États-Unis d'Amérique

Le gouvernement des États-Unis d'Amérique se fait un plaisir de répondre à l'invitation lancée aux États Membres de l'Organisation des Nations Unies de présenter leurs vues sur la portée, les objectifs et les éléments structurels de la nouvelle convention, concernant l'application des résolutions 74/247 et 75/282 de l'Assemblée générale de l'Organisation. Les États-Unis attendent avec impatience d'œuvrer de concert avec les autres États Membres et les parties prenantes intéressées pour produire un instrument mondial axé sur un renforcement des processus d'enquête et de poursuites judiciaires relatifs à la cybercriminalité conforme aux droits et obligations en vigueur et faisant fond sur eux. Les États-Unis réitèrent l'importance du maintien d'un processus ouvert, inclusif, transparent et à multiples parties prenantes qui permettra à tous les États Membres de négocier de bonne foi en vue de l'adoption de solutions pratiques, bien informées et à base consensuelle, ce qui, estiment-ils, encouragera une large adhésion à un nouvel instrument mondial de lutte contre la cybercriminalité.

La date butoir proposée pour notre travail impose des contraintes temporelles qui seraient exigeantes en temps ordinaire, mais qui le sont encore davantage étant donné le contexte de la pandémie mondiