collecté des informations pertinentes. Ce sont notamment l'Équipe d'enquêteurs des Nations Unies chargée d'amener Daech/l'État islamique d'Iraq et du Levant à répondre de ses crimes, le Mécanisme international, impartial et indépendant sur la Syrie et la Cour pénale internationale – certains de ces mécanismes ayant l'obligation de conserver et de partager les informations qu'ils ont collectées.

Les États ont aussi **obtenu des informations auprès d'acteurs non gouvernementaux** :

1. Le terme « service » fait référence à tous les services, agences ou départements gouvernementaux concernés ayant des fonctions militaires et/ou de renseignement.
2. L'expression « coordination interagences » désigne la coordination entre des services, agences ou départements gouvernementaux distincts.

- Plusieurs États ont mis en place des canaux de communication avec la société civile et d'autres organisations non gouvernementales, des journalistes et d'autres acteurs privés présents dans des zones touchées par des conflits, et les incitent à partager des informations.

3. Étapes de l'analyse et de l'utilisation des informations

Les pays suivent une série d'étapes en vue d'apprécier la valeur probante des informations provenant de zones de conflit, de faciliter leur utilisation dans des procédures pénales, d'orienter les enquêtes, d'appuyer le processus juridique ou de pouvoir les présenter comme preuves devant un tribunal.

Lors de l'utilisation d'informations recueillies dans des zones de conflit comme preuves dans le cadre de procédures pénales relatives à des infractions terroristes menées par des juridictions civiles, **les États reconnaissent l'importance d'agir conformément aux exigences de la Convention européenne des droits de l'homme**, en particulier le droit à un procès équitable tel que prévu à l'article 6, ainsi qu'aux **autres normes internationales applicables en matière de droits humains**.

Les **praticiens** ayant obtenu des informations en provenance de zones de conflit **commencent par évaluer leur valeur probante potentielle, avant de déterminer les étapes suivantes**.

- Les informations sont habituellement exploitées pour **ouvrir des pistes d'enquête ou trouver des preuves supplémentaires** ; les éléments peuvent servir à ouvrir des pistes d'enquête indépendamment de leur admissibilité en justice.
- Lorsque les praticiens constatent que les informations seraient précieuses pour des enquêtes ouvertes à l'étranger, les États **peuvent prendre l'initiative de les partager avec les autorités du pays concerné**, mais c'est assez rare étant donné le **volume** des informations collectées et leur caractère **classifié**.

Dans la plupart des codes de procédure pénale, aucune disposition n'empêche d'utiliser comme preuves des informations collectées dans des zones de conflit. Les États utilisent divers mécanismes et procédures pour **conférer à ces informations le statut de preuves** tout en **ménageant les enjeux de sécurité nationale**, notamment les sources et les méthodes de collecte, et en **respectant les garanties d'un procès équitable**.

- Dans de nombreux pays, ces informations peuvent être soumises comme preuves après une **déclassification formelle**, une **certification par l'entité détentrice** et/ou des **coupes pratiquées dans le texte par les services répressifs**.
- Lorsque des informations ne peuvent être entièrement déclassifiées, les autorités recourent à une **déclassification partielle, au moyen de versions expurgées et/ou synthétisées**, et invoquent les enjeux de sécurité pour justifier la **non-divulgation de certains éléments**.
- Certains codes de procédure pénale autorisent le **huis clos sélectif** lorsqu'il est nécessaire pour protéger des informations ou écarter d'autres risques pour la sécurité.
- Comme protection supplémentaire, il arrive que des tribunaux demandent au procureur et au conseil de la défense d'obtenir une **habilitation de sécurité avant d'obtenir l'accès à des informations sensibles**.

Les praticiens utilisent **diverses techniques** pour expliquer l'importance des informations recueillies dans des zones de conflit, décrire le contexte de leur collecte, attester de leur intégrité et de leur chaîne de conservation et, plus généralement, **corroborer leur authenticité et leur fiabilité et/ou confirmer leur valeur probante**. Parmi ces techniques :

- **réanalyser et réexploiter les objets matériels originaux ; utiliser des copies** ou des descriptions lorsque les originaux ne sont pas disponibles, et **inclure des informations sur le contexte**, par exemple l'historique officiel des processus de traitement, de transmission, de stockage, d'analyse et de partage.
  - Les États ont également élaboré des politiques et des procédures et entrepris d'organiser des formations pour améliorer les processus en question ;
- **identifier et présenter des éléments supplémentaires** issus de sources indépendantes, à la fois pour recouper la teneur des informations recueillies dans la zone de conflit et pour appuyer les charges à prouver ;
- **présenter des témoignages concordants**, non seulement des acteurs ayant collecté les informations, mais aussi de hauts responsables et de techniciens spécialisés des institutions nationales concernées, d'universitaires, experts et chercheurs, de victimes, de réfugiés ou d'anciens combattants terroristes étrangers et autres témoins « de l'intérieur » capables d'éclairer l'importance des informations.

- Les États utilisent aussi des **mécanismes procéduraux**, comme le fait de masquer les témoins à la vue ou de déformer leur voix, l'anonymat et/ou les dépositions hors prétoire pour **protéger les témoins vulnérables ou sensibles** lorsque nécessaire.

Les informations recueillies dans les zones de conflit sont également utilisées de manière déterminante dans des domaines autres que le terrorisme, tels que **les crimes de guerre, les crimes contre l'humanité et le génocide**. Les affaires de crimes internationaux peuvent s'accompagner d'exigences renforcées en matière de preuves, exigences que les informations recueillies dans des zones de conflit peuvent contribuer à remplir.

Les informations recueillies dans des zones de conflit vont conserver une importance cruciale dans les affaires de terrorisme, ainsi que pour la poursuite des auteurs d'actes contraires au droit international humanitaire et d'autres infractions, et **les pouvoirs publics devraient donc continuer de renforcer la coopération internationale et la coordination interne sur la communication et l'utilisation effectives de ces informations**, dans l'intérêt de la justice et de la lutte contre l'impunité.

Introduction

Objectif principal du document, public visé, sources, et définitions des termes clés (« informations », « preuves », « zone de conflit ») d'après la Recommandation CM/Rec(2022)8.

L'efficacité des enquêtes et des poursuites dans les affaires de terrorisme suppose que les professionnels de la justice pénale aient accès à suffisamment de preuves fiables, pertinentes et pouvant être présentées à un tribunal. **Étant donné le nombre de groupes terroristes actifs dans des zones de conflit ou ayant des rapports avec ces zones, les informations qui en proviennent sont cruciales** pour de nombreuses enquêtes et poursuites. Les praticiens de la justice pénale doivent donc savoir à la fois comment obtenir de telles informations et comment les analyser, s'assurer de leur fiabilité et de leur authenticité, confirmer leur valeur probante et les présenter comme éléments de preuve devant une juridiction nationale dans le respect des droits humains, de l'État de droit et des lois et réglementations nationales.

Plusieurs États membres du Comité du Conseil de l'Europe de lutte contre le terrorisme (CDCT) (ci-après : « les États[3] »), ayant déjà poursuivi des individus accusés d'infractions terroristes dans des zones de conflit, **ont une grande expérience en la matière,** s'agissant notamment **d'identifier de telles informations, y accéder, les diffuser et les utiliser comme preuves dans une procédure pénale**. Ces États ont mis au point des méthodes effectives, variées et adaptées au contexte pour obtenir, analyser, authentifier et présenter ce type d'informations. **Le but de ces Pratiques comparées est de rassembler ces expériences et méthodes en un seul document** pour pouvoir les partager avec les professionnels de la justice et d'autres parties prenantes dans les différents États.

Ces Pratiques comparées ont été **élaborées par le Secrétariat du CDCT** en partenariat avec l'**Institut international pour la justice et l'État de droit (IIJ)**. Elles s'**appuient sur la Recommandation CM/Rec(2022)8 du Comité des Ministres** aux États membres sur l'utilisation d'informations recueillies dans des zones de conflit comme preuves dans le cadre de procédures pénales relatives à des infractions terroristes (ci-après « CM/Rec(2022)8 » ou « la Recommandation »). Elles prennent en compte les normes et bonnes pratiques internationales, les expériences des États membres et observateurs du Conseil de l'Europe et des grandes institutions internationales spécialisées, et les recommandations antérieures du CDCT.

Bien qu'il existe plusieurs autres sources d'orientation pertinentes sur ce sujet (voir la section « Questions fréquemment posées par les praticiens (FAQ) » en annexe), ces Pratiques comparées n'ont cependant pas la même étendue, les mêmes sources et le même but que ces publications.

- **Étendue :** elles se concentrent sur les infractions pénales liées aux zones de conflit, mais couvrent toutes les sources potentielles d'informations dans ces zones (sans se limiter aux forces armées).
- **Sources :** elles reposent principalement sur les informations transmises par les autorités compétentes des États en réponse à un questionnaire détaillé envoyé par le Secrétariat en 2020 et 2023 (ci-après : « le questionnaire »). Elles puisent aussi dans les connaissances personnelles et institutionnelles des membres du CDCT-CZ (Groupe de travail du CDCT sur l'utilisation des informations collectées dans les zones de conflit comme preuves aux fins de poursuite pénale des infractions terroristes).
- **But :** elles présentent des cas et des exemples concrets, dans le contexte des procédures pénales ordinaires. Elles offrent aux enquêteurs, procureurs, responsables politiques et autres parties prenantes des orientations pratiques sur l'utilisation des informations collectées dans les zones de conflit comme preuves dans des procédures pénales, au service de la justice et de la lutte contre l'impunité et dans le respect de l'État de droit et du droit international et national, notamment celui des droits humains.

3. Sauf indication contraire, le mot « États » avec une majuscule désigne les États qui sont membres du Comité du Conseil de l'Europe de lutte contre le terrorisme, qu'ils soient membres ou membres observateurs du Conseil de l'Europe.

Définitions : dans ces Pratiques comparées comme dans la Recommandation, on entend par :

- « preuves », toute information conforme aux règles juridiques en matière de preuve des États membres, telles qu'elles sont établies dans leur droit pénal national et qui est utilisée dans une procédure judiciaire pour confirmer ou infirmer l'existence d'une infraction pénale présumée ;
- « informations », la preuve dans sa forme brute originale ; ce terme renvoie aux objets matériels ou immatériels recueillis dans une zone de conflit ;
- « zone de conflit », une zone touchée par un conflit armé, ou se relevant tout juste d'un conflit ou se trouvant dans une situation à haut risque, où des infractions liées au terrorisme ont été commises.

Ces définitions des notions de « preuves », d'« informations » et de « zone de conflit » ne s'appliquent que dans le contexte de la Recommandation et des présentes Pratiques comparées. Les États membres du Conseil de l'Europe ne sont pas tenus d'adopter les mêmes définitions en droit national.

Le présent document utilise de manière interchangeable les termes « infractions terroristes » et « infractions liées au terrorisme » pour désigner tout l'éventail des infractions pénales qui peuvent avoir un rapport avec le terrorisme dans la législation nationale, dont la planification ou la perpétration d'attentats, l'appartenance ou le soutien matériel à des groupes terroristes spécifiques et le financement du terrorisme. Comme observé au chapitre VII de la Recommandation et au chapitre 3.5 de ces Pratiques comparées, les informations recueillies dans des zones de conflit peuvent aussi servir à prouver d'autres infractions, dont les actes interdits en vertu du droit international humanitaire.

1. Informations recueillies dans des zones de conflit : sources et typologie

Les réponses au questionnaire diffusé en 2020 montraient que, à cette date, une majorité d'États (18 sur les 29 ayant répondu[4]) avaient déjà utilisé des informations obtenues dans des zones de conflit comme preuves dans des procédures pénales relatives à des infractions terroristes. Deux États au moins parmi ceux qui n'avaient pas signalé cette expérience en 2020 ont utilisé ce type d'informations depuis. Presque tous les autres États n'ayant pas signalé d'expérience en 2020 ont expliqué qu'ils n'avaient pas encore eu à traiter d'affaires de terrorisme dans lesquelles des informations recueillies dans des zones de conflit auraient présenté un intérêt, mais qu'ils pourraient utiliser ce type d'informations comme preuves si le besoin s'en présentait. En outre, en réponse au questionnaire supplémentaire diffusé en 2023, plusieurs États qui n'avaient pas répondu à celui de 2020 ont signalé avoir eux aussi utilisé des informations issues de zones de conflit dans des affaires de terrorisme. Dans l'ensemble, cela indique qu'à ce jour, au moins 22 des États interrogés ont utilisé des informations provenant des zones de conflit dans des affaires liées au terrorisme.

Les informations que les États ont utilisées sont de nature très variée et proviennent de différentes sources. Le chapitre 1 est consacré aux sources potentielles et aux types d'informations pouvant être recueillies dans les zones de conflit.

1.1. Sources d'informations

Éventail des sources d'informations concernées : institutions nationales, institutions d'autres pays, mécanismes de conservation et de partage des informations entre pays, acteurs multilatéraux et acteurs non gouvernementaux.

1.1.1. Sources nationales

Il appartient généralement aux acteurs de la **justice pénale ordinaire** de collecter des preuves ; or, il est rare qu'ils aient accès aux scènes de crime potentielles dans des zones de conflit ou qu'ils jouissent des autorisations et des capacités nécessaires pour y collecter des informations (comme le montre l'exemple de la Syrie et, dans une large mesure, de l'Irak). Par ailleurs, d'autres acteurs – principalement les **armées** et les **services de renseignement** – sont souvent présents dans ces zones et bien que n'agissant généralement pas dans un cadre judiciaire, ils collectent régulièrement d'importants volumes d'informations pertinentes pour leurs propres missions. Bien qu'initialement recueillies à des fins militaires ou de renseignement, ces informations peuvent s'avérer cruciales pour les procédures pénales relatives aux actes terroristes commis dans ces zones difficiles à atteindre[5].

4. Les 29 réponses reçues au total ne comprennent pas la Russie, qui n'est plus membre du Conseil de l'Europe.
5. Voir CM/Rec(2022)8, chapitre III – Informations recueillies par le personnel militaire, par. 6, et chapitre IV – Informations recueillies par les services de renseignement, par. 11. Dans leurs réponses au questionnaire de 2020, 10 États ont signalé avoir utilisé comme preuves des informations de sources militaires, et au moins 10 – sans compter un État qui a affirmé « ne pas avoir la liberté de répondre » à cette question – ont signalé avoir utilisé des informations provenant des services de renseignement. Toutefois, le questionnaire n'invitait pas les États à distinguer, dans leurs réponses, les informations issues de leurs propres armées et agences de renseignement de celles issues d'armées et d'agences étrangères.

1.1.2. Sources officielles étrangères et mécanismes de partage entre pays

Des informations essentielles pour les enquêtes pénales peuvent aussi être obtenues auprès de pouvoirs publics étrangers et de bases de données multilatérales. Comme rappelé dans le préambule de la Recommandation, les enquêtes et les poursuites pour infractions terroristes présumées revêtent souvent un caractère transnational qui rend la coopération entre États membres nécessaire. Les efforts des États pour traduire en justice les membres de l'autoproclamé « État islamique en Irak et au Levant » (EIIL ou Daech, ci-après : « EI ») l'ont particulièrement bien illustré. Depuis 2014, on estime que plus de 40 000 combattants terroristes étrangers, en provenance de 120 pays différents, ont été attirés par l'EI dans les territoires sous son contrôle en Irak et en Syrie[6]. Après le renversement de l'EI par une coalition internationale de 80 pays, beaucoup de ces combattants ont quitté ces territoires pour leur pays d'origine ou un autre pays, tandis que d'autres sont encore détenus dans des camps et des prisons en Syrie et en Irak, représentant une menace permanente.

Comme l'a mis en lumière l'expérience de la lutte contre l'EI, à l'heure de demander des comptes aux combattants terroristes étrangers et aux autres auteurs d'infractions terroristes, les informations recueillies par le personnel **répressif, militaire ou de renseignement** d'un État sont souvent très précieuses pour les procès engagés **dans d'autres pays**.

Les bases de données gouvernementales, qui réunissent parfois des données issues de différents types d'agences, constituent une ressource essentielle pour le partage d'informations au-delà des frontières. Par exemple, le FBI (Federal Bureau of Investigation, États-Unis) a créé en 2003 le **TEDAC (Terrorist Explosive Device Analytical Center)**, qui répertorie les détonateurs, composants de bombes et engins explosifs improvisés saisis sur des théâtres d'opération à l'étranger par le personnel militaire et civil étasunien, mais aussi remis par des pays tiers. Le TEDAC exploite méthodiquement ces objets pour déterminer leur fonctionnement, l'origine de leurs composants et les traces d'ADN et autres susceptibles de les relier à des individus.

Autre source importante, les mécanismes intergouvernementaux de stockage et de partage des informations obtenues par différents États. **Interpol** gère de nombreuses bases de données. Par exemple, la base **Project Watchmaker**, créée en 2014, répertorie l'identité et/ou la méthodologie de milliers de fabricants ou fabricants présumés d'engins explosifs improvisés. Les États membres de l'Union européenne ont aussi accès aux informations que d'autres États membres ont obtenues et enregistrées dans le **système d'information Schengen**, ainsi que dans d'autres fichiers comme le **système d'information Europol** et **Eurodac** (relevés d'empreintes digitales des demandeurs d'asile).

L'**Operation Gallant Phoenix (OGP)**, initiative interagences et multinationale lancée par les États-Unis en 2014 pour lutter contre les organisations extrémistes violentes, a joué un rôle particulièrement marquant dans la diffusion internationale d'informations issues de zones de conflit. L'OGP gère une énorme base d'éléments récoltés en Irak, en Syrie et dans d'autre zones de conflits. De nombreux États ont qualifié les informations issues de l'OGP de cruciales pour leurs enquêtes sur les crimes commis par l'EI et par d'autres organisations terroristes dans ce pays et pour la poursuite de leurs auteurs.

1.1.3. Acteurs multilatéraux

En outre, des entités multilatérales présentes dans des zones de conflit recueillent des informations qui peuvent s'avérer précieuses pour les affaires de terrorisme.

Dans sa Résolution 2379 (2017), le Conseil de sécurité de l'ONU a prié le Secrétaire général de constituer une Équipe d'enquêteurs à l'appui des efforts engagés à l'échelle nationale pour amener l'EI à rendre des comptes « en recueillant, conservant et stockant des éléments de preuve en Iraq d'actes susceptibles de constituer des crimes de guerre, des crimes contre l'humanité et des crimes de génocide perpétrés par le groupe terroriste […] en Iraq, […] pour que ces preuves puissent être utilisées le plus largement possible devant les tribunaux nationaux, et en complétant les enquêtes menées iraquiennes, ou […] par les autorités de pays tiers à leur demande[7] ». Depuis sa création, cette **Équipe d'enquêteurs des Nations Unies chargée d'amener Daech/l'État islamique d'Iraq et du Levant à répondre de ses crimes (UNITAD)** a rassemblé un énorme volume

6. Voir le Rapport explicatif de la Recommandation CM/Rec(2022)8, par. 20.
7. Résolution 2379 (2017) du Conseil de sécurité, par. 2.

de données potentiellement précieuses pour les procédures concernant cette organisation terroriste. Elle a, entre autres, numérisé plus de 8 millions de pages de documents de l'EI[8].

En outre, le **Mécanisme international, impartial et indépendant sur la Syrie** a rassemblé des données qui pourraient être tout aussi précieuses et qu'il est habilité à partager, comme l'UNITAD. Et d'autres acteurs multilatéraux, dont la **Commission d'enquête internationale indépendante sur la République arabe syrienne**, gèrent des bases de données similaires.

1.1.4. Acteurs non gouvernementaux

Enfin, il n'est pas à exclure que des informations recueillies dans les zones de conflit, pour leur propre usage, par différents acteurs privés aient force probante devant la justice ordinaire. La Recommandation et les réponses au questionnaire mentionnent ici les organisations de la **société civile** et autres **organisations non gouvernementales (OSC/ONG)**, les **universitaires et experts**, les **média d'information** et les **entreprises et prestataires privés**. La majorité des États ayant répondu au questionnaire signalent avoir utilisé des éléments de preuve recueillis par ce type de sources non gouvernementales dans des zones de conflit pour poursuivre des terroristes présumés.

1.2. Types d'informations

Typologie des informations recueillies dans les zones de conflit : matérielles, numériques, sur papier, interceptées, générées par satellite ou drone, humaines.

1.2.1. Matérielles

Le large éventail des objets récupérés dans les zones de conflit comprend généralement des **armes**, des **composants d'engins explosifs improvisés**, des **téléphones portables**, des **disques durs et d'autres supports de stockage**. Plusieurs bases de données nationales et internationales – dont certaines sont évoquées plus haut, comme les bases TEDAC et Project Watchmaker – conservent, stockent et analysent des types spécifiques d'éléments matériels.

1.2.2. Numériques

Les informations peuvent aussi prendre la forme de **données numériques**, notamment **communications écrites, photos et vidéos, données de trafic** et autres données électroniques telles que les **informations sur les portefeuilles de cryptomonnaies**. Comme pour les éléments matériels, plusieurs bases de données nationales et internationales sont consacrées à la conservation, au stockage et à l'analyse de ces données.

1.2.3. Sur papier

On peut aussi trouver dans les zones de conflit d'énormes volumes de **documents sur papier**, qu'ils soient **imprimés ou manuscrits :** notes personnelles, courriers, journaux, registres officiels ou quasi-officiels. Pour asseoir son projet politique, à savoir la création d'un « État » autoproclamé, l'EI a ainsi produit des masses de récépissés et autres documents administratifs. Les documents récupérés en lien avec l'EI sont variés : fiches d'enrôlement, listes d'inscription dans différents groupes, états de service des combattants, bulletins de paie, quittances de loyer, attestations fiscales, certificats de naissance et de décès, etc.

1.2.4. Interceptées et générées par satellite ou drone

Différents acteurs étatiques **interceptent** dans les zones de conflit, à des fins judiciaires ou dans le cadre de leurs propres missions, **des communications téléphoniques et autres** qui peuvent contenir des informations pertinentes pour les enquêtes et les poursuites dans des affaires de terrorisme. En outre, étant donné la difficulté d'accéder au terrain, la force probante des **prises de vues par satellite ou par drone** n'est pas à négliger.

8. Lettre adressée le 22 mai 2023 au président du Conseil de sécurité par le Conseiller spécial et chef de l'Équipe d'enquêteurs des Nations Unies chargée d'amener l'EIIL/Daech à répondre de ses crimes. Il convient de noter que dans la résolution 2697 (2023), le Conseil de sécurité des Nations Unies n'a prorogé le mandat de l'UNITAD que jusqu'au 17 septembre 2024, de sorte que, si les informations de l'UNITAD ont été précieuses à des fins d'enquêtes et de poursuites, en avril 2024, il reste à déterminer si les États auront accès à ces informations pour leurs affaires à l'avenir. Voir la section 2.2.5.

1.2.5. Déclarations et témoignages

Enfin, les déclarations faites volontairement par les accusés ou par d'autres personnes interrogées ainsi que les **témoignages**, **déclarations** et **autres informations** fournies par des **témoins, victimes, informateurs et autres personnes** peuvent aussi s'avérer précieuses.

2. Mécanismes permettant d'accéder aux informations et de les partager

Pour accéder à des informations provenant de zones de conflit et les partager à des fins de poursuite pénale, les États ont déjà eu recours à différents mécanismes[9]. Les praticiens n'étant pas nécessairement au courant des informations pertinentes disponibles, ils devront d'abord faire une demande de recherche d'informations auprès d'agences gouvernementales locales ou étrangères, de mécanismes intergouvernementaux, ou d'acteurs multilatéraux et non gouvernementaux.

2.1. Coordination et partage des informations au niveau national

Mécanismes juridiques et procéduraux utilisés par les États pour solliciter ou autoriser le partage des informations, améliorer la coordination entre agences nationales et déclassifier les informations, le cas échéant.

2.1.1. Cadres juridiques nationaux

Le large mandat dont bénéficient certains services militaires et de renseignement les autorise à partager des informations provenant de zones de conflit avec d'autres institutions nationales ou étrangères. Dans d'autres cas, la réglementation confère à l'entité l'autorisation, et parfois même l'obligation, de partager des informations. Les dispositions pertinentes peuvent être inscrites dans le code de procédure pénale et/ou dans les statuts des agences non répressives concernées. Pour plus de clarté, certaines législations autorisent expressément cette communication d'informations – voire la rendent obligatoire, dans le cas d'une communication entre agences nationales –, soit à l'initiative de ces agences, soit à la demande d'une autorité judiciaire.

En Allemagne, par exemple[10], le Code de procédure pénale autorise les procureurs et la police à demander à toutes les autres autorités publiques, y compris militaires et de renseignement, des informations susceptibles de faire progresser les enquêtes sur des soupçons d'infractions pénales. Dans les affaires de terrorisme, le procureur général fédéral demande régulièrement des informations non seulement à l'Office fédéral de police criminelle, mais aussi aux services nationaux de renseignement et à d'autres agences publiques du pays. Les services de renseignement, pour leur part, ont l'*obligation* de communiquer au parquet les informations pertinentes si cela paraît, sur la base d'éléments factuels, nécessaire pour prévenir ou sanctionner des infractions pénales[11].

Dans plusieurs États, des **services auxquels la loi confie à la fois des missions de répression et de renseignement** peuvent faciliter de manière particulièrement efficace l'échange et l'utilisation d'informations. La Direction générale de la sécurité intérieure ou DGSI, en France, en est un excellent exemple. La coexistence au sein de la DGSI d'agents du renseignement et de la police judiciaire permet à l'autorité judiciaire française d'être avisée, après déclassification, des informations recueillies dans le cadre du renseignement, y compris dans les zones de conflit, qui peuvent présenter une utilité dans le cadre d'une enquête pénale, et de recevoir ces informations le cas échéant.

Parmi les autres services « à double casquette », on peut citer le Service de sécurité suédois, qui dispose de pouvoirs répressifs et peut partager des informations avec la police et le parquet, ainsi que le FBI.

9. Ce qui confirme le passage de la Recommandation selon lequel les États devraient « continuer à renforcer la coopération internationale et la coordination nationale en matière d'utilisation d'informations provenant de zones de conflit comme preuves aux fins de poursuites pénales d'infractions terroristes et d'autres infractions, afin d'intensifier l'échange d'informations et de bonnes pratiques. »
10. La Moldavie, tout en précisant ne jamais avoir utilisé cette possibilité dans une affaire de terrorisme, a expliqué de même que son Code de procédure pénale autorisait les services de renseignement à transmettre des informations aux procureurs.
11. La loi fédérale sur la protection de la Constitution (article 20) impose cette obligation à l'Office fédéral pour la protection de la Constitution ; des réglementations analogues s'appliquent aux autres services de renseignement.

2.1.2. Mécanismes de coordination interagences

Sur le plan procédural, les États ont constaté que la **désignation de chargés de liaison** pouvait faciliter les transferts d'informations. En République tchèque par exemple, la communication aux autorités judiciaires des informations recueillies par l'armée se fait via un service de liaison spécialisé qui, au sein de la police, sert de point de contact avec l'ensemble des services de renseignement du pays.

Plusieurs États ont également élargi la coordination, au niveau national, en créant des **mécanismes permanents** d'échange et de collaboration entre agences. C'est ainsi que l'**Allemagne** a mis en place, à Berlin, un **Centre conjoint de lutte contre le terrorisme (GTAZ)**. Spécialisé dans le recueil et l'analyse d'informations, le Centre assure des briefings quotidiens et hebdomadaires à l'attention de ses membres, à savoir l'Office fédéral de police criminelle, les agences de renseignement et de police des États allemands (les *Länder*), les agences de renseignement fédérales, l'Office d'enquête douanière, l'Office fédéral pour les migrations et les réfugiés et le Procureur général près la Cour fédérale de justice. La législation antiterroriste adoptée en 2016 par la **Pologne** a instauré un mécanisme du même type, qui permet aux services de sécurité et aux autres agences gouvernementales concernées de coopérer et de se coordonner en vue de prévenir et de réprimer les activités terroristes.

Outre ces mécanismes permanents, on trouve dans certains États, comme l'**Allemagne**, des **groupes de travail spéciaux** formés **ponctuellement** lorsqu'il faut réagir à des menaces immédiates. De même, lorsqu'une collaboration s'avère nécessaire sur des affaires pénales précises, le **Danemark** met en place des comités de pilotage réunissant les services danois de sécurité et de renseignement, la police, le parquet et d'autres acteurs concernés.

