Mémorandum de New York sur les bonnes pratiques visant à empêcher les déplacements de terroristes

Introduction

À mesure que les combattants terroristes étrangers sont poussés hors des territoires autrefois occupés par l'EIIL/*Da'esh*, les États devraient adopter des mesures proactives afin de s'assurer que ces voyageurs sont détectés, identifiés, localisés et, s'il y a lieu, interceptés. La mise en œuvre efficace de mécanismes renforcés de détection de terroristes et la coopération internationale à des fins d'échange d'informations sont fondamentaux à cet effet.

En décembre 2017, le Conseil de sécurité des Nations Unies a adopté la Résolution du Conseil de sécurité des Nations Unies (RSCNU) 2396. Cette Résolution exige des États membres qu'ils élaborent et mettent en œuvre des systèmes de collecte de données biométriques et qu'ils mettent en place des listes de personnes à surveiller ou des bases de données de terroristes connus et présumés, en y incluant les combattants terroristes étrangers. Les États membres sont également tenus de collecter et d'analyser les renseignements préalables concernant les voyageurs (RPCV) et les données des dossiers passagers (sigle anglais : PNR) lors de contrôles aux frontières, afin de dissuader les terroristes connus et présumés de voyager, tout en exigeant des compagnies aériennes présentes sur leur territoire qu'elles fournissent les RPCV aux autorités nationales compétentes. Une analyse des données des dossiers passagers peut aider un pays à détecter des liens auparavant inconnus entre des terroristes et d'autres voyageurs. En outre, la RCSNU 2396 encourage les États membres à échanger ces informations par l'intermédiaire de mécanismes bilatéraux et multilatéraux. La mise en œuvre de ces dispositions de la RCSNU peut comporter de grandes complexités, exiger une haute intensité de ressources et se révéler onéreuse.

Reconnaissant ces défis, les États-Unis et le Maroc ont lancé en septembre 2018 une Initiative sous l'égide du Groupe de Travail du Forum mondial de lutte contre le terrorisme (GCTF) sur les combattants terroristes étrangers, visant à formuler des lignes directrices pour améliorer les mécanismes de détection de terroristes et les capacités d'empêcher les déplacements de terroristes. Le présent document est le résultat des enseignements tirés, des inquiétudes évoquées, des défis recensés et des études de cas échangées entre praticiens et décideurs politiques dans le but de corriger les failles systémiques perçues et de mettre en œuvre les mesures juridiques et politiques nécessaires pour sécuriser davantage les frontières contre les déplacements de terroristes, tout en veillant à la mise en œuvre de la RCSNU 2396.

En outre, le présent document fait la synthèse des thématiques abordées lors des ateliers régionaux de New York (États-Unis) ; Berlin (Allemagne), Kuala Lumpur (Malaisie) et Rabat (Maroc) ainsi que de leurs conclusions. Les lignes directrices non contraignantes que sont les Bonnes pratiques ici proposées doivent être considérées à la lumière des circonstances, des normes juridiques nationales, et des obligations et engagements internationaux de chaque État, notamment ceux qui relèvent du droit international des droits de l'homme, du droit international des réfugiés et du droit international humanitaire, selon le cas.

Bonnes pratiques

I. Cadres juridiques et politiques

Bonne pratique n° 1 : Établir des cadres juridiques et politiques relatifs aux listes de surveillance afin d'en faciliter la création au niveau national, et prévoir un processus exhaustif de tenue des listes des personnes à surveiller et de filtrage des passagers.

Des directives législatives et politiques peuvent se révéler nécessaires pour permettre aux agences de sécurité nationales d'établir un processus cohérent et rationalisé d'élaboration de listes de surveillance, qui soit en conformité avec les obligations imposées par le droit international. L'organisation de politiques et de lignes directrices pangouvernementales sur la tenue des listes de surveillance permet d'assurer avec la plus haute efficacité et effectivité la détection des déplacements de terroristes en vue de les empêcher. La législation doit prévoir la base juridique en vertu de laquelle les transporteurs de passagers se verraient obligés à fournir aux autorités compétentes des données relatives aux passagers, notamment les renseignements préalables concernant les voyageurs et/ou les données des dossiers passagers, en passant par un guichet unique et des systèmes dédiés.

Les autorités doivent également prendre des mesures pour préserver l'intégrité du processus de filtrage des passagers et protéger les informations à caractère personnel, particulièrement lors de la collecte et l'utilisation de données biométriques, des RPCV et des données des dossiers passagers. La tenue des listes de surveillance doit faire l'objet d'une supervision indépendante et transparente, par exemple sous la forme d'un contrôle judiciaire. Un mécanisme indépendant de radiation des listes de surveillance permettra le respect des droits de l'homme tout en garantissant un procès équitable, et les États devraient décider si un rôle doit être dévolu à cette fin aux tribunaux lors de l'inscription sur les listes ou de la radiation d'une personne de ces listes (voir Bonnes pratiques n^{os} 4 et 16). Les cadres juridiques et politiques devraient comporter des lignes directrices précisant les informations relatives à l'identité incluses dans les systèmes de filtrage, les raisons légitimes justifiant l'utilisation de ces informations, la durée de conservation de ces informations, les normes d'intégrité et de protection des données, et les procédures permettant de contester ou de rectifier toute inclusion illicite, inappropriée ou erronée dans une liste de surveillance (voir Bonne pratique n° 16). Il convient de désigner clairement, dans ce cadre, qui détient l'autorité pour communiquer certains identifiants biographiques et biométriques, de manière appropriée et uniquement à des fins de tenue de listes de surveillance de filtrage des passagers.

Organiser et décrire les processus et procédures interagences nationaux concernant les listes de surveillance dans un document unique, sur la base des lignes directrices juridiques et politiques, permettra de garantir l'utilisation uniforme des listes de surveillance entres les diverses agences gouvernementales et l'institutionnalisation des processus relatifs à la tenue de listes de surveillance et au filtrage des passagers, permettant ainsi de détecter et d'empêcher les déplacements de terroristes (voir Bonne pratique n° 5). Lors du développement des processus et procédures interagences nationaux d'élaboration de listes de surveillance, toutes les parties prenantes (responsables de l'origine, de l'inscription, de la tenue des listes de surveillance et du filtrage) doivent débattre des nouvelles procédures pour prendre en compte leurs effets potentiels[1].

[1] Ce document utilise les définitions suivantes : L'entité d'**origine** désigne la première entité responsable de la collecte et de l'identification des informations corroborant la suspicion qu'une personne est un terroriste connu ou présumé. L'entité d'**inscription** est celle qui dispose d'informations lui indiquant qu'une personne remplit les critères pour être qualifiée de terroriste connu ou présumé, et qui va procéder à l'inscription de cette personne sur une liste de surveillance, sur la base des informations provenant de cette même entité. L'entité de **tenue des listes de surveillance** désigne l'entité chargée d'entretenir les listes de surveillance de terroristes connus ou

Bonne pratique 2 : Organiser et appliquer les normes internationales concernant les processus relatifs aux listes de surveillance, et faire en sorte que la législation sur les RPCV/données PNR soit fondée sur les normes et pratiques internationales en vigueur.

Les organisations internationales telles que l'Organisation mondiale des douanes (OMD), l'Organisation de l'aviation civile internationale (OACI) et l'Association internationale du transport aérien (IATA) ont mis au point des normes et recommandé des pratiques visant à soutenir les opérations de filtrage des données relatives aux passagers qu'il serait bon que les États envisagent d'intégrer. L'OACI a promulgué des normes et recommandé des pratiques relatives aux RPCV à annexer à la *Convention relative à l'aviation civile internationale* (Convention de Chicago) et se prépare à faire de même pour les données PNR. Ces normes et pratiques constitueront un cadre juridique international établi permettant de promouvoir la coopération en matière de sécurité de l'aviation civile, d'intégrité des frontières et de facilitation, et seront un instrument efficace de rationalisation des capacités[2]. L'annexe 9 de la Convention de Chicago sur la facilitation prévoit déjà des normes et pratiques recommandées relatives aux renseignements préalables concernant les voyageurs et aux données des dossiers passagers. Ces dispositions renvoient aux documents d'orientation et aux lignes directrices de mise en œuvre des RPCV/données PNR développés par l'OMD, IATA et l'OACI. Tous les États doivent se conformer au cadre réglementaire international lors de la mise en œuvre des programmes RPCV/ données PNR. Les *Bonnes pratiques dans les domaines de la sécurité et de la gestion des frontières dans un contexte de lutte contre le terrorisme visant à endiguer la circulation des combattants terroristes étrangers* du GCTF ont également décrit des bonnes pratiques en matière de sécurité des frontières et de coopération internationale pouvant également servir de feuille de route aux États[3]. En outre, les *Recommandations d'Abuja sur la collecte, l'utilisation et le partage d'éléments de preuve aux fins des poursuites pénales de terroristes présumés* et d'autres documents de Bonnes pratiques du GCTF fournissent des orientations concernant le traitement des données et la gestion des affaires dans le cadre des poursuites judiciaires liées au terrorisme[4]. Les Nations Unies ont publié un *Compendium de la biométrie* afin d'aider les États dans leur processus d'intégration des technologies biométriques dans leurs systèmes de détection des déplacements de terroristes en vue d'empêcher ces déplacements[5].

Les États pourraient envisager de coopérer pour rendre compatibles leurs normes en matière d'inclusion sur les listes de surveillance, de fidélité des données, de méthodes de collecte et d'utilisations autorisées des informations contenues dans les bases de données. Cette compatibilité des normes fondamentales relatives à l'inclusion sur les listes de surveillance pourrait être codifiée à travers des accords législatifs ou politiques, tout en gardant à l'esprit les restrictions potentielles découlant du droit national de pays souverains. L'interopérabilité peut permettre de rationaliser la détection des déplacements de terroristes et l'interception des voyageurs concernés en renforçant la confiance entre partenaires internationaux, en réduisant l'ambiguïté quant aux mesures à prendre lors d'interactions, en améliorant la compatibilité des systèmes de filtrage, et en veillant à ce que les pratiques relatives aux listes de surveillance et à l'échange d'informations respectent les interdictions

---

présumés, qui accepte les inscriptions et communique les informations pertinentes aux entités de filtrage. Enfin, l'entité de **filtrage** désigne une entité qui utilise les informations recueillies dans les listes de surveillance à des fins de recoupement pour déterminer si une personne correspond à un terroriste connu ou présumé.

[2] Organisation de l'aviation civile internationale, *Annexe 9 de la Convention relative à l'aviation civile (« Convention de Chicago ») :* Facilitation, octobre 2017.

[3] GCTF, *Bonnes pratiques dans les domaines de la sécurité et de la gestion des frontières dans un contexte de lutte contre le terrorisme visant à endiguer la circulation des combattants terroristes étrangers,* Bonne pratique n° 3. www.theGCTF.org.

[4] GCTF, *Recommandations d'Abuja sur la collecte, l'utilisation et le partage d'éléments de preuve aux fins des poursuites pénales de terroristes présumés.* www.theGCTF.org.

[5] UNOCT, UNCTED, & Biometrics Institute, *United Nations Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter-terrorism*, 2018, 52.

de toute ingérence arbitraire ou illicite dans la vie privée et soient conformes aux autres obligations et engagements relatifs aux droits de l'homme.

Bonne pratique n° 3 : Mettre au point des mécanismes et des normes sur l'échange international d'informations et adopter, selon qu'il convient, une législation permettant cet échange.

On n'insistera jamais trop sur l'importance d'un échange conforme aux droits de l'homme, durable, systématique et complet (et non ponctuel, sporadique et partiel) des informations relatives au terroristes connus et présumés contenues dans les listes de surveillance. L'échange doit avoir lieu d'un commun accord et inclure des informations biographiques et contextuelles non confidentielles suffisantes pour que les États échangeant ces informations puissent prendre des mesures adéquates lors du repérage d'un individu suspect (voir Bonne pratique n° 9). Il doit être possible de procéder à de tels échanges indépendamment de tout déplacement, permettant ainsi une analyse préalable au voyage et la réception d'informations pertinentes en temps voulu[6]. Les États doivent envisager de conclure des accords écrits précisant les conditions de l'échange de données et incluant des dispositions relatives à la protection requise pour les informations échangées et à leurs utilisations autorisées.

La législation relative à la protection des données et de la vie privée doit prévoir suffisamment de possibilités pour que les transporteurs de passagers puissent révéler les données personnelles appropriées sur les passagers et les membres d'équipage à un pays étranger dans le but de lutter contre les déplacements de terroristes, à la condition qu'il existe une protection de la vie privée et une base juridique adéquates (voir Bonne pratique n° 14).

Bonne pratique n° 4 : Établir des mécanismes de supervision indépendants assurant le respect des normes d'insertion dans les bases de données.

Une surveillance appropriée aide aussi bien à assurer la protection des droits de l'homme et des libertés fondamentales qu'à améliorer la sécurité nationale. Protéger une base de données relative aux listes de surveillance contre l'inclusion de données insuffisantes ou illégales, ou bien contre l'inclusion d'individus pour des raisons politiques n'ayant aucun lien avec le terrorisme, et s'assurer que les processus de filtrage des passagers et de tenue de listes de surveillance respectent des normes convenues, aide à garantir la qualité, l'intégrité et la valeur de ces listes aussi bien pour leurs utilisateurs qu'aux yeux du public. Une autorité indépendante de suivi peut s'assurer du respect des exigences juridiques et de l'intégrité des données. Une organisation de supervision peut publier un rapport périodique garantissant que les activités de tenue de listes de surveillance et de filtrage sont menées conformément à la législation et aux directives nationales en vigueur, aux processus et procédures interagences et aux obligations internationales. Une telle organisation peut être appelée à recommander des mesures correctives pour pallier les failles et proposer des procédures d'alignement des pratiques nationales sur le droit international et les bonnes pratiques en vigueur[7].

---

[6] GCTF, *Mémorandum de La Haye-Marrakech sur les bonnes pratiques pour répondre plus efficacement au phénomène des combattants terroristes étrangers,* Bonnes pratiques n^{os} 10 et 12. www.theGCTF.org.

[7] L'*Additif aux Principes directeurs relatifs aux combattants terroristes étrangers (Principes directeurs de Madrid)* (2018) de l'ONU fournit davantage d'orientations sur l'élaboration des listes de surveillance et sur la coopération avec des partenaires bilatéraux et multilatéraux.

