Nations Unies CTOC/COP/WG.2/2017/L.1/Add.2–CTOC/COP/WG.3/2017/L.1/Add.2

Conférence des Parties à la Convention des Nations Unies contre la criminalité transnationale organisée

Distr. limitée
13 octobre 2017
Français
Original: anglais

Groupe de travail sur la coopération internationale
Vienne, 9-13 octobre 2017

Groupe de travail d'experts gouvernementaux sur l'assistance technique
Vienne, 11-13 octobre 2017

Projet de rapport sur les travaux des réunions du Groupe de travail sur la coopération internationale et du Groupe de travail d'experts gouvernementaux sur l'assistance technique tenues à Vienne du 9 au 13 octobre 2017

Additif

III. Résumé des délibérations (*suite*)

Groupe de travail sur la coopération internationale

C. Faits nouveaux en matière d'obtention de preuves électroniques (point 4 de l'ordre du jour)

1. À sa 3e séance, le 10 octobre 2017, le Groupe de travail sur la coopération internationale a examiné le point 4 de l'ordre du jour, intitulé "Faits nouveaux en matière d'obtention de preuves électroniques". Au titre de ce point, les intervenants ont mis en lumière les principales difficultés auxquelles se heurtaient leurs pays pour obtenir et communiquer des preuves électroniques, et les bonnes pratiques qu'ils adoptaient à cet égard. La plupart des intervenants ont souligné que les preuves électroniques constituaient une part essentielle de l'enquête dans la quasi-totalité des affaires transnationales complexes concernant des infractions graves, car les groupes criminels organisés profitaient de plus en plus de l'anonymat que permettaient les technologies actuelles de l'information et des communications pour commettre des crimes, atteindre leurs victimes ou développer leurs activités, mais aussi pour dissimuler l'origine des produits de leurs activités illégales. Des intervenants ont cité, au nombre de ces crimes, la fraude, la criminalité liée à l'identité, l'utilisation d'Internet à des fins terroristes, le trafic de stupéfiants et d'armes à feu, la traite des êtres humains, les crimes commis contre des enfants ou des femmes et l'utilisation du darknet pour les commettre.

2. Plusieurs intervenants ont déclaré que le nombre de demandes d'entraide judiciaire liées à l'obtention de preuves électroniques ou à leur préservation augmentait très rapidement, et de nombreux autres ont fait remarquer que les méthodes utilisées actuellement pour traiter ces demandes n'étaient pas suffisamment efficaces, tant du point de vue du fond que des délais, en raison de la nature éphémère et précaire des données électroniques. À cet égard, on a souligné qu'une coopération et une coordination avec le secteur privé étaient vitales pour garantir la préservation des données et l'accès à ces données. Comme exemples de bonnes pratiques, des intervenants ont cité, au niveau national, la coopération entre les autorités de la justice

Merci de recycler

pénale et les fournisseurs d'accès à Internet, qui permettait de préserver les données électroniques avant que la justice n'autorise à les obtenir, et, au niveau international, la présentation de demandes de préservation des données avant la communication officielle d'une demande d'entraide judiciaire. L'utilisation de moyens électroniques pour communiquer les demandes d'entraide judiciaire a également été citée comme exemple de bonne pratique, et de nombreux intervenants ont déclaré que leurs services travaillaient essentiellement, sinon exclusivement, avec des documents électroniques. Des intervenants ont également noté qu'une coopération dans le cadre de réseaux fonctionnant de manière ininterrompue facilitait la préservation des données.

3. De nombreux intervenants ont souligné qu'il importait que les entreprises utilisant des monnaies virtuelles se conforment aux normes internationales en matière de lutte contre le blanchiment d'argent, y compris aux recommandations du Groupe d'action financière, comme celles qui portent sur les mesures de vigilance, en déterminant la source et la destination des avoirs et le but de leurs mouvements, et en luttant contre le financement du terrorisme.

4. La plupart des intervenants ont souligné qu'une spécialisation était nécessaire et qu'il était donc crucial d'organiser, à l'intention des professionnels concernés, des cours sur le traitement des preuves électroniques et sur leur utilisation dans des enquêtes et des procédures pénales. À cet égard, on a noté que les agents des services de répression qui se trouvaient en première ligne, les avocats, les procureurs, les juges et ceux qui travaillaient avec ces professionnels de la justice pénale devaient recevoir une formation adaptée afin d'être en mesure de recueillir des preuves électroniques, de mener des expertises judiciaires numériques, d'utiliser ces preuves au tribunal et de les communiquer à leurs homologues étrangers lorsqu'ils traitaient des affaires transnationales. Quelques intervenants se sont déclarés satisfaits du travail que l'ONUDC accomplissait dans leurs pays ou leurs régions pour dispenser des cours sur ces sujets, et ils ont demandé qu'il continue à fournir une assistance technique dans ce domaine, tant au niveau national qu'au niveau régional. On a aussi noté que, pour que des preuves électroniques puissent être recevables par les tribunaux, il fallait que le droit interne le prévoie. Ainsi, de nombreux intervenants ont décrit les mesures prises par leurs pays pour adopter les lois nécessaires ou actualiser celles qui étaient en vigueur (qu'elles soient matérielles ou procédurales). Ces informations ont été complétées, dans de nombreux cas, par des informations sur des initiatives nationales prises au niveau institutionnel pour créer des centres de cybersécurité ou de prévention et de lutte contre la cybercriminalité, ou pour mettre en place, au sein du système de justice pénale et des services de détection et de répression, des unités spéciales chargées de lutter contre la cybercriminalité. Plusieurs intervenants ont indiqué que la coopération avec des organisations internationales telles qu'INTERPOL et le Conseil de l'Europe, ainsi qu'avec des organisations régionales telles que l'Organisation des États américains facilitait la mise au point d'une législation nationale adaptée sur la cybercriminalité et les preuves électroniques.

5. Se référant aux travaux du groupe d'experts intergouvernementaux à composition non limitée chargé de mener une étude approfondie sur le problème de la cybercriminalité, certains intervenants ont souligné qu'il serait utile, y compris pour la Conférence des Parties et son Groupe de travail sur la coopération internationale, de prendre en compte les futurs travaux de ce groupe d'experts, en particulier sur l'échange d'informations sur les législations nationales, les pratiques de référence, l'assistance technique et la coopération internationale faisant intervenir des preuves électroniques, et conformément à la résolution 26/4 de la Commission pour la prévention du crime et la justice pénale.

IV. Organisation des réunions

B. Déclarations (*suite*)

6. Au titre du point 4 de l'ordre du jour du Groupe de travail sur la coopération internationale, des déclarations ont été faites par les représentants des États parties à la Convention suivants: Algérie, Brésil, Chine, Colombie, Côte d'Ivoire, Équateur, États-Unis d'Amérique, Iraq, Jamaïque, Japon, Kenya, Maurice, Mexique, Nigéria, Oman, République-Unie de Tanzanie, Roumanie, Rwanda, Soudan, Sri Lanka et Suisse.