Ces mécanismes de coordination permanents et ponctuels servent de multiples objectifs. Il s'agit tout d'abord d'améliorer le travail d'enquête et de poursuites dans des affaires précises, mais aussi « la confiance mutuelle et la coopération entre l'ensemble des autorités compétentes et des services concernés[12] ». Grâce à ces mécanismes, en outre, les parties prenantes au niveau national se familiarisent avec les informations recueillies dans des zones de conflit, leur disponibilité, leur utilité et leurs sources potentielles[13]. L'Allemagne indique en effet qu'en 2020, l'ensemble des procureurs et des enquêteurs travaillant sur des affaires de terrorisme connaissaient la possibilité de demander à d'autres pays des informations recueillies par l'armée. À cette fin, quelques États ont également organisé des formations communes à différents praticiens, en vue de « renforcer leurs connaissances quant au caractère unique des preuves en question et à l'environnement exceptionnel dans lequel les acteurs concernés opèrent »[14].

2.1.3. Procédures de déclassification

Les États ont également adopté des procédures formelles permettant de déclassifier des informations à des fins de justice pénale. En effet, pour certaines juridictions, la déclassification est une condition préalable à l'utilisation comme preuve (voir le chapitre 3.4, ci-dessous[15]). Habituellement, l'**autorité à l'origine de la classification**, juridiquement considérée comme détentrice des informations, peut abaisser le niveau de classification soit d'office, soit à la demande des autorités judiciaires ; dans certains cas, seule la personne au sommet de la hiérarchie de cette autorité détentrice est habilitée à le faire.

Certains États ont mis en place des **organes consultatifs** habilités à accéder aux informations et à rendre des avis sur l'opportunité de les déclassifier. En France, l'autorité judiciaire peut solliciter à cette fin la Commission du secret de la défense nationale (CSDN). La CSDN examine les éléments, s'assure qu'ils intéressent la procédure et rend un avis motivé sur l'opportunité de les déclassifier, en prenant en considération les missions du service public de la justice, le respect de la présomption d'innocence et des droits de la défense, le respect des engagements internationaux de la France et la nécessité de préserver ses capacités de défense et la sécurité des personnels. La décision de déclassifier appartient en dernier ressort au ministère de tutelle de l'organe détenteur des informations, qui n'est pas lié par l'avis de la CSDN, mais doit le prendre en compte.

La confidentialité excessive des informations reste une difficulté couramment pointée. En 2020, s'éloignant de la politique suivie jusqu'alors, le **ministère de la Défense des États-Unis** a donné pour instruction que, à partir de ce moment-là, tous les matériels exploitables nouvellement acquis et non exploités, saisis, recueillis

12. CM/Rec(2022)8, chapitre III – Informations recueillies par le personnel militaire, par. 10.
13. Voir CM/Rec(2022)8, chapitre VIII – Coordination nationale, par. 24.
14. CM/Rec(2022)8, chapitre VIII – Coordination nationale, par. 26
15. Voir CM/Rec(2022)8, chapitre III – Informations recueillies par le personnel militaire, par. 9 et 10, et chapitre IV – Informations recueillies par les services de renseignement, par. 11 et 14.

ou utilisés par les forces armées américaines au cours d'opérations militaires puissent être présumés non classifiés à moins que des sources, des méthodes ou des activités sensibles n'aient été utilisés pour acquérir de tels matériaux[16]. Ce changement de politique a été en partie motivé par la volonté de partager plus facilement ces éléments avec les pays partenaires et de faciliter les enquêtes et les poursuites à l'encontre des personnes qui constituent une menace pour la sécurité des États-Unis et des pays partenaires.

2.2. Coopération internationale

Approches adoptées par les États pour obtenir des informations, dont – parfois par étapes successives – la coordination informelle, les communications d'informations entre forces de l'ordre et l'entraide judiciaire officielle, ainsi que la coopération sur les enquêtes via Eurojust, la coordination avec les organisations et agences internationales et la consultation de bases de données internationales.

2.2.1. Coordination informelle avec des homologues étrangers

Les acteurs de terrain indiquent que lorsqu'ils partagent des informations issues de zones de conflit avec des homologues à l'étranger, le processus a souvent commencé par un dialogue informel entre membres des forces de l'ordre ou d'autres agents publics. Dans le cadre d'une enquête en cours, un agent prend contact avec un homologue à l'étranger et apprend à cette occasion que les pouvoirs publics de l'autre pays pourraient disposer d'informations pertinentes. Les liens professionnels noués à l'occasion de collaborations précédentes, ainsi que les liens entre institutions, peuvent faciliter de tels échanges informels. Aujourd'hui, les réseaux informels jouent un rôle d'autant plus essentiel que les services répressifs connaissent mieux la force probante des différents types d'informations recueillies dans les zones de conflit, y compris numériques, et de diverses sources, y compris des services militaires et de renseignement. Les échanges internationaux d'informations et de connaissances ont alimenté et élargi ces réseaux informels, avec notamment l'organisation de réunions consacrées à des types particuliers de preuves par le Conseil de l'Europe (CDCT), l'Unité de coordination de la lutte antiterroriste de l'UE, le Forum mondial de lutte contre le terrorisme, la Section de lutte contre le terrorisme de l'Otan, le Pacte mondial de coordination contre le terrorisme (ONU) et l'IIJ.

2.2.2. Conditions à la communication d'informations

Les États appliquent généralement la règle du « **tiers service** », c'est-à-dire qu'une entité publique ayant reçu des informations d'un État étranger s'abstient de les transmettre à un tiers ou de les divulguer sans l'autorisation de l'État qui les a fournies. Ce principe du « contrôle par le détenteur » est parfois, mais pas toujours, entériné par des accords formels, et présente un intérêt pour plusieurs raisons. Non seulement cette règle favorise la confiance mutuelle, mais elle évite qu'un État, destinataire de la même information via de multiples canaux, ne croie à tort avoir reçu de sources indépendantes plusieurs éléments qui se corroborent.

2.2.3. Partage d'informations par les voies policières ou judiciaires officielles

Souvent, le partage d'informations sur les enquêtes et poursuites pour terrorisme dans un autre État se fait initialement – et parfois exclusivement – via les **canaux officiels entre services répressifs ou de renseignement**. Dans de nombreux cas, l'État destinataire peut ensuite utiliser les informations non seulement à des fins d'enquête, mais aussi comme preuves dans une procédure pénale, à moins qu'elles ne soient soumises à des conditions spécifiques et à des procédures de classification. Les services à « double casquette », tels que la DGSI française et le FBI américain mentionnés ci-dessus, peuvent faciliter ce partage international, d'autant plus que les praticiens de certains pays ne sont pas en mesure d'utiliser les informations reçues directement d'un service militaire ou d'un service de renseignement étranger à des fins de poursuite pénale.

Le dialogue entre services répressifs ou de renseignement peut suffire à convaincre l'État d'origine de déclassifier les éléments, de lever les réserves initialement attachées à leur communication ou d'en autoriser l'utilisation comme preuves. En Suisse par exemple, lorsque le Service de renseignement de la Confédération (SRC) reçoit de services étrangers des renseignements intéressants dans une affaire de terrorisme, il demande au service partenaire l'autorisation de les utiliser dans une procédure judiciaire. Au Royaume-Uni, les services répressifs recevant de pouvoirs publics étrangers des éléments ayant force probante s'efforcent, de même, d'obtenir ces éléments sous forme déclassifiée.

16. Ce principe ne s'applique toutefois pas aux objets collectés des agences de renseignement.

Dans d'autres situations, les États choisissent, ou cela peut être nécessaire, de déposer **des demandes d'entraide pénale internationale par voie diplomatique.** Des États comme l'Allemagne, l'Autriche ou les Pays-Bas considèrent l'**entraide judiciaire** comme un outil précieux. Par ce biais, les autorités compétentes peuvent parfois demander des informations obtenues initialement dans des zones de conflit, au même titre que celles obtenues ailleurs. Ce faisant toutefois, elles doivent garder à l'esprit que d'un point de vue pratique, les personnes ayant collecté les informations sont moins susceptibles de pouvoir témoigner (voir le chapitre 3.5.2, plus loin).

Au sein de l'Union européenne, l'échange d'informations est étayé par la décision 2005/671/JAI du Conseil relative à l'échange d'informations et à la coopération concernant les infractions terroristes, récemment modifiée par la directive (UE) 2023/2123.

Pour les États membres de l'UE, la **décision d'enquête européenne (DEE)** représente un autre moyen de demander la divulgation d'informations. Il s'agit d'une décision judiciaire émise ou validée par l'autorité judiciaire d'un pays de l'UE pour que des mesures d'enquête soient prises afin de recueillir ou d'utiliser des preuves dans le cadre d'affaires pénales menées dans un autre pays de l'UE[17]. Plusieurs états membres de l'UE, y compris l'Allemagne, l'Espagne et la Pologne signalent avoir utilisé ce moyen pour partager et demander de telles informations[18].

Eurojust facilite également les processus d'entraide judiciaire, y compris par le biais d'instruments de coopération judiciaire tels que la décision d'enquête européenne et les équipes communes d'enquête, permettant notamment la communication de preuves d'un pays à l'autre. Eurojust contribue également à l'utilisation plus efficace des informations provenant des zones de conflit grâce à sa coordination entre les autorités nationales, et peut fournir des conseils sur les catégories d'informations utiles aux fins de procédures pénales.

Parfois, les demandes d'entraide judiciaire et autres processus de coopération facilitent l'obtention d'informations sous forme déclassifiée et/ou non restreinte. Le Royaume-Uni signale que lorsqu'il a pu ouvrir des poursuites sur la base d'informations recueillies par des militaires et fournies par des gouvernements étrangers, les demandes d'entraide judiciaire ont conduit ces partenaires internationaux à déclassifier les informations pour qu'elles puissent servir dans la procédure[19].

Il arrive aussi que seuls soient admissibles les éléments obtenus par des voies judiciaires. En Italie par exemple, les procureurs peuvent utiliser dans les procédures pénales des informations recueillies par l'armée à condition qu'elles leur aient été transmises par la police judiciaire. Même dans les pays dont la législation peut être considérée comme plus souple sur les critères de recevabilité d'éléments de preuve, les tribunaux sont parfois plus enclins à accepter et à utiliser des informations obtenues au travers de processus formels.

De nombreux États ont recours, parfois successivement, à l'ensemble des approches évoquées ci-dessus, en fonction de la nature et des nécessités de l'affaire. Cette **approche flexible** peut commencer par un dialogue informel entre agents, se poursuivre par des échanges par des voies plus institutionnelles au sein des services répressifs ou de renseignement, et aboutir à des demandes formelles[20]. La Turquie signale, par exemple, que la coopération judiciaire internationale peut se faire en vertu d'une convention pertinente du Conseil de l'Europe, si la Turquie et l'autre pays concerné y ont adhéré ; d'un accord bilatéral, le cas échéant ; ou du principe de droit international de la réciprocité, si aucun accord ou convention n'est en vigueur. En Autriche, le *Bundesamt für Verfassungsschutz und Terrorismusbekämpfung* (Office fédéral pour la protection de la Constitution et la lutte contre le terrorisme, BVT) partage des éléments de preuve et des renseignements sur une base aussi bien bilatérale que multilatérale. Lorsqu'il y a des raisons de considérer que des informations venant des zones de conflit sont susceptibles d'être obtenues, les autorités allemandes cherchent à les obtenir auprès du pays concerné à travers une demande de la police, une décision d'enquête européenne ou une demande d'entraide judiciaire.

Un partage d'informations réussi dépend non seulement de la quantité de détails fournie par l'État demandeur sur l'infraction concernée ou sur l'individu soupçonné, mais aussi de sa capacité à convaincre l'autre État que les informations seront concrètement utiles à l'enquête et aux poursuites. Pour assurer une bonne coopération à l'avenir, beaucoup d'États jugent par conséquent crucial que les praticiens **tiennent les entités qui leur ont fourni des éléments au courant du résultat de leur démarche**, que ces éléments aient transité par des moyens de coopération internationale judiciaire ou policière.

17. Voir : https://www.eurojust.europa.eu/judicial-cooperation/instruments/european-investigation-order.
18. La directive concernant la DEE, qui établit un régime unique pour l'obtention de preuves détenues et recueillies dans un autre État membre de l'UE, s'applique à tous les États membres de l'UE qui y sont liés (l'Irlande et le Danemark ne le sont pas).
19. Ce type de communication fondée sur un traité peut bien sûr être assortie de conditions sur les usages autorisés.
20. Il peut également s'agir de demandes de recherche dans les bases de données et les systèmes d'information intergouvernementaux. Voir la section 2.2.4 ci-dessous.

2.2.4. Bases de données intergouvernementales et initiatives de partage des informations

Les États effectuent régulièrement des recherches ciblées dans des bases de données intergouvernementales, qui sont précieuses pour livrer des informations initialement collectées dans des zones de conflit.

Interpol gère une série de bases de données pertinentes en plus de Project Watchmaker, notamment centrées sur les combattants terroristes étrangers et sur les documents de voyage. Dans le cadre du **Mi-Lex (*Military-to-Law-Enforcement Exchange Programme*)**, déployé pour la première fois en Afghanistan et en Irak, Interpol a permis à ses États membres de transmettre à leurs services répressifs des informations de sources militaires, via les Plateformes de coopération en matière de sécurité (PCMS) au niveau régional et via le réseau des Bureaux centraux nationaux d'Interpol[21].

Les systèmes d'information Europol et Schengen, mentionnés au chapitre 1.1.2, sont de moins grande envergure : seuls les États membres de l'UE peuvent y intégrer des informations et y effectuer des recherches. A plusieurs occasions, des États ont fourni aux bases Europol et Schengen des informations qui se sont avérées précieuses pour les enquêtes et poursuites pour terrorisme : la France, la Hongrie et les Pays-Bas, entre autres, signalent avoir trouvé dans ces bases de données des informations issues de zones de conflit qui ont ultérieurement été utilisées comme preuves.