II. Élaboration et mise en œuvre des systèmes de filtrage des passagers

Bonne pratique n° 5 : Mobiliser l'ensemble des pouvoirs publics dans l'élaboration et la mise en œuvre de systèmes de filtrage des passagers.

Il incombe aux États d'assurer l'interopérabilité entre agences gouvernementales et en leur sein afin d'assurer un traitement rigoureux, précis et en temps voulu des informations contenues dans les systèmes de filtrage[8]. Cela comprend la rédaction de définitions et de normes juridiques précises relatives à l'inclusion sur les listes de surveillance, ainsi que l'harmonisation des formats de données et des configurations du système. Les États pourraient envisager d'adopter à cette fin une législation appropriée. S'assurer de l'interopérabilité des systèmes gouvernementaux internes permet un accès en temps voulu aux données pertinentes pour l'élaboration de listes de surveillance entre agences et systèmes, et contribue à une mise en œuvre cohérente des cadres juridiques et politiques[9]. Au cours des premières étapes de l'élaboration de systèmes de listes de surveillance, les États doivent s'assurer que leur personnel opérationnel et informatique coopère afin que les listes de surveillance répondent aux besoins des opérateurs et soient techniquement viables. Il est indispensable de tenir compte des apports de tous les utilisateurs de listes de surveillance avant l'élaboration des systèmes y afférant. Il convient également de s'assurer que les agences gouvernementales échangent régulièrement des informations afin de faciliter les réponses appropriées lors des interactions avec des personnes figurant sur une liste de surveillance. Les informations à échanger peuvent inclure des preuves recueillies sur le champ de bataille et des données biométriques collectées ou traitées par du personnel militaire (voir aussi Bonnes pratiques n^{os} 10 et 12).

Il serait bon que les agences gouvernementales pertinentes travaillent ensemble à la création des listes de surveillance et à l'organisation des processus et procédures de filtrage qui tiennent compte et mettent en œuvre les directives et lignes directrices juridiques et politiques provenant d'un niveau supérieur. Le document issu de cette coopération doit avoir pour vocation l'institutionnalisation des rôles et responsabilités des agences dans l'alimentation des listes de surveillance et l'utilisation des informations contenues sur ces listes. Le document doit établir des définitions, des normes et des exigences générales en matière de données concernant l'élaboration de listes de surveillance, notamment des exigences biographiques et biométriques ainsi que des pratiques de conservation des données. Le document doit être régulièrement mis à jour et mis à la disposition de tous les utilisateurs des listes de surveillance, notamment les parties prenantes politiques, juridiques et opérationnelles (voir Bonne pratique n° 1).

Les États pourraient désigner une seule agence qui deviendrait le centre des informations relatives aux passagers, et serait responsable du traitement des données et du signalement de passagers figurant sur ces listes aux autorités compétentes. Cette approche du « guichet unique » permet de réduire les retards administratifs ainsi que les coûts, et d'éviter tout accès abusif aux informations contenues dans les bases de données.

---

[8] GCTF, *Mémorandum de La Haye-Marrakech sur les bonnes pratiques pour répondre plus efficacement au phénomène des combattants terroristes étrangers,* Bonne pratique 11. www.theGCTF.org.

[9] GCTF, *Bonnes pratiques dans les domaines de la sécurité et de la gestion des frontières dans un contexte de lutte contre le terrorisme visant à endiguer la circulation des combattants terroristes étrangers,* Bonne pratique 2. www.theGCTF.org.

Bonne pratique n° 6 : Mobiliser des partenaires internationaux dans l'élaboration et la mise en œuvre de systèmes de filtrage des passagers.

Les États pourraient envisager de forger des partenariats avec d'autres États ou avec des organisations internationales possédant une expérience spécialisée dans les systèmes de filtrage des passagers et offrant des outils de soutien et informatiques permettant d'assurer l'efficacité et la durabilité de ces systèmes sur le long terme[10]. Plusieurs États offrent déjà leur soutien à d'autres pays en partageant leurs propres législations et guides de mise en œuvre, en proposant des formations et un soutien technique. Des organisations internationales telles que le Bureau de lutte contre le terrorisme des Nations Unies[11], l'OMD et l'Organisation pour la sécurité et la coopération en Europe (OSCE) proposent des programmes de renforcement des capacités et des solutions logicielles permettant d'améliorer les aptitudes de détection des terroristes.

Bonne pratique n° 7 : Mobiliser les transporteurs aériens et les partenaires de l'industrie et du secteur privé en vue de rationaliser l'élaboration et la mise en œuvre des systèmes de filtrage des passagers.

Il convient, si possible, de consulter et d'établir des partenariats ainsi que de coopérer avec les parties prenantes pertinentes du secteur privé, dont les transporteurs nationaux et multinationaux, dans l'établissement des fondements réglementaires et des caractéristiques techniques des systèmes de filtrage des passagers. Cette mobilisation permet de garantir l'engagement des partenaires du secteur privé chargés de la mise en œuvre des réglementations de transfert de données passagers, là où elles existent, et permet aussi d'en garantir la conformité et l'efficacité. Les parties prenantes du secteur privé sont susceptibles d'avoir acquis ailleurs une expérience en matière de mise en œuvre de ces systèmes et peuvent offrir leur savoir-faire procédural dans la mise en œuvre, permettant ainsi l'alignement des systèmes nationaux sur les bonnes pratiques internationales et leur conformité. Dans un premier temps, les États peuvent envisager d'établir des partenariats avec un seul transporteur aérien, afin de bêta-tester le fonctionnement de ces systèmes, servant de galop d'essai avant une mise en œuvre à l'échelle du secteur. La préparation d'un document de mise en œuvre technique incluant les informations requises et les normes relatives à la transmission, ainsi qu'un calendrier de la mise en conformité, destiné au secteur privé, peuvent aider à assurer une conception et un fonctionnement efficaces des systèmes de filtrage des passagers.

Bonne pratique n° 8 : Évaluer les ressources disponibles, les capacités et les besoins pour la mise en place des systèmes de filtrage.

Au moment d'envisager la mise en œuvre de systèmes de filtrage des passagers, les États doivent choisir des systèmes qui répondent à leurs besoins et tiennent compte de leurs capacités. L'utilisation des RPCV et de données des dossiers passagers doit renforcer et, à terme, améliorer la facilitation du passage des voyageurs aux postes de contrôle en permettant aux gardes-frontières de porter leur attention sur les passagers à plus haut risque. Les systèmes locaux de traitement et recoupement de renseignements préalables concernant les voyageurs et de données des dossiers passagers peuvent certes permettre une réduction des coûts, mais exigent cependant une plus grande capacité d'entretien et un besoin de personnel onéreux car hautement qualifié. Autrement, les États peuvent

[10] OSCE, *Outcome Document from the 2nd OSCE-wide Seminar on Passenger Data Exchange*, SEC.GAL/190/18 (3 décembre 2018). www.osce.org.

[11] Le Bureau de lutte contre le terrorisme des Nations Unies coordonne les efforts de renforcement des capacités basé sur le système logiciel goTravel, offert aux États membres dans le processus d'élaboration et de mise en œuvre de systèmes de transfert des données passagers en apportant une aide technique et technologique gratuite. https://www.un.org/cttravel/goTravel

également travailler avec des partenaires commerciaux, multilatéraux ou bilatéraux dans le développement et la mise en œuvre de tels systèmes (voir Bonne pratique 2). Les États doivent également mettre en œuvre des stratégies alignées sur les normes internationales afin de garantir leur compatibilité avec les systèmes de compagnies aériennes déjà existants, d'engranger des gains d'efficacité, de réduire les coûts et d'accélérer la mise en œuvre. En plus du cadre juridique international figurant à l'annexe 9 de l'OACI, l'OMD, l'OACI et IATA proposent aux États des lignes directrices de mise en œuvre de ces systèmes[12].

Bonne pratique n° 9 : Faire en sorte que les systèmes de filtrage des passagers offrent un accès en temps opportun à des données actualisées, complètes et exploitables.

Les autorités ont besoin d'accéder à des données actualisées, spécifiques et exactes afin de prendre des mesures adéquates et éclairées. Les systèmes doivent permettre d'obtenir des informations émanant de sources publiques, telles que les rapports d'enquêtes ou les actualités, disponibles en ligne, afin de procéder à une mise à jour rapide des informations relatives aux personnes figurant sur les listes de surveillance. Le système doit être flexible et permettre d'intégrer et d'exporter de multiples formats de données et de supporter l'enrichissement futur des jeux de données. Le système de listes de surveillance doit bénéficier d'un soutien technique à tout moment, fourni par un service d'assistance technique, afin d'empêcher qu'un problème technique ne ralentisse l'accès aux données. Les États doivent accorder une attention particulière aux champs à remplir dans leur base de données. Ajouter aux données des informations contextuelles peut également permettre aux autorités de prendre les mesures appropriées en temps voulu. Afin de garantir la sécurité complète des frontières, il convient que les utilisateurs finaux puissent se connecter à tout moment aux listes de surveillance et sachent que leurs mises à jour sont régulières. Tous les systèmes mobilisés dans le filtrage des passagers doivent être connectés et pouvoir se relier aux listes de surveillance nationales en temps réel. En outre, les autorités gouvernementales responsables doivent avoir accès aux bases de données et aux notices pertinentes de l'Organisation internationale de police criminelle (INTERPOL) à travers la plateforme I-24/7 (voir Bonne pratique n° 13). Un processus d'analyse des données relatives aux passagers, à l'aide d'un système de ciblage automatisé – avant, pendant et après un voyage aérien, maritime, ferroviaire et routier (en autocar) – peut permettre de révéler des tendances et garantir un niveau de fidélité accru par rapport aux évaluations menées dans le vide.

Bonne pratique n° 10 : Collecter et utiliser de manière responsable les informations biométriques pour une fidélité et une précision accrues des bases de données de filtrage.

Les systèmes de collecte biométrique interopérables avec les systèmes de filtrage et ceux des forces de maintien de l'ordre peuvent fusionner leurs informations afin d'identifier plus précisément les terroristes connus et présumés. La biométrie permet de réduire considérablement les risques d'identification erronée d'une personne fondée uniquement sur des données biographiques, et permet de détecter les personnes voyageant avec de faux documents en reliant les données biométriques aux passeports. Toute donnée biométrique utilisée comme preuve dans un tribunal doit avoir été collectée légalement, et toute preuve recueillie sur le terrain doit l'être conformément aux obligations nationales et internationales, ainsi qu'aux bonnes pratiques énoncées dans les *Recommandations d'Abuja sur la collecte, l'utilisation et le partage d'éléments de preuve aux fins des poursuites pénales de terroristes présumés* du GCTF[13].

---

[12] OACI, *Guidelines on Passenger Name Record (PNR) Data, 2010 ; OACI, International Standards and Recommended Practices: Annex 9 to the Convention on International Civil Aviation "Chicago Convention"* – Facilitation, chapitre 9, octobre 2017 ; OMD, IATA, et OACI, *Guidelines on Advance Passenger Information (API),* 2014.

[13] GCTF, *Recommandations d'Abuja sur la collecte, l'utilisation et le partage d'éléments de preuve aux fins des poursuites pénales de terroristes présumés,* Recommandations 20-21. www.theGCTF.org.

III. Échange et accès à l'information

Bonne pratique n° 11 : Entretenir un équilibre entre « besoin de savoir » et « responsabilité de partage » en améliorant la coopération inter- et intra-agences.

Afin que les bases de données de filtrage fonctionnent comme prévu, les agences gouvernementales doivent surmonter leurs réticences à échanger les renseignements sur les personnes figurant sur les listes de surveillance et les informations sous-jacentes avec les agences de renseignements et les autorités de première ligne, telles que les forces de l'ordre, les gardes-frontières et les agents consulaires. Les États peuvent envisager plusieurs stratégies visant à encourager une telle coopération tout en protégeant les renseignements à caractère sensible[14].

L'établissement d'un centre de fusion d'informations pour le filtrage des passagers, auquel seraient affectés des agents du renseignement aux côtés de représentants des forces de l'ordre peut être un mécanisme efficace permettant d'assurer l'intégration en temps voulu des informations dans la base de données appropriée, tout en garantissant l'accès à ces informations aux autorités compétentes grâce à la possibilité de consulter les services du renseignement et d'obtenir des réponses en temps quasi réel. En l'absence d'un tel centre de fusion, des solutions informatiques et techniques peuvent servir le même objectif. Le fait de séparer et de protéger les informations confidentielles sous-jacentes (provenant des services du renseignement ou d'informateurs) dans une base de données distincte de celle contenant des informations non confidentielles de nature contextuelle et personnelle (la liste de surveillance) protège les réseaux du renseignement et permet aux agents des services du renseignement d'être plus à l'aise dans leurs échanges réguliers d'informations relatifs aux listes de surveillance.

Dans les cas où il n'est pas possible de consulter un agent de ces services, des algorithmes de recoupement de données et une analyse informatisée des recherches ou des demandes d'informations par les agents de première ligne permettront de déverrouiller l'accès à des informations de filtrage plus sensibles, lorsque la situation le justifie, sans porter atteinte à l'intégrité des informations. De tels outils sont d'autant plus fructueux qu'ils sont associés à des systèmes interopérables qui distribuent et fournissent l'accès aux données à l'ensemble des agences gouvernementales. L'établissement d'un cycle complet d'échange d'informations permet de protéger les données confidentielles tout en facilitant un large accès aux informations de filtrage non confidentielles. Cela permet de compléter les données non confidentielles avec des données confidentielles lorsque la présence d'un possible suspect justifie un tel accès à ces dernières.

Bonne pratique n° 12 : Organiser les structures et les processus de tenue de listes de surveillance de sorte à permettre un accès efficace et efficient à l'information.

Lors de l'attribution des rôles et responsabilités relatifs à la tenue des listes de surveillance, les administrateurs de ces listes doivent être distincts des entités responsables de l'origine, de l'inscription et du filtrage des informations afin d'éviter les biais dans l'utilisation des informations et dans l'analyse de leur qualité et fiabilité. Les États devraient se doter d'une norme faisant une distinction claire entre les données à haut risque et les données à faible risque, en fonction des informations sur des menaces sous-jacentes, dans le but d'assurer une meilleure gestion des informations en temps opportun. Les normes d'accès à l'information doivent se fonder sur les besoins et les capacités des entités de filtrage plutôt que sur le corpus de données disponibles. Les informations provenant d'interactions avec des personnes figurant sur une liste de surveillance peuvent être utilisées pour compléter les bases de données, en tant que de besoin. Afin d'identifier

[14] Voir l'*Additif aux Principes directeurs de Madrid de 2015 (2018),* Bonne pratique 2 pour plus d'orientations sur l'intégration des systèmes.

plus efficacement les personnes figurant sur les listes de surveillance, il convient de regrouper les différentes identités d'une même personne sous une seule entrée afin d'éviter que la personne n'apparaisse plusieurs fois sous ses différentes identités connues.

Bonne pratique nº 13 : Utiliser les bases de données multilatérales existantes pour traiter les données relatives aux passagers et en faciliter l'échange international.

Les États doivent travailler avec les organisations internationales chargées de l'application de la loi, telles qu'INTERPOL, afin de fournir autant d'informations que la loi le permet sur des personnes suspectes et de filtrer les passagers en utilisant toutes les informations disponibles[15]. La transmission de mises à jour cohérentes à INTERPOL permet de préserver l'exactitude et la pertinence de sa base de données au profit de toutes les parties prenantes ; à l'inverse, le filtrage en temps réel réalisé à l'aide des bases de données d'INTERPOL produit un effet multiplicateur. Équiper les agents locaux des forces de l'ordre d'un accès aux bases de données d'INTERPOL permet d'aider à identifier des terroristes connus et présumés. Il incombe aux États de fournir autant d'éléments de contexte que possible relatifs aux identités signalées à INTERPOL afin d'aider la police à prendre des décisions en cas de correspondance avec une entrée de la liste. Les États doivent également envisager de créer ou d'enrichir des bases de données régionales afin d'échanger des informations de filtrage, permettant ainsi de détecter et d'empêcher les déplacements de terroristes à l'échelle régionale.

IV. Vie privée, droits et recours

Bonne pratique nº 14 : Prendre des mesures proactives afin d'assurer la sécurité et la confidentialité des listes de surveillance et des informations relatives aux passagers.

Les États devraient veiller à la mise en place et à la normalisation de mesures d'intégrité des données contenues dans les bases de données nationales et internationales. La collecte, le stockage, l'utilisation et l'échange d'informations relatives aux passagers et de données biométriques doivent se poursuive en conformité avec les moyens autorisés par la loi. Prévoir une clause de suppression automatique dans la législation ou les politiques peut être un bon moyen de s'assurer que les personnes ne remplissant plus les critères d'inclusion soient retirées de la liste (voir Bonnes pratiques nºs 1 et 5 relatives à la création d'un document national d'orientation exhaustif sur l'élaboration de listes de surveillance).

En l'absence de normes multilatérales relatives aux listes de surveillance protégeant l'intégrité des données et garantissant l'absence de toute ingérence arbitraire ou illégale, les informations confidentielles sous-jacentes à une liste de surveillance doivent être échangées de manière bilatérale à travers des dispositifs internationaux qui incluent des mesures de protection de l'intégrité des données et de la vie privée[16].

---

[15] GCTF, *Bonnes pratiques dans les domaines de la sécurité et de la gestion des frontières dans un contexte de lutte contre le terrorisme visant à endiguer la circulation des combattants terroristes étrangers,* Bonne pratique 3. www.theGCTF.org.

[16] OSCE, *Outcome Document from the 2nd OSCE-wide Seminar on Passenger Data Exchange*, SEC.GAL/190/18 (3 décembre 2018). www.osce.org.

Bonne pratique n° 15 : S'assurer que la collecte et l'utilisation des informations provenant des listes de surveillance et les informations relatives aux passagers soient alignées sur le droit national et sur les obligations et engagements internationaux.

Les États doivent définir un ensemble de normes claires et transparentes fondées sur les risques dans le but de déterminer quels individus devront figurer sur une liste de surveillance, sur la base de critères raisonnables et factuels. Le droit international interdit l'inscription de toute personne sur une liste de surveillance pour des raisons politiques ou pour tout motif discriminatoire. Tous les dispositifs d'échange d'informations doivent comporter des garanties permettant de s'assurer que l'information fournie par un partenaire à un autre ne sera pas utilisée à mauvais escient, par exemple dans le cadre de violations ou d'atteintes aux droits de l'homme. Des contrôles doivent être mis en place, et dûment réexaminés, afin de garantir que les données figurant dans les listes de surveillance et les informations relatives aux passagers ne sont pas utilisées à des fins de profilage non conforme aux obligations des États en vertu du droit national ou international[17]. Plus particulièrement, les États doivent s'assurer que les listes de surveillance et les bases de données d'informations relatives aux passagers n'exercent aucune discrimination fondée sur la race, la couleur, le sexe, la langue, la religion, l'opinion politique ou toute autre conviction, l'origine nationale ou sociale, la fortune, la naissance ou tout autre situation, comme le prévoit le droit international. Les autorités ayant accès aux informations des listes de surveillance doivent être dûment formées en matière de protection juridique des personnes, notamment en ce qui concerne les droits fondamentaux de chacun à entrer dans son propre pays, le principe d'égalité devant la loi et le droit à une égale protection de la loi[18].

Les informations biométriques peuvent être un puissant outil permettant d'améliorer les capacités d'identification (voir Bonne pratique n° 10). Mais elles peuvent également présenter un danger, celui de révéler accidentellement et sans consentement des informations privées non pertinentes et à caractère personnel susceptibles d'être utilisées à des fins illicites. Il est donc indispensable de s'assurer que la collecte, le stockage, le traitement et la transmission des données biométriques se font de manière sécurisée. Les risques évoqués peuvent être minimisés par une utilisation des systèmes biométriques en conformité avec les normes internationales et par l'accréditation formelle de la police scientifique, deux facteurs qui contribuent aux garanties procédurales et à l'efficacité de la supervision[19].

Bonne pratique n° 16 : Mettre en œuvre des mécanismes de vérification de l'exactitude des données collectées, ainsi que des voies de recours accessibles à toute personne pour contester son statut dans une base de données de détection de terroristes (« recours »)

Les individus inscrits par inadvertance ou à tort dans une base de données de détection de terroristes doivent disposer de voies de recours accessibles, claires, rapides, et suffisamment transparentes pour pouvoir contester une décision, demander un réexamen et faire retirer toute information erronée. La remise en question d'une insertion douteuse dans une base de données doit faire l'objet de procédures de traitement adéquates afin de garantir la protection de toute information confidentielle ou autrement sensible. Des mécanismes de révision automatisée des données peuvent permettre

---

[17] L'article 12 de la *Déclaration universelle des droits de l'homme* énonce clairement des paramètres de protection de la vie privée individuelle et de protection de ces droits en vertu de la loi en vigueur. https://www.un.org/fr/universal-declaration-human-rights/

[18] Voir : Bureau de lutte contre le terrorisme des Nations Unies, *Les droits de l'homme et les contrôles effectués dans le cadre de la sécurité et de la gestion des frontières. Guide de poche sur le contrôle des frontières,* édition 2018. https://www.un.org/counterterrorism/ctitf/.

[19] Pour un examen plus approfondi de ces outils et orientations biométriques, voir UNOCT, UNCTED, & Biometrics Institute, *United Nations Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter-terrorism*, 2018, 52.

d'identifier les informations erronées de manière efficace et en temps voulu. En outre, les parties prenantes inter-agences doivent pouvoir exiger une révision ou un recours efficace d'une identité spécifique figurant sur une liste de surveillance afin de préserver l'exactitude de la base de données, de concentrer les ressources de sécurité sur des menaces crédibles, et de fournir des programmes de sécurité nationale de confiance au public.

Conclusion

La pleine mise en œuvre de la RCSNU 2396 est indispensable afin de détecter les déplacements de terroristes et de prendre les mesures appropriées pour répondre au défi posé par ces déplacements. Le partage d'expériences et de bonnes pratiques à travers la présente Initiative du GCTF a pour but de faciliter le développement et l'utilisation des listes de surveillance, des données biométriques, des renseignements préalables concernant les voyageurs, des données des dossiers passagers, et autres outils relatifs au filtrage des passagers dans la lutte contre les déplacements de terroristes dans le monde. Le présent document est conçu comme une ressource destinée aux États, afin qu'ils développent et mettent en œuvre des systèmes et procédures d'élaboration de listes de surveillance permettant la détection des terroristes, conformément à la RCSNU 2396.

Des processus interagences fragmentés ou insuffisamment développés ainsi que des capacités limitées de filtrage et de tenue de listes de surveillance pourraient priver les États de la possibilité de fournir aux entités de filtrage et aux agents de première ligne l'accès aux informations critiques nécessaires pour élaborer une réponse appropriée lors des interactions avec des terroristes connus et présumés. Un cadre juridique et politique complet est nécessaire à l'élaboration d'un processus de filtrage adapté et rationalisé. Les États devraient développer une stratégie pangouvernementale permettant de garantir l'actualité, l'exactitude et l'exploitabilité des informations recueillies dans les listes de surveillance. L'échange institutionnalisé d'informations facilite le partage de données entre les parties prenantes nationales pertinentes, tout en protégeant les renseignements confidentiels. Les échanges d'informations entre agences nationales sont indispensables, mais doivent être complétés par un échange approprié d'informations à l'échelon international afin de lutter contre les déplacements de terroristes dans le monde. En outre, le respect de la vie privée et des droits de l'homme ainsi que l'existence de voies de recours sont essentiels afin d'éviter toute utilisation abusive de ces systèmes à des fins politiques et pour obtenir l'adhésion du public aux mesures de traitement des données, de gestion des listes de surveillance, ainsi qu'aux mesures coercitives et aux opérations de protection qui pourraient s'ensuivre.