Les États appliquent aussi un processus éprouvé pour rechercher et obtenir des informations stockées par l'OGP (Operation Gallant Phoenix). Les États-Unis ont créé un formulaire standardisé qui permet aux États de lancer des requêtes ciblées et détaillées. Les agences sont incitées à prioriser les personnes soupçonnées dans des affaires de terrorisme et à livrer le plus d'informations possible sur les suspects absolument prioritaires : actes criminels présumés, antécédents d'activités criminelles, antécédents de voyages, rôle dans le groupe terroriste, proches et autres personnes associées. Il peut aussi être utile de préciser les chefs d'accusation éventuels et le degré d'importance de l'information pour permettre une condamnation sur cette base. Dans les ambassades des États-Unis du monde entier, les attachés juridiques du FBI assurent la liaison avec l'OGP. À travers des discussions préalables, ils aident les pouvoirs publics concernés à affiner les recherches ou demandes d'informations qu'ils envisagent et à déterminer, entre autres, si un partage via les voies judiciaires formelles est utile ou nécessaire. Ils assurent également une aide a posteriori.

Pour faciliter encore la circulation des informations, certains États ont déployé auprès de l'OGP des représentants permanents de diverses agences, y compris répressives et de renseignement. Certains États ont également jugé intéressant de désigner un point de contact national unique pour le partage des informations de sources militaires pouvant avoir force probante. En Espagne par exemple, le CITCO (*Centro de Inteligencia contra el Terrorismo y el Crimen Organizado*) fait office de point de contact national pour la coordination des échanges d'informations avec l'OGP. La désignation formelle de points de contact peut aider à clarifier quelle agence et, au sein de cette agence, quel individu doit primer dans ce processus. Elle peut aussi nourrir la mémoire institutionnelle en matière de partage international d'informations provenant de zones de conflit. Les arrangements informels, souvent personnels, évoqués plus haut peuvent être efficaces dans de nombreux cas, mais on risque de perdre ces relations ou de devoir les recréer dès que les personnes concernées quittent la fonction publique ou changent simplement de poste.

2.2.5. Coordination avec des acteurs multilatéraux

Certains États ont pris l'initiative de se coordonner avec des acteurs multilatéraux qui, présents dans des zones de conflit, sont susceptibles d'y recueillir des informations pertinentes. En France par exemple, le Parquet national antiterroriste (PNAT) peut solliciter via l'émission de demandes d'entraide pénale internationale des éléments de preuve détenues par les organes des Nations Unies, dont le Mécanisme sur la Syrie (MIII), l'UNITAD et diverses commissions d'enquête.

Beaucoup de ces entités internationales sont expressément tenues de préserver et de partager les informations qu'elles collectent. Le mandat de l'UNITAD, par exemple, affirme que « [l]'Équipe d'enquêteurs organise, catalogue, enregistre, conserve et stocke systématiquement tous éléments de preuve et autres pièces à conviction en Iraq, […] afin de garantir leur recevabilité et leur utilisation le plus large possible dans des procédures pénales régulières et indépendantes conduites par des tribunaux nationaux compétents en Iraq *et*

21. Voir Interpol, « Le G5 Sahel », https://www.interpol.int/fr/Infractions/Terrorisme/Projets-de-lutte-contre-le-terrorisme/G5-Sahel, et https://www.interpol.int/fr/Qui-nous-sommes/Les-pays-membres/Les-Bureaux-centraux-nationaux-B.C.N.

dans d'autres États conformément au droit international applicable[22] ». D'après la lettre adressée le 16 novembre 2023 à la Présidente du Conseil de sécurité par le Conseiller spécial et chef de l'Équipe d'enquêteurs, l'UNITAD a répondu aux demandes d'assistance de 20 États tiers en plus de l'Irak – et de 45 autorités compétentes dans ces pays – et prêté son concours à un nombre croissant de juridictions nationales. « La capacité de l'Équipe », écrit le Conseiller spécial, « de recueillir des témoignages en réponse directe à des demandes d'assistance, associée à l'aptitude de répertorier des documents internes de Daech/EIIL corroborant les preuves numériques du champ de bataille, a été d'un grand secours pour appuyer les enquêtes menées par les juridictions nationales[23] ». Dans la résolution 2697 (2023), le Conseil de sécurité des Nations Unies a prolongé le mandat de l'UNITAD jusqu'au 17 septembre 2024 seulement. Ainsi, bien que les informations de l'UNITAD aient été précieuses dans les enquêtes et les poursuites, en avril 2024, il reste à déterminer si les États auront accès à ces informations pour leurs affaires à l'avenir.

En 2016, l'Assemblée générale des Nations Unies a créé le Mécanisme international, impartial et indépendant sur la Syrie, chargé de se pencher sur les crimes et exactions commis sur le territoire syrien depuis mars 2011 en fonctionnant « à la fois comme un centre d'échange des informations produites au fil des ans par d'autres entités – dont la commission d'enquête, les acteurs de la société civile et les pouvoirs publics – mais aussi comme une proto-équipe d'enquête, qui recueille elle-même des informations pour combler les lacunes et préparer des dossiers en vue de futures poursuites[24] ». D'après son rapport du 14 février 2024 à l'Assemblée générale, le Mécanisme a reçu 344 demandes d'assistance de la part de 16 juridictions, « 166 [des enquêtes et poursuites concernées] ayant déjà bénéficié de l'aide du Mécanisme qui a communiqué aux juridictions concernées des informations, des éléments de preuve ou des travaux d'analyse », et a intensifié son partage volontaire d'informations avec les juges et les procureurs[25].

La Cour pénale internationale (CPI) peut aussi, dans certaines circonstances, partager des informations avec des autorités judiciaires nationales. La compétence de la Cour, qui est « limitée aux crimes les plus graves qui touchent l'ensemble de la communauté internationale », à savoir le génocide, les crimes contre l'humanité, les crimes de guerre et le crime d'agression[26], est « complémentaire des juridictions pénales nationales[27] ». L'article 93.10 du Statut de Rome habilite la CPI à appliquer ce que les juristes ont appelé la « complémentarité positive » : « Si elle reçoit une demande en ce sens, la Cour peut coopérer avec l'État Partie qui mène une enquête ou un procès concernant un comportement qui constitue un crime relevant de la compétence de la Cour ou un crime grave au regard du droit interne de cet État », assistance qui comprend notamment la « transmission de dépositions, documents et autres éléments de preuve recueillis au cours d'une enquête ou d'un procès menés par la Cour[28] ».

2.3. Informations des acteurs non gouvernementaux

Moyens de communiquer avec les ONG/OSC, les média d'information et d'autres acteurs privés et de les encourager à partager des informations.

Plusieurs États membres ont également mis en place de canaux de communication avec les ONG/OSC, les média d'information et d'autres acteurs privés afin de les encourager à partager des informations. En France, le PNAT a pu être destinataire d'éléments probatoires issus du travail d'ONG œuvrant sur les théâtres de guerre, dont la fiabilité est étroitement vérifiée par l'autorité judiciaire et qui recueillent des témoignages, collectent de la documentation diverse et prennent des photographies ou réalisent des vidéos qui peuvent constituer des éléments de preuve. Les Pays-Bas ont eux aussi établi des relations de travail avec des ONG qui documentent, en gérant des bases de données numérisées, les crimes commis en Syrie et/ou en Irak. Dans plusieurs affaires, les autorités judiciaires néerlandaises ont pu utiliser comme preuves des vidéos ou d'autres informations obtenues par ce biais.

L'Allemagne, l'Autriche, le Danemark, l'Espagne, les États-Unis, la Géorgie, la Hongrie, le Royaume-Uni et la Serbie ont également utilisé des documents, des preuves médico-légales ou des dépositions de témoins fournis par

22. https://digitallibrary.un.org/record/1472986/files/S_2018_118-FR.pdf?ln=en/.
23. Lettre datée du 16 novembre 2023, adressée à la Présidence du Conseil de sécurité par le Conseiller spécial et chef de l'UNITAD.
24. Beth Van Schaack, « Innovations in International Criminal Law Documentation Méthodologies and Institutions », 5 février 2019, disponible sur SSRN : https://ssrn.com/abstract=3329102 ou http://dx.doi.org/10.2139/ssrn.3329102.
25. Dixième rapport du Mécanisme international, impartial et indépendant chargé de faciliter les enquêtes sur les violations les plus graves du droit international commises en République arabe syrienne depuis mars 2011 et d'aider à juger les personnes qui en sont responsables, transmis par le Secrétaire général des Nations Unies dans sa lettre datée du 14 février 2024.
26. Statut de Rome de la Cour pénale internationale, art. 5.1.
27. Statut de Rome, art. 1.
28. Statut de Rome, art. 93.10.

des ONG, des entreprises privées ou des médias d'information. L'Espagne, par exemple, s'est appuyée sur des informations transmises par des journalistes pour émettre une notice rouge Interpol.

Dans l'**affaire *Mohammed Abdallah***, le Royaume-Uni a présenté comme preuve au tribunal un registre de combattants de l'EI qu'un membre du groupe ayant fait défection avait initialement transmis à Sky News. L'accusé, que le registre présentait comme *sniper* volontaire et décrivait à l'aide de détails personnels ultérieurement corroborés par la police, a été jugé coupable d'infraction terroriste et condamné à 10 ans de prison.

La **Commission for International Justice and Accountability (CIJA)**, ONG à but non lucratif qui s'attache à recueillir les preuves d'exactions commises dans des zones difficiles d'accès, figure en bonne place parmi les sources non gouvernementales d'informations en provenance de zones de conflit. Depuis 2014, les enquêteurs de terrain de la CIJA en Syrie et en Irak ont collecté « des passeports de combattants étrangers, du matériel informatique, des formulaires de recrutement et d'autres documents organisationnels, et conservent plus de 58 000 pages de documents dans son archive consacrée à Daech ». Ils ont aussi interrogé plus de 1 300 témoins (en date d'avril 2024)[29]. L'équipe de la CIJA, composée de personnes expérimentées en matière d'enquêtes et de poursuites sur des infractions pénales internationales, mène des enquêtes structurelles et monte des dossiers juridiques qu'elle transmet aux tribunaux compétents. Plusieurs de ces dossiers ont rendu possible la condamnation de combattants de l'EI.

Conflict Armament Research (CAR), ONG spécialisée dans les enquêtes, recense les armes, munitions, engins explosifs improvisés et autres matériels illicites sur des lieux touchés par des conflits dans le monde entier. CAR remonte ensuite jusqu'aux sources d'approvisionnement et verse les données dans un système financé par l'Union européenne, iTrace, base de données mondiale en expansion rapide qui contient des informations ayant force probante[30].

En général, les États apprécient au cas par cas la réputation et la fiabilité de chaque acteur non gouvernemental en tant que source d'informations concernant une zone de conflit particulière. Il convient de noter qu'en 2022, Eurojust et le Bureau du Procureur de la CPI ont publié des lignes directrices destinées à aider les organisations de la société civile à recueillir et préserver des informations concernant des crimes internationaux et des atteintes aux droits humains susceptibles de devenir des preuves admissibles en justice[31].

29. CIJA, « Da'esh / Islamic State », disponible à l'adresse https://cijaonline.org/daesh-islamicstate.
30. Voir Conflict Armament Research, « iTRACE », sur https://www.conflictarm.com/itrace/.
31. Voir Eurojust, *Eurojust and ICC Prosecutor launch practical guidelines for documenting and preserving information on international crimes*, sur https://www.eurojust.europa.eu/news/eurojust-and-icc-prosecutor-launch-practical-guidelines-documenting-and-preserving-information.

3. Étapes de l'analyse et de l'utilisation des informations

Les pays suivent une série d'étapes en vue d'apprécier la valeur probante des informations provenant de zones de conflit, de faciliter leur utilisation dans des procédures pénales, d'orienter les enquêtes, d'appuyer le processus juridique ou de pouvoir les présenter comme preuves devant un tribunal.

3.1. Normes et garanties en matière de droits humains[32]

Droit à un procès équitable (article 6 CEDH) et normes de droits humains applicables (article 3 CEDH).

Dans la prévention et la répression du terrorisme, les États membres ne peuvent en aucun cas déroger à leurs obligations découlant du droit international, concernant les droits humains, l'action humanitaire et l'asile. Lors de l'utilisation d'informations recueillies dans des zones de conflit comme preuves dans le cadre de procédures pénales de juridictions civiles relatives à des infractions terroristes, les États membres reconnaissent l'importance d'agir conformément aux exigences de la **Convention européenne des droits de l'homme**, ainsi qu'aux autres normes internationales en matière de droits humains. Toute action doit être proportionnée aux buts légitimes poursuivis et conforme à l'État de droit. Nul ne doit faire l'objet d'une discrimination fondée sur le sexe, la race, la couleur, la langue, la religion, les opinions politiques ou autres, l'origine nationale ou sociale, l'appartenance à une minorité nationale, la fortune, la naissance ou toute autre situation.

Le **droit à un procès équitable, prévu par l'article 6** de la Convention européenne des droits de l'homme, s'applique à toutes les formes de criminalité[33]. Les considérations de sécurité nationale peuvent, dans certaines circonstances, justifier des restrictions procédurales plus sévères. Cela dit, même lorsque la sécurité nationale est en jeu, les États membres doivent veiller à ce que les mesures qui ont des incidences sur les droits fondamentaux comme le droit à un procès équitable soient légales, nécessaires et proportionnées pour remplir leur fonction de protection. Et quelle que soit la gravité des charges, l'admission comme preuves de déclarations obtenues par des moyens contraires à l'**article 3** de la Convention européenne des droits de l'homme entache d'iniquité l'ensemble de la procédure et constitue une violation de l'article 6[34].

3.2. Analyse à des fins de constitution du dossier

Évaluation de la potentielle force probante des informations et passage aux étapes suivantes du travail d'investigation, notamment pour obtenir d'autres preuves qui compléteront les informations issues de zones de conflit ou s'y substitueront, pour appuyer le processus juridique national ou pour faire progresser les enquêtes et les poursuites dans d'autres pays.

3.2.1. Évaluation et utilisation des informations pour ouvrir des pistes d'enquête

Lorsque des acteurs de la justice pénale obtiennent des informations provenant de zones de conflit qui paraissent pertinentes dans une affaire de terrorisme, ils commencent par en évaluer la force probante : sont-elles authentiques et fiables ? Quels faits tendent-elles à prouver ? À quels actes criminels pourraient-elles être liées ? Sont-elles susceptibles d'être reçues et examinées par un tribunal ? À l'issue de cette évaluation, il s'agit de déterminer les mesures d'investigation ultérieures, en suivant les pistes suggérées par l'exploitation de ces informations (dont la possibilité de recueillir des informations supplémentaires via les diverses formes de coopération internationale évoquées plus haut).

32. Étant donné que la grande majorité des affaires évoquées ici relève du pénal, les normes et garanties de droits humains peuvent aussi s'appliquer aux moyens employés par les États pour accéder aux informations et les partager.
33. Voir Cour eur. DH, *Ramanauskas c. Lituanie* [GC], 2008, par. 53.
34. Voir Cour eur. DH, *Gäfgen c. Allemagne* [GC], 2010, par. 166. De nombreux États ont renforcé cette interdiction en l'intégrant expressément à leur code de procédure pénale.

Dans toute enquête, les agents des services répressifs, les magistrats instructeurs et les procureurs (en fonction des pays) s'efforcent de rassembler toutes les informations pertinentes pour déterminer si un crime a été commis et si oui, comment et par qui. La première utilité des informations recueillies dans des zones de conflit est d'aider à **ouvrir des pistes d'enquête et à combler les lacunes dans la compréhension des faits.**

Ainsi, les informations recueillies dans des zones de conflit peuvent mettre les enquêteurs sur la piste d'**autres éléments clés** : posts ou messages sur les réseaux sociaux et autres contenus numériques en ligne ; interceptions de communications des suspects ; entretiens avec leurs proches, amis, collègues et autres ; déclarations de témoins « de l'intérieur » qui se sont désengagés des organisations terroristes et peuvent livrer un récit de première main des événements ; et interrogatoire des suspects eux-mêmes. La Turquie, entre autres pays, observe que les informations recueillies dans des zones de conflit peuvent aiguiller les enquêteurs vers des faits qui seront corroborés par d'autres sources indépendantes (éléments matériels, données numériques ou dépositions de différents témoins).

De telles informations peuvent jouer un rôle essentiel dans l'enquête y compris lorsqu'elles sont incomplètes, non vérifiées et/ou irrecevables en justice. Certains tribunaux l'ont explicitement reconnu. En 2022 par exemple, la **Cour suprême de République tchèque** a confirmé la condamnation d'un ressortissant tchèque pour des **infractions terroristes dans les régions ukrainiennes de Donetsk et Louhansk**, refusant la demande d'annulation au motif que l'enquête s'était en partie fondée sur un rapport des services de contre-espionnage ukrainiens. Le tribunal a jugé que si les autorités tchèques avaient utilisé le rapport en question pour progresser dans leur enquête, elles ne l'avaient pas présenté comme élément de preuve, si bien que la question de sa recevabilité ne se posait pas.

À différentes étapes du processus juridique, les praticiens peuvent utiliser de telles informations à diverses fins, indépendamment de la question de la recevabilité. En fonction de la procédure pénale en vigueur dans le pays, les informations peuvent servir à justifier des citations à comparaître ou d'autres demandes formelles d'informations, à motiver un mandat d'arrêt ou à inciter un suspect à coopérer avec les autorités judiciaires.

3.2.2. Partage spontané avec des autorités étrangères

Examiner « les moyens les plus efficaces de rendre la justice[35] » suppose souvent que les praticiens identifient et analysent l'ensemble des informations et moyens de preuve dont ils disposent. Ils peuvent constater, ce faisant, que certaines informations seraient extrêmement précieuses pour une enquête menée dans un autre pays. En pareil cas, les États prennent souvent l'initiative de communiquer ces informations, de manière spontanée ou dans le cadre d'échanges relevant de la coopération policière et/ou judiciaire internationale et bilatérales ou multilatérales (voir le chapitre 2.2.2, ci-dessus), même si le quantité importante d'informations potentiellement pertinentes collectées et la classification de ces informations rendent le partage plus difficile.. Les Pays-Bas, par exemple, expliquent partager spontanément les informations recueillies auprès de réfugiés, de victimes, d'anciens combattants terroristes étrangers ou de témoins avec d'autres pays lorsqu'elles ont trait à des crimes internationaux ou liés au terrorisme. Les États détenteurs d'importants volumes d'informations partagent parfois en priorité celles qui pourraient faire progresser les enquêtes et les poursuites sur des crimes particulièrement graves. Les États-Unis, par exemple, se voient contraints d'opérer ce type de tri, étant donné l'énorme masse d'informations numériques et sur papier qu'ils ont recueillies dans des zones de conflit. Cependant, lorsque l'analyse d'engins explosifs improvisés et autres éléments par le TEDAC semble dévoiler l'identité d'un individu ayant confectionné des explosifs, les États-Unis prennent l'initiative de partager l'information avec le pays d'origine et/ou de séjour probable de l'individu.

3.3. De l'information à la preuve

Procédures et techniques permettant de présenter comme preuves des informations issues de zones de conflit en gardant le secret sur les sources, les méthodes et d'autres enjeux de sécurité nationale.

3.3.1. Considérations sur la recevabilité

En général, les codes de procédure pénale des États membres du Conseil de l'Europe n'interdisent pas de présenter comme preuves dans les procédures pénales ordinaires des informations touchant à des enjeux de sécurité nationale. Beaucoup d'États estiment qu'il convient d'appliquer à ces informations (examen, réception,

35. CM/Rec(2022)8, chapitre VII – Utilisation des informations recueillies dans des zones de conflit pour la poursuite d'autres infractions que le terrorisme, par. 22.

appréciation de la valeur probante) **les mêmes règles de procédure et de recevabilité qu'à toutes les autres**. De nombreux pays de droit continental adhèrent au principe fondamental de la liberté de la preuve, selon lequel les tribunaux peuvent évaluer les éléments de preuve sans s'encombrer de règles formelles excluant certaines catégories de preuves ou imposant un degré préétabli de force probante. Et la plupart des pays de *common law* n'interdisent pas non plus catégoriquement les preuves issues de zones de conflit. Au Royaume-Uni par exemple, si les informations sont jugées authentiques et fiables et remplissent les critères habituels de recevabilité, le parquet peut les présenter comme preuves.

Point à noter, les réponses des États vont dans le même sens que les conclusions du Mémorandum d'Eurojust sur les preuves recueillies sur le théâtre des opérations (septembre 2020), centré sur les informations recueillies par l'armée. Ce document constate qu'en général, « le droit national n'exclut pas l'utilisation de preuves recueillies sur le théâtre des opérations[36] ».

Certaines juridictions nationales ont explicité cette règle. En Suisse par exemple, le Tribunal fédéral a affirmé que les rapports officiels non classifiés rédigés par le Service de renseignement de la Confédération à l'attention du Ministère public de la Confédération (MPC) pouvaient être considérés comme moyens de preuve et versés au dossier d'une procédure pénale. En confirmant que les informations fournies par d'autres acteurs que les services répressifs peuvent servir de preuves, le pouvoir judiciaire apporte à l'ensemble des tribunaux une clarté et une prévisibilité bienvenues.

3.3.2. Protection des intérêts de sécurité nationale

Pour la plupart des États, le principal problème ne tient pas à la recevabilité théorique des informations issues de zones de conflit, mais à la **manière d'intégrer de telles informations à la procédure pénale** en assurant la protection des sources et des méthodes de collecte sensibles, entre autres considérations de sécurité nationale, tout en respectant les garanties d'un procès équitable. Les mécanismes et procédures appliqués par les États pour relever ce défi sont variés.

Certains systèmes juridiques autorisent l'utilisation, dans les procédures pénales, d'informations *non officiellement déclassifiées*. C'est le cas en Allemagne, en Hongrie et en Roumanie. Dans la plupart des pays toutefois, les éléments recueillis par l'armée, le renseignement ou d'autres acteurs hors services répressifs doivent être **officiellement déclassifiés, certifiés par l'entité détentrice et/ou expurgés** par les services répressifs pour pouvoir être présentés comme preuves.

Indépendamment des conditions de recevabilité, il convient d'éviter de porter certaines informations sensibles à la connaissance de personnes soupçonnées dans une affaire de terrorisme. En pratique, les États utilisent les procédures mentionnées au chapitre 2.1.3, ci-dessus, pour obtenir des informations sous forme déclassifiée, mais ces informations et/ou leurs sources et méthodes de collecte restent partiellement couvertes par le secret. Dans de nombreux pays, les autorités recourent à la **déclassification partielle** et à un travail éditorial pour présenter les informations sous forme expurgée ou synthétisée, en supprimant les passages qui ne peuvent être déclassifiés et en taisant les sources et les méthodes de collecte qui ne sauraient être portées à la connaissance de la défense ou du public. Ils invoquent, de même, les **impératifs de sécurité** pour justifier la **non-transmission d'éléments** qui risqueraient d'être divulgués à la partie défenderesse.

En **France** par exemple, des informations initialement classifiées peuvent être intégrées à une procédure pénale après un procédé de déclassification d'initiative désignée sous le terme de « **judiciarisation** ». En pratique, dans les procédures portant sur des infractions terroristes, la transmission à l'autorité judiciaire d'informations déclassifiées est réalisée par la DGSI, service chef de file en matière de lutte anti-terroriste, après autorisation par le ministère compétent. La DGSI établit un procès-verbal résumant les informations recueillies en renseignement, initialement couvertes par le secret de la défense nationale, qu'elle choisit de révéler à l'autorité judiciaire et omettant les éléments qui restent couverts par le secret. Ce procès-verbal est transmis à l'autorité judiciaire.

La « double compétence » de la DGSI facilite ce processus. Lorsqu'il s'agit d'informations en possession de l'armée française, le ministère des Armées peut soit répondre directement à une requête de l'autorité judiciaire soit adresser spontanément les documents ou objets en question à la DGSI qui dresse un procès-verbal incluant ces éléments et l'adresse au magistrat compétent pour versement en procédure. S'il s'agit de documents ou d'objets, ils sont placés sous scellés.

36. Eurojust, *Mémorandum sur les preuves recueillies sur le théâtre des opérations*, septembre 2020, p. 21.

En **Allemagne**, de même, les services de renseignement transmettent les informations aux autorités judiciaires via une procédure dite de ***Behördenerklärung* (certification officielle)**, qui leur permet de fournir les informations pertinentes accompagnées d'une évaluation de leur fiabilité sans révéler où, comment et auprès de qui elles ont été recueillies. Les informations ainsi transmises peuvent déclencher l'ouverture d'une enquête ou même servir de preuves devant un tribunal, mais un accusé ne peut être condamné sur leur seule foi : d'autres indices, au minimum, doivent venir corroborer les éléments. En **Hongrie**, les informations issues des services de renseignement peuvent être transformées en preuves via des **autorisations officielles**, quoiqu'uniquement dans les affaires portant sur des infractions pénales d'une certaine gravité. Et en **Suisse**, comme déjà évoqué, le Service de renseignement de la Confédération autorise l'emploi de ses informations comme éléments de preuve en adressant au Ministère public un **rapport officiel** comportant les **informations sous forme non classifiée**.

Aux **Pays-Bas**, des documents de l'EI obtenus via les services militaires ou de renseignement, utilisés comme preuves, ont appuyé de nombreux verdicts de culpabilité dans des affaires de terrorisme. Dans la première de ces affaires, jugée par le **tribunal de district de Rotterdam** en 2017, le dossier comportait un **registre des membres de l'EI**. Au lieu de déclassifier tout le document – ce qui n'aurait pas été faisable –, le Service de renseignement et de sécurité militaire néerlandais (MIVD) a **réuni dans un rapport des extraits déclassifiés** concernant l'individu accusé en l'espèce. Le tribunal a jugé ce rapport recevable et s'est fondé sur lui pour reconnaître le suspect coupable. Dans une affaire distincte mais similaire, les services de renseignement de **Belgique** ont transmis à la justice trois **extraits de bulletins de paie de l'EI**, sur lesquels le **tribunal d'Anvers** s'est fondé pour condamner une personne soupçonnée d'appartenance à ce groupe. Le tribunal belge a explicitement affirmé que pour lui, ces informations prouvaient que l'accusé était un combattant de l'EI.

Aux **États-Unis**, lorsque des éléments ne peuvent être déclassifiés dans leur intégralité, les procureurs peuvent demander la déclassification des extraits pertinents, en combinaison avec la ***Classified Information Procedures Act* (CIPA)** (loi sur les procédures relatives aux informations classifiées) pour protéger les informations restantes ainsi que les sources et méthodes sensibles. La CIPA est une loi procédurale qui protège contre la divulgation non autorisée d'informations classifiées. En vertu de la CIPA, les procureurs peuvent demander au tribunal l'autorisation de supprimer du dossier certaines informations classifiées et/ou de fournir les informations requises à la défense sous la forme de résumés non classifiés.

Les informations recueillies dans des zones de conflit sont couramment utilisées lors des audiences. Aux Pays-Bas par exemple, les informations transmises au Service de renseignement et de sécurité militaire néerlandais (MIVD) par des partenaires étrangers ne sont pas seulement versées au dossier, lequel est transmis à la fois à la défense et aux juges, mais aussi débattues en audience publique et mentionnées dans les jugements publiés. Dans certains pays, toutefois, la procédure pénale autorise le **huis clos sélectif** lorsqu'il est nécessaire pour protéger des informations ou écarter d'autres risques pour la sécurité. En Allemagne, par exemple, entre autres procédures spéciales permettant de présenter comme preuves des informations classifiées, le tribunal peut exclure le public d'une audience ou d'une partie de l'audience, selon les besoins.

Au Royaume-Uni, lorsque la défense demande la divulgation d'informations que le gouvernement juge couvertes par l'immunité d'intérêt public, le tribunal peut examiner ce point à huis clos et *ex parte*. Dans certaines circonstances, un « avocat spécial » demande leur divulgation au nom de la défense, mais il lui est interdit de communiquer avec l'accusé après avoir pris connaissance des éléments en question. Dans ce scénario toutefois, lorsque le tribunal juge que les éléments concernés sont effectivement couverts par l'immunité d'intérêt public, ils ne sont pas utilisés comme preuves et ne sont pas révélés. Si la demande d'immunité d'intérêt public n'aboutit pas, les options sont les suivantes : divulguer les informations d'une manière qui ne compromette pas leur caractère sensible ; abandonner l'affaire ; ou divulguer les éléments parce que l'intérêt public global de la poursuite est plus grand que si l'affaire était abandonnée.

Comme protection supplémentaire, il arrive que des tribunaux demandent au procureur et au conseil de la défense d'obtenir une **habilitation de sécurité** avant de pouvoir traiter certaines informations. En Roumanie par exemple, la procédure pénale autorise l'utilisation d'informations classifiées comme preuves dans un procès, mais uniquement si l'agence détentrice des informations a habilité les deux conseils à les consulter. Délivrer ainsi des habilitations de sécurité aux conseils des parties est également une composante essentielle de la loi CIPA aux États-Unis, ainsi que du recours aux avocats spéciaux dans les audiences sur des questions couvertes par l'immunité d'intérêt public au Royaume-Uni.

3.4. Confirmation de l'authenticité, de la fiabilité et de la valeur probante

Techniques visant à expliquer l'importance des informations, à décrire le contexte de leur collecte, à attester de leur intégrité et de leur chaîne de conservation et, plus généralement, à corroborer leur authenticité et leur fiabilité et/ou à confirmer leur valeur probante.

Dans de nombreux systèmes juridiques, rien n'empêche des informations issues de zones de conflit de jouer un rôle décisif dans une condamnation pénale, voire d'en former la seule base. En pratique, toutefois, **il est crucial que d'autres éléments viennent corroborer l'authenticité et la fiabilité des informations et appuyer leur valeur probante**. De tels éléments sont nécessaires, en partie, parce que les circonstances exceptionnelles dans lesquelles les informations ont été recueillies créent souvent une discontinuité dans la chaîne de conservation[37]. Retracer la chaîne de conservation peut s'avérer particulièrement important pour les preuves matérielles, comme les armes ou les téléphones, qu'il peut être impossible de distinguer à première vue d'autres objets similaires ; c'est un peu moins le cas pour les documents, dont le contenu peut être vérifié à l'aide de sources indépendantes.

Dans les deux cas, l'existence d'une chaîne de conservation complète et ininterrompue n'est pas un critère d'admissibilité. Dans les pays de *common law* comme de droit continental, les discontinuités dans la chaîne de conservation ont une incidence sur la force probante des éléments mais ne les rendent pas irrecevables. Néanmoins, les tribunaux de nombreux pays peuvent n'attribuer qu'une très faible valeur probante à des éléments dont il est impossible de déterminer où, quand et/ou par qui ils ont été obtenus. En outre, au-delà des préoccupations sur la provenance des informations et leur contamination éventuelle, la confirmation peut être essentielle pour vérifier leur teneur et expliquer leur importance pour le dossier.

3.4.1. Documents, mises en contexte et résultats d'analyses techniques

Les praticiens utilisent des techniques diverses pour corroborer et appuyer les informations issues de zones de conflit. En certaines circonstances, ils parviennent à obtenir l'**objet matériel original**. Le personnel des services répressifs peut ainsi mener son propre travail d'**analyse et d'exploitation**, indépendant de celui éventuellement déjà effectué par le personnel du pays étranger qui a recueilli les informations. Les autorités italiennes ont procédé ainsi dans l'**affaire dite « Mamma ISIS »**. Un ressortissant italien s'était rendu en Syrie avec sa femme et ses enfants pour rejoindre l'EI ; sa femme avait été arrêtée ultérieurement et extradée vers l'Italie. Entre-temps, l'Operation Gallant Phoenix avait permis d'obtenir des informations relatives aux activités du couple en Syrie, dont leurs téléphones portables, qui contenaient des informations démontrant la participation volontaire de la suspecte aux activités de l'EI. Le FBI a transmis les téléphones au procureur, au tribunal de Milan. Les autorités italiennes ont alors réalisé leur propre analyse technico-légale et utilisé les résultats lors du procès pour corroborer les informations à charge. Le tribunal a jugé l'accusée coupable d'appartenance et de participation à une organisation terroriste et l'a condamnée à quatre ans de prison.

Les autorités françaises ont également appréhendé des engins explosifs artisanaux et des documents papier originaux initialement recueillis par les États-Unis dans des zones de conflit, pour les réexploiter et les placer sous scellés comme éléments de preuve. Aux Pays-Bas, l'Institut national de forensique peut analyser l'authenticité de documents écrits, de photos ou de vidéos recueillis dans des zones de conflit afin de faciliter leur utilisation comme preuves.

Il peut arriver que l'original d'un document ou d'un objet ne soit pas disponible. En pareil cas, de nombreux systèmes autorisent à produire comme preuve **la copie de l'élément ou sa description**. En Allemagne et au Danemark, lorsqu'un objet n'est pas disponible, le tribunal peut admettre comme preuve une photographie ou (dans le cas d'un appareil électronique) une copie judiciaire. La Suède signale que le plus souvent, une photographie de l'objet suffit, et en Belgique, le procureur présente en général une copie numérique du contenu d'un téléphone et non le téléphone lui-même.

Pour parer aux problèmes d'authenticité ou d'intégrité, il peut être très utile de prévoir un **historique officiel des processus de traitement, transmission, stockage, analyse et partage**. Même dans les systèmes continentaux, où la chaîne de conservation ne fait pas l'objet de dispositions spécifiques, le fait de pouvoir dire où, quand, par qui et dans quelles circonstances des éléments ont été recueillis peut renforcer leur valeur probante.

Pour pouvoir retracer de façon crédible les processus de collecte, de traitement et de partage des preuves, l'État doit bien sûr avoir appliqué ce type de processus standard. C'est pour cette raison que la Recommandation

37. Voir CM/Rec(2022)8, Rapport explicatif, chapitre VI – Chaîne de conservation et risque d'altération.

– tout en soulignant que « les activités de recueil d'informations par les forces militaires dans les zones de conflit ne devraient en aucun cas empêcher ces dernières de remplir efficacement leurs missions premières » – suggère néanmoins aux États d'« assurer une formation adéquate aux agents qui interviennent dans le processus de recueil de telles informations de manière à renforcer leur valeur probatoire » et les encourage à « élaborer et à fournir aux acteurs concernés des orientations et des procédures claires sur la manière d'assurer la continuité de la chaîne de conservation et la traçabilité des informations, et d'éviter tout risque d'altération de ces informations recueillies dans les zones de conflit[38] ».

En pratique, plusieurs États et acteurs multilatéraux ont développé ce type de politiques et de procédures et organisent des formations. Le Royaume-Uni, par exemple, signale que des enquêteurs de la police nationale ont formé des membres de la Coalition internationale aux processus de collecte, de documentation et de stockage des éléments pouvant être saisis sur le champ de bataille. Différents pays ont également supporté la formation du personnel militaire et répressif de pays partenaires à la collecte et à la préservation de données sur des sites sensibles, à l'appui des enquêtes sur le terrorisme.

L'Operation Gallant Phoenix, notamment, a fortement standardisé les processus de traitement, stockage, exploitation et analyse des éléments, en vue de préserver leur intégrité et, à terme, leur intérêt pour les enquêtes et les poursuites. Les attachés juridiques du FBI qui partagent des informations avec des pays partenaires sont en mesure de fournir l'historique de ces processus, ainsi que des informations contextuelles spécifiques sur le lieu d'origine, la date de collecte et les conditions de stockage et d'utilisation de chaque élément. Ce travail systématique a renforcé la confiance des tribunaux envers l'authenticité et la fiabilité des informations fournies par l'OGP.

La fourniture d'**informations contextuelles** sur les circonstances de la collecte et sur le traitement ultérieur s'est avérée cruciale pour corroborer et appuyer la valeur de différents types d'informations provenant de zones de conflit. Exemple particulièrement frappant, l'**affaire *Khalid Ali*** (2018, Royaume-Uni) a tourné en partie autour de l'admission des empreintes digitales de l'accusé, détectées par le TEDAC sur des composants d'engin explosif artisanal récupérés en Afghanistan des années plus tôt. Le FBI a fourni aux autorités britanniques un rapport retraçant en détail la collecte, la préservation et l'examen technico-légal de ces composants. Ce rapport a joué un rôle important pour faire admettre les empreintes digitales comme preuves, entraînant l'inculpation de Khalid Ali pour – entre autres – possession de substances explosives, et sa condamnation à la réclusion à perpétuité.

3.4.2. Preuves matérielles ou numériques supplémentaires

Plus généralement, au-delà de la confirmation contextuelle ou technico-légale de l'authenticité, les États constatent qu'**identifier et présenter des preuves corroborantes** est essentiel pour que des informations issues de zones de conflit se voient reconnaître toute leur force probatoire.

Il arrive, même si c'est exceptionnel, que **de multiples éléments indépendants** concernant les mêmes individus et la même zone de conflit se corroborent mutuellement. Le **procès dit « Ulysse »**, en 2021, lors duquel des djihadistes présumés ont comparu devant la cour d'assises spéciale de Paris, en est un exemple. L'un des suspects niait non seulement avoir exercé des activités de recrutement et de financement pour le compte de l'organisation terroriste État Islamique (EI) mais aussi s'être jamais rendu en Syrie. Via la coopération réalisée dans le cadre de l'Operation Gallant Phoenix, un document établi par une administration de l'État Islamique indiquant clairement que l'accusé avait été présent en Syrie et enregistré par l'EI comme « combattant » a été communiqué à la DGSI et versé en procédure. De la même manière, d'autres documents obtenus dans la même zone de conflit, dont des registres de distribution de nourriture et d'essence à l'accusé et le reçu d'une pension versée à sa mère au titre de son fils « prisonnier-martyr », ont été transmis à l'autorité judiciaire et versés en procédure. L'ensemble de ces éléments concordants a été pris en compte dans la démonstration de l'appartenance de l'accusé à l'organisation terroriste EI. L'accusé a été condamné à 30 ans de réclusion.

Un exemple récent aux États-Unis est **le procès d'Ibrahim « Izzy » Musaibli en 2023**. Au cours de ce procès, les procureurs ont présenté différents dossiers et documents de l'ISIS concernant Musaibli. Certains de ces éléments ont été obtenus par l'armée américaine et les forces partenaires et d'autres ont été collectés par l'UNITAD. Les procureurs ont été en mesure de corroborer une grande partie du contenu de chacun des documents individuels, et de démontrer que ces multiples documents étaient cohérents entre eux, contribuant

38. CM/Rec(2022)8, chapitre III – Informations recueillies par le personnel militaire, par. 6 ; chapitre VIII – Coordination nationale, par. 25 ; chapitre VI – Chaîne de conservation et risque d'altération, par. 19.

ainsi à renforcer l'authenticité de l'ensemble des documents. Musaibli a été reconnu coupable d'avoir fourni un soutien matériel à l'EI à l'issue du procès et condamné à 14 ans de réclusion.

Plus couramment, les praticiens se fondent sur des **éléments issus d'autres sources** pour appuyer l'authenticité et la fiabilité des preuves issues de zones de conflit. Lors du **procès de 2017** aux Pays-Bas évoqué plus haut, le **tribunal de district de Rotterdam** a vérifié l'authenticité et la fiabilité du registre de l'EI sur lequel figurait le nom du suspect en comparant les informations qu'il contenait avec le registre d'état civil néerlandais, ainsi qu'avec les déclarations de l'accusé lui-même et avec son passeport yéménite, retrouvé en un lieu différent.

Des tribunaux ont également jugé les éléments de sources indépendantes précieux non seulement pour recouper la teneur des informations provenant de zones de conflit, mais aussi pour appuyer les chefs d'inculpation concernés. Dans l'**affaire *Anis Sardar***, l'une des tâches majeures du ministère public britannique a consisté à démontrer qu'en déployant des engins explosifs improvisés en Irak, l'accusé visait à tuer non seulement des membres de milices chiites, mais aussi des soldats américains. Le ministère public y est parvenu, notamment, en produisant comme preuve les CD gravés qu'Anis Sardar avait rapportés d'Irak au Royaume-Uni, « qui comportaient non seulement un manuel sur les explosifs, avec une formule pour fabriquer du TNT, mais aussi des contenus violemment antiaméricains ». L'accusé lui-même, ultérieurement « soumis à un contre-interrogatoire, […] a affirmé que « l'intervention des Américains en Irak » l'avait « mis en rage ». Le juge chargé de prononcer la peine a qualifié ces éléments d' « éclairants » et s'est dit « convaincu qu'à l'époque en question, dans l'esprit d'Anis Sardar, les Américains constituaient tout autant des ennemis que les milices chiites. [Il envisageait] en permanence ces deux cibles[39] ».

Des **éléments de sources publiques** (reportages journalistiques, études réalisées par des organisations non gouvernementales) peuvent aussi aider à mettre en contexte et à expliquer l'importance des informations recueillies dans des zones de conflit. Certaines **informations librement accessibles en ligne** peuvent être particulièrement précieuses ; bien que leur crédibilité puisse parfois être contestée, une série précise de vérifications techniques a montré son efficacité. Le *Berkeley Protocol on Digital Open Source Investigations* propose des étapes utiles pour établir l'exactitude et la validité des informations recueillies en ligne[40]. En pratique, lorsque les autorités d'un État comme les Pays-Bas obtiennent des éléments numériques concernant des crimes commis en Syrie et/ou en Irak, la police recourt à la géolocalisation ou à d'autres analyses technico-légales pour examiner et vérifier les informations avant de les utiliser dans une affaire pénale.

3.4.3. Témoignages concordants

Dans de nombreux cas, les États ont constaté que les **témoignages** constituaient un important moyen de confirmer la fiabilité des informations issues de zones de conflit et de renforcer leur valeur probante. Il arrive que les personnes mêmes qui ont récolté les informations puissent venir témoigner. Mais le plus souvent, il s'avère impossible de les localiser ou de recueillir leur déposition. Cependant, d'autres témoins peuvent être en mesure de décrire les circonstances dans lesquelles les informations ont été collectées, d'attester de leur intégrité et de celle de leur chaîne de conservation et/ou d'expliquer leur importance.

Parmi ces témoins potentiels figurent les **hauts fonctionnaires** ou les **techniciens spécialisés** représentant les **institutions publiques concernées**. Dans l'**affaire *Sardar***, au Royaume-Uni, le tribunal a auditionné les chefs de l'équipe étasunienne de neutralisation des explosifs qui opérait sur site au moment où les informations ont été collectées. Ces témoins, bien que n'ayant pas recueilli eux-mêmes les composants présentés comme preuves, ont pu décrire leurs méthodes de réception et de traitement des matériels en général, et donc replacer les composants dans leur contexte. Leurs connaissances pointues ont également permis de confirmer l'importance de cet élément de preuve en l'espèce : le juge a été convaincu par leur explication selon laquelle « l'emploi de doubles plateaux de pression montre que [les engins explosifs en question] étaient conçus pour être déclenchés par des véhicules lourds sur essieux à voie large, tels que ceux utilisés par l'armée américaine, et non par les véhicules plus étroits et plus légers » utilisés par les milices chiites[41].

L'Allemagne confirme elle aussi qu'en certaines circonstances, le personnel des services de renseignement peut témoigner devant un tribunal. Pour prendre un autre exemple, dans l'**affaire pré-citée « Ulysse »**, en 2021 en France, un enquêteur de la DGSI a été cité en tant que témoin à l'audience afin de présenter, dans

39. *R v. Anis Sardar*, Remarques sur le verdict.
40. Voir Human Rights Center de l'Université Berkeley et Haut-Commissariat des Nations Unies aux droits de l'homme, *Berkeley Protocol on Digital Open Source Investigations : A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law*, 2022, pp 62-65.
41. *R v. Anis Sardar*, Remarques sur le verdict.

un cadre contradictoire, les divers éléments d'informations issues de zones de conflit obtenus par le service, permettant au tribunal d'en apprécier le caractère probant.

Les **acteurs multilatéraux ou non gouvernementaux** peuvent aussi fournir des témoignages précieux. Dans l'**affaire *Zoher J.*** (2019), le directeur exécutif de la CIJA et l'un de ses enquêteurs de terrain ont présenté respectivement devant le tribunal régional supérieur de Munich « les objectifs, les structures et les méthodes de travail de la CIJA », et « plus important encore […], la responsabilité pénale individuelle de l'accusé ». Le tribunal s'est fondé sur ces dépositions pour juger l'accusé coupable de soutien matériel à une organisation terroriste et l'a condamné à sept ans de prison[42]. Des représentants de l'UNITAD ont également fourni des dépositions et des rapports dans le cadre de diverses procédures nationales.

Dans plusieurs pays, des **universitaires, chercheurs ou autres spécialistes** ont témoigné sur des sujets tels que la structure et l'idéologie des groupes terroristes, afin de donner des éclairages sur la force probante des informations recueillies dans des zones de conflit[43]. La Norvège signale que des dépositions d'experts ont joué un rôle central, voire décisif dans l'issue d'affaires de terrorisme, et le Danemark a reconnu que la déposition devant un tribunal de spécialistes reconnus constituait un solide élément de preuve. La France, l'Allemagne, la Hongrie, la Suisse et les Etats Unis ont également indiqué qu'ils ont utilisé des informations obtenues par des experts académiques.

Des **victimes, réfugiés, anciens combattants étrangers** et autres **témoins « de l'intérieur »** ont également livré de précieuses dépositions. Dans leurs réponses au questionnaire du CDCT de 2020, l'Allemagne, le Danemark, les États-Unis, la Finlande, la France, la Hongrie, la Norvège, les Pays-Bas, la Serbie, la Suisse et la Turquie ont tous indiqué avoir utilisé des informations de ce type de sources.

Dans la plupart des exemples décrits, ni les considérations de sécurité, ni les règles de procédure n'ont entravé de façon notable la libre expression des témoins devant le tribunal. Dans d'autres cas, toutefois, la sécurité, voire l'identité même de certains témoins appellent une protection spéciale. Les victimes ou les témoins oculaires peuvent vivre dans des lieux touchés par un conflit, avoir des proches ou des amis en danger ou se trouver exposés à des représailles de la part de groupes terroristes. De même, certains agents de l'État risqueraient de ne plus pouvoir travailler – sans parler de leur sécurité personnelle – s'ils témoignaient en personne en audience publique.

Les États recourent à différents **moyens de procédure pour présenter les témoignages de témoins vulnérables ou sensibles** en protégeant leur sécurité ou, dans certains cas, en gardant le secret sur leur identité. Ces procédures englobent, comme déjà évoqué, le huis clos pour tout ou partie du procès[44]. Les personnes déposant en direct peuvent aussi s'exprimer **derrière un paravent**, avec une technologie de **déformation de leur voix**, etc. Ces dernières années, et en particulier depuis le début de la pandémie de COVID-19, les tribunaux de nombreux pays se sont également montrés plus réceptifs à l'idée d'autoriser le témoignage par vidéo lorsque les circonstances de l'affaire le justifient.

En cas de stricte nécessité, les tribunaux de certains pays accordent même l'**anonymat** à certains témoins. Au Royaume-Uni, le parquet peut protéger les témoins dans les affaires de terrorisme en déposant des demandes d'anonymat, entre autres mesures spéciales. Les Pays-Bas y ont eu recours pour **poursuivre quatre individus soupçonnés d'implication dans l'attaque du vol MH17 de la Malaysia Airlines, le 17 juillet 2014**. Une chambre du tribunal de district de La Haye, sur demande du juge d'instruction, a autorisé une dizaine de personnes qui encouraient un risque réel de graves représailles à témoigner anonymement. En vertu de dispositions spécifiques du Code néerlandais de procédure pénale, le juge d'instruction a interrogé ces témoins lors d'audiences séparées. Le parquet et la défense ont pu soumettre des questions à l'avance, mais non participer à ces audiences. Des transcriptions expurgées ont été versées au dossier, les témoins n'étant identifiés que par des noms de code. Le tribunal s'est fondé sur leurs témoignages, en plus d'un important volume d'autres preuves, pour juger trois des accusés coupables d'avoir abattu l'avion et tué ses 298 passagers, et les a condamnés à la réclusion à perpétuité[45].

42. CIJA, « Da'esh / Islamic State », disponible sur https://cijaonline.org/daesh-islamicstate.
43. Parmi les difficultés dans certaines affaires de terrorisme, le Royaume-Uni a identifié la méconnaissance par le tribunal du déroulement de certains conflits armés et de la nature et de la structure des groupes terroristes impliqués, dont notamment le rôle des femmes dans ces groupes. Voir RQ 2020, Royaume-Uni.
44. Voir la Recommandation Rec(2005)9 du Comité des Ministres aux États membres relative à la protection des témoins et des collaborateurs de justice, telle que mentionnée dans la CM/Rec(2022)8, chapitre V – Informations fournies par d'autres sources, par. 18.
45. Voir tribunal de district de La Haye, verdict MH 17, 17 novembre 2022.

Il est difficile de recueillir des dépositions ou de faire venir des témoins lorsque l'affaire porte sur des infractions pénales commises dans des pays éloignés. La Finlande a trouvé une solution innovante lors des **poursuites contre des frères jumeaux irakiens soupçonnés de participation au massacre du camp Speicher**, près de Tikrit (Irak), en juin 2014. En première instance, les frères avaient été acquittés des accusations de crimes de guerre, meurtre et attaque à motivation terroriste, par manque de preuves. Le parquet avait cherché à auditionner des témoins supplémentaires en appel. L'UNITAD, avec le soutien et l'assistance des autorités irakiennes, a organisé la déposition de huit personnes depuis son siège à Bagdad, visionnée par la cour d'appel et les accusés au moyen d'un lien vidéo sécurisé. Le procureur et un avocat de la défense étaient physiquement présents à l'audience, et des témoins à charge comme à décharge ont été auditionnés, contrebalançant toute atteinte possible aux droits des accusés à un procès équitable[46].

De même, aux États-Unis, lors du **procès de Mohamad Jamal Khweis en 2017**, un responsable peshmerga kurde a été autorisé à témoigner par vidéo depuis l'Irak sur son implication dans la récupération d'un document de l'ISIS en rapport avec l'accusé. Ce témoignage a contribué à la condamnation ultérieure de Khweis pour avoir fourni un soutien matériel à l'EI et à sa condamnation à 20 ans de réclusion.

Dans de nombreux systèmes de droit continental où les règles de procédure n'interdisent pas les preuves par des propos rapportés, des **transcriptions de dépositions recueillies avant le procès** ou des comptes rendus d'autres entretiens hors tribunal peuvent être présentés en lieu et place des témoignages en direct. En Allemagne par exemple, une déclaration hors prétoire peut être admise comme preuve lorsque nécessaire pour protéger l'identité du personnel militaire ou de renseignement, ou lorsque l'auteur de la déclaration n'est pas disponible pour déposer à la barre pour d'autres raisons légitimes. Même dans les pays de *common law*, le parquet peut admettre en certaines circonstances des propos rapportés.

Même lorsqu'un témoin peut se présenter à la barre et lorsque toutes les mesures sont prises pour le protéger, d'autres difficultés se posent (difficultés qui sont parfois, paradoxalement, amplifiées par les mesures de protection). Il peut être particulièrement délicat, par exemple, d'établir la fiabilité d'un témoignage. La Finlande signale que la fiabilité des témoins qui vivent dans une zone de conflit ou ont un rapport avec le lieu en question est souvent mise en doute. L'Allemagne reconnaît que les déclarations des réfugiés, des victimes et des anciens combattants terroristes étrangers doivent être prises avec précaution, car elles peuvent contenir aussi bien des entorses délibérées à la vérité que des inexactitudes involontaires.

Face à ces difficultés, plusieurs États jugent utile de s'appuyer sur les expériences antérieures de recueil et d'évaluation des témoignages dans des affaires de crimes de guerre. Le Royaume-Uni observe que dans l'idéal, les dépositions de témoins devraient être recueillies conformément aux normes internationales en matière de droit pénal, et que les témoins devraient donner leur consentement éclairé au partage des informations avec les autorités judiciaires. Les Pays-Bas, quant à eux, expliquent que si les juges ont l'habitude d'évaluer la fiabilité des dépositions recueillies par la police auprès de réfugiés, des victimes, des témoins et des anciens combattants terroristes étrangers sur leurs expériences en Irak et/ou en Syrie, comme pour tous les autres témoins, ils appliquent aux affaires de crimes internationaux un cadre d'estimation de la fiabilité particulièrement étoffé, incluant la prise en compte des différences culturelles.

3.5. Utilisation dans le cadre d'autres infractions que le terrorisme

Considérations particulières à l'utilisation des informations dans les affaires de crimes de guerre, de crimes contre l'humanité et de génocide.

Dans un rapport paru en 2020, Eurojust conclut : « La jurisprudence nationale existante des États membres de l'UE et les pratiques nationales émergentes montrent qu'il est possible, à l'encontre des combattants terroristes étrangers, de **cumuler les charges** de crimes de guerre, crimes contre l'humanité et crime de génocide, en plus des infractions à caractère terroriste », et qu'un tel cumul « permet d'engager pleinement la responsabilité pénale des auteurs, entraîne des peines plus lourdes et rend mieux justice aux victimes[47] ». De fait, dans plusieurs affaires pénales, des informations recueillies dans des zones de conflit ont également joué un rôle crucial pour prouver d'autres infractions que le terrorisme, dont **les crimes de guerre, les crimes contre l'humanité et le génocide**[48].

46. Voir TRIAL international, *Universal Jurisdiction Annual Review 2021*, p. 27, et l'allocution de Karim Khan, Conseiller spécial et chef de l'UNITAD, devant le Conseil de sécurité de l'ONU, 26 novembre 2019.
47. Rapport d'Eurojust, *Cumulative Prosecution of Foreign Terrorist Fighters for Core International Crimes and Terrorism-Related Offences*, mai 2020, p. 3.
48. Voir CM/Rec(2022)8, chapitre VII – Utilisation des informations recueillies dans des zones de conflit pour la poursuite d'autres infractions que le terrorisme, par. 21 et 22, et chapitre IX – Coopération entre États et avec les organisations internationales, par. 30.

Les Pays-Bas ont utilisé, avec succès, des informations recueillies dans des zones de conflit pour poursuivre des terroristes pour un crime de guerre, à savoir l'atteinte à la dignité humaine de dépouilles mortelles. En France, les poursuites en matière de crimes contre l'humanité et crimes de guerre sont en pratique exercées par le Parquet national antiterroriste (PNAT) qui dispose d'un pôle spécialisé en la matière. Comme déjà mentionné, le PNAT a pu obtenir et exploiter en procédure des informations transmises par les organisations non gouvernementales actives en zone de conflit et par des organes de l'ONU, informations dont la valeur probante est ensuite débattue contradictoirement. De même, l'autorité judiciaire autrichienne a utilisé des informations recueillies dans des zones de conflit pour poursuivre les auteurs de crimes de guerre et de crimes contre l'humanité, et la Hongrie a ouvert au moins une procédure contre un terroriste présumé pour des allégations de crimes internationaux.

L'Allemagne a joué un rôle moteur dans la poursuite des membres d'organisations terroristes pour crimes internationaux. À cet égard, l'**affaire *Taha Al J.*** a été particulièrement marquante. Ce membre de l'EI avait réduit en esclavage une mère et sa fille, dans le nord de l'Irak, et « puni la fillette yézidie en l'attachant à une fenêtre par une chaleur torride, sans aucune protection contre le soleil »[49], la laissant agoniser sous les yeux de sa mère. Le tribunal régional supérieur de Francfort l'a reconnu coupable de crimes de guerre, de crimes contre l'humanité et de génocide et condamné à la réclusion à perpétuité. C'était la première fois au monde qu'une juridiction pénale qualifiait de génocide les crimes commis contre les Yézidis.

Le Réseau européen d'enquête et de poursuite du crime de génocide, des crimes contre l'humanité et des crimes de guerre facilite une coopération étroite entre les autorités nationales chargées d'enquêter sur les principaux crimes internationaux et d'en poursuivre les auteurs. Le réseau réunit les points de contact nationaux des États membres de l'UE (procureurs, enquêteurs et agents spécialisés dans l'entraide judiciaire) ainsi que des représentants d'États observateurs, d'organes de l'Union européenne et des Nations Unies et d'autres entités, lors de réunions semestrielles qui permettent à ces praticiens d'échanger des informations, des expériences et des bonnes pratiques opérationnelles[50].

La présentation d'éléments issus de zones de conflit pour prouver des crimes internationaux requiert les mêmes analyses que pour les infractions à caractère terroriste. Cela étant, les crimes internationaux peuvent appeler des critères de preuve supplémentaires, par exemple la preuve de l'existence d'un conflit armé. À l'appui des éléments structurels et des faits spécifiques pertinents dans les affaires de crimes de guerre commis en Irak et en Syrie, par exemple, la Suède a utilisé des informations rassemblées par des ONG et par différents organes de l'ONU. Ces informations provenaient notamment de la Commission d'enquête internationale indépendante sur la République arabe syrienne, de la Mission d'assistance des Nations Unies pour l'Iraq (UNAMI), du Comité international de la Croix-Rouge (CICR), d'Amnesty International, de Human Rights Watch et de l'Institute for the Study of War. Bien que ces critères supplémentaires rendent encore plus difficile de prononcer des condamnations pour crimes internationaux, ils amplifient également la valeur potentielle des éléments recueillis sur les lieux mêmes où ces crimes ont été commis.

À l'avenir, il serait bénéfique de suivre la manière dont les États utilisent les informations recueillies dans les zones de conflit pour appuyer les poursuites des infractions liées au terrorisme et d'autres infractions pénales, afin de continuer à évaluer l'impact de ces informations sur l'avancement de la justice et l'obligation de rendre des comptes. Ce suivi permettra en outre d'identifier les défis persistants, de générer des discussions et de prendre les mesures appropriées au sein d'instances telles que le Comité du Conseil de l'Europe de lutte contre le terrorisme.

49. Amnesty International, « Germany/Iraq World's first judgement on crime of genocide against the Yazidis", 30 novembre 2021.
50. Voir Eurojust, « Genocide Network », disponible sur https://www.eurojust.europa.eu/judicial-cooperation/practitioner-networks/genocide-network.

Conclusion

Comme l'ont montré ces Pratiques comparées, les États ont la possibilité d'utiliser des informations recueillies dans des zones de conflit comme preuves dans des procédures pénales nationales ordinaires concernant des infractions terroristes et d'autres infractions. Différents types d'informations pertinentes peuvent être disponibles, issus d'une grande diversité de sources. Les États disposent d'une série de mécanismes pour accéder à ces informations et les partager, et peuvent prendre une série de mesures pour analyser la valeur probante des informations et en faciliter l'usage en tant que pistes d'enquête, moyens d'appui au processus judiciaire ou preuves devant un tribunal.

La description que nous venons de faire des méthodes et des pratiques n'est pas exhaustive. Les États vont sans nul doute continuer de trouver des techniques innovantes pour identifier, récupérer, partager et utiliser les informations pertinentes. Ce faisant, ils resteront tenus d'agir conformément aux lois nationales et aux normes internationales en matière de droits de l'homme et d'État de droit. Étant donné le nombre de groupes terroristes qui opèrent dans des zones de conflit ou en lien avec elles, les informations qui y sont recueillies vont conserver leur importance cruciale pour les procès relatifs aux infractions terroristes et pour la poursuite d'autres infractions, dont les actes interdits en vertu du droit international humanitaire. Les gouvernements devraient donc « continuer à renforcer la coopération internationale et la coordination nationale en matière d'utilisation d'informations provenant de zones de conflit comme preuves aux fins de poursuites pénales d'infractions terroristes et d'autres infractions[51] ». Ces Pratiques comparées devraient s'avérer instructives pour les personnes chargées des enquêtes, des poursuites, de l'élaboration des politiques, et pour tous les acteurs qui cherchent à faire un usage efficace de ces informations pour faire progresser la justice et amener les criminels à rendre des comptes.

51. CM/Rec(2022)8.

Questions fréquemment posées par les praticiens (FAQ)

Cette annexe aux Pratiques comparatives sur l'utilisation des informations recueillies dans des zones de conflit comme preuves dans le cadre de procédures pénales aborde un certain nombre de questions générales que les praticiens peuvent se poser sur les informations provenant des zones de conflit. L'objectif est de guider les praticiens dans le partage efficace de ce type d'informations et dans leur utilisation comme preuve lors d'enquêtes et de poursuites sur des infractions terroristes, ainsi que sur des actes interdits par le droit international humanitaire et d'autres infractions.

Comment les informations provenant des zones de conflit peuvent-elles consolider mon dossier ?

Les informations provenant des zones de conflit peuvent :

- **Établir ou corroborer l'identité d'un suspect**, ce qui peut s'avérer particulièrement difficile dans les affaires impliquant des crimes complexes et/ou des situations de conflit incertaines ;
- **Déterminer l'emplacement physique d'un suspect pendant une période donnée** ou à une date particulière, ce qui peut en soi constituer une infraction pénale, compte tenu des interdictions légales prévues par une majorité d'États de se rendre dans des zones de conflit particulières sans autorisation appropriée, et peut également aider à relier l'action du suspect par rapport à la scène et à l'heure d'un crime, à mettre en question la crédibilité d'un suspect ou d'un autre témoin, ou à désavouer un alibi ;
- **Démontrer l'appartenance d'un suspect à une organisation terroriste** (ce qui peut en soi constituer un crime dans certaines juridictions), y compris la volonté du suspect de commettre des actes criminels spécifiques (tels qu'un attentat suicide) ;
- **Apporter des éléments concernant un acte criminel particulier** qu'un suspect est accusé d'avoir commis, soit directement (par exemple à travers des photos ou des vidéos) soit à travers des déclarations fournies par des témoins, des victimes ou des coaccusés ;
- **Apporter des renseignements concernant les projets d'un suspect de commettre un crime** avant le passage à l'acte ou **décrivant le crime** après coup, ou aider de toute autre manière **à prouver l'intention de commettre un crime** d'un suspect ; et/ou
- Par ailleurs, **contribuer à établir la responsabilité pénale** pour les actes préparatoires, le financement du terrorisme ou la complicité de crimes.

Quels types d'informations provenant des zones de conflit peuvent exister ?

- **Matérielles** (par exemple, armes, composants d'engins explosifs improvisés, téléphones portables, disques durs et autres supports de stockage).
- **Numériques** (par exemple, données numériques, y compris les communications écrites, photos et vidéos ; données de trafic ; et autres données électroniques telles que les informations sur le portefeuille de crypto-monnaie).
- **Sur papier** (matériel imprimé ou manuscrit).
- **Communications téléphoniques ou autres interceptées** et images et prises du vues générées par satellite ou par système autonome sans pilote (UAS).
- **Déclarations et témoignages** (c'est-à-dire les déclarations faites volontairement par les accusés ou par d'autres personnes lors d'entretiens ou d'interrogatoires, ainsi que les témoignages, déclarations et autres informations fournies par des témoins, des victimes, des informateurs et d'autres sources humaines).

Comment puis-je identifier les informations pertinentes pour mon cas et les obtenir sous une forme utilisable ?

- **Coordonner avec les collègues** des services militaires et de renseignement par le biais des mécanismes interinstitutionnels existants pour déterminer quelles informations possèdent ces agences nationales.
- **Envisager toute la gamme d'options pour obtenir des informations auprès d'agences gouvernementales étrangères et de mécanismes intergouvernementaux** qui stockent et partagent des informations, et utiliser les méthodes les plus rapides et les plus efficaces adaptées au cas spécifique et au système juridique. Ces options peuvent inclure :
  - Engager des homologues étrangers directement par le biais des canaux du renseignement et des services répressifs ;
  - Introduire une demande formelle d'informations, y compris par le biais de l'entraide judiciaire et de décision d'enquête européenne (DEE) ; et
  - Effectuer des recherches dans les bases de données et systèmes d'information intergouvernementaux :
    - INTERPOL : contacter le Bureau Central National ;
    - Système d'information Schengen de l'Union européenne : demander aux autorités nationales compétentes de consulter une base de données commune ;
    - Système d'information d'Europol : demander aux autorités nationales désignées d'effectuer une recherche dans la base de données ;
    - Opération Gallant Phoenix : contactez l'attaché juridique du FBI de l'ambassade des États-Unis pour présenter une demande.
- **Vérifiez auprès des acteurs multilatéraux concernés** :
  - L'Équipe d'enquêteurs des Nations Unies chargée d'amener Daech/l'État islamique d'Iraq et du Levant à répondre de ses crimes (UNITAD)[52] ;
  - Le Mécanisme international, impartial et indépendant sur la Syrie : prendre contact avec l'IIIM via son site Web avant de passer à des processus plus sécurisés de partage d'informations ;
  - La Cour pénale internationale (CPI) : soumettre les communications au Bureau du Procureur par voie électronique via OTPLink.
- **Envisagez de contacter des acteurs non gouvernementaux** réputés et fiables (par exemple, des organisations de la société civile, des chercheurs et experts universitaires, des médias d'information, ainsi que des entreprises et entrepreneurs privés) pour les encourager à partager des informations au cas par cas.

Comment puis-je corroborer les informations sur les zones de conflit pour les utiliser comme preuve ?

- **Réanalyser et réexploiter tous les éléments matériels** ; **utiliser des copies** lorsque les originaux ne sont pas disponibles ; et **inclure des informations contextuelles**, telles que la documentation sur comment et quand les informations ont été collectées, transmises, stockées, analysées et partagées.
- **Utiliser du matériel supplémentaire** généré à partir de sources indépendantes (par exemple, médias sociaux et autres matériels numériques, communications interceptées, déclarations de témoins et entretiens avec les suspects eux-mêmes).
- **Utilisez des témoignages à l'appui**, non seulement de ceux qui ont recueilli les informations, mais également de représentants d'agences gouvernementales, de spécialistes techniques, d'experts ou de témoins possédant des connaissances pertinentes. **Envisager des mesures procédurales pour protéger les témoins vulnérables ou autrement sensibles**, y compris la protection physique, le déformation de la voix, l'anonymat et/ou les audiences par vidéo, lorsque cela est nécessaire et approprié.

Quelles considérations critiques dois-je garder à l'esprit ?

- **Une seule recherche ou demande peut ne pas suffire.** Le volume d'informations disponibles provenant des zones de conflit n'est pas figé, mais augmente constamment, à mesure que davantage d'informations sont recueillies et que les informations précédemment collectées sont traitées, traduites et/ou analysées

52. Dans la résolution 2697 (2023), le Conseil de sécurité des Nations Unies a prolongé le mandat de l'UNITAD jusqu'au 17 septembre 2024 seulement. Ainsi, bien que les informations de l'UNITAD aient été précieuses dans les enquêtes et les poursuites, en avril 2024, il reste à déterminer si les États auront accès à ces informations pour leurs affaires à l'avenir.

et exploitées. Même si une recherche d'informations est infructueuse ou donne des résultats insuffisants, **envisagez de la relancer ou de l'élargir au fur et à mesure que l'enquête avance**.

- **Les informations recueillies ou obtenues par l'armée ou les renseignements, ou par des acteurs multilatéraux ou non gouvernementaux, peuvent être admissibles comme preuve**. La plupart des pays n'imposent aucun obstacle catégorique à la présentation de telles informations au procès. Par conséquent, il faut considérer toutes les options avant de conclure qu'une information n'est pas admissible.
- **Les informations provenant d'une zone de conflit peuvent être pertinentes même si elles sont incomplètes, non vérifiées ou irrecevables** devant un tribunal. Considérez sa valeur pour démarrer ou faire avancer une enquête et pour générer des informations supplémentaires pouvant être utilisées comme preuve.
- **Les informations provenant des zones de conflit peuvent être pertinentes pour des crimes qui ont eu lieu ailleurs** (par exemple en démontrant qu'un suspect qui a commis des crimes ailleurs était membre d'une organisation terroriste) ou pour les suspects eux-mêmes situés ailleurs (par exemple en établissant des liens entre des crimes qui ont eu lieu dans une zone de conflit et ceux qui les ont financés).
- **Les affaires reposent rarement sur un seul élément d'information**, qu'il provienne d'une zone de conflit ou d'ailleurs. Les condamnations pénales reposent le plus souvent sur plusieurs types de preuves provenant de sources multiples, chaque élément de preuve contribuant à renforcer le dossier.

Quelles autres ressources puis-je consulter ?

- **Les sources pertinentes d'orientation** sur les informations provenant des zones de conflit comprennent :
  - Recommandation CM/Rec(2022)8 du Conseil de l'Europe du Comité des Ministres aux États membres sur l'utilisation d'informations recueillies dans des zones de conflit comme preuves dans le cadre de procédures pénales relatives à des infractions terroristes ;
  - Directives des Nations Unies relatives aux éléments de preuve recueillis par le personnel militaire ;
  - Mémorandum Eurojust 2020 sur les preuves recueillies sur le théâtre des opérations ;
  - Recommandations du Forum mondial de lutte contre le terrorisme d'Abuja sur la collecte, l'utilisation et l'échange d'éléments de preuve aux fins des poursuites pénales de terroristes présumés ;
  - Principes directeurs non contraignants des États-Unis relatifs à l'utilisation des preuves obtenues sur le champ de bataille dans la procédure pénale ordinaire.

Le Secrétariat du CDCT et l'IIJ tiennent à jour une liste d'experts qui ont contribué au développement de ces pratiques comparatives et qui ont de l'expérience dans l'utilisation des informations provenant des zones de conflit dans des affaires de terrorisme. Veuillez nous contacter pour poser une question ou pour fournir des commentaires sur ces pratiques comparatives.

Depuis plus de quarante ans, le Conseil de l'Europe contribue à l'élaboration et au renforcement de normes juridiques essentielles pour prévenir et réprimer les actes de terrorisme. Suivant une approche globale, il travaille à aider les États membres à lutter plus efficacement contre le terrorisme, en renforçant et améliorant leur législation nationale, facilitant ainsi la coopération internationale. Dans le plein respect des droits de l'homme et de l'État de droit, le Conseil de l'Europe œuvre en permanence à améliorer la coopération internationale pour traduire les terroristes en justice.

PREMS 108024

FRA

www.coe.int

Le Conseil de l'Europe est la principale organisation de défense des droits humains du continent. Il comprend 46 États membres, dont l'ensemble des membres de l'Union européenne. Tous les États membres du Conseil de l'Europe ont signé la Convention européenne des droits de l'homme, un traité visant à protéger les droits humains, la démocratie et l'État de droit. La Cour européenne des droits de l'homme contrôle la mise en œuvre de la Convention dans les États membres.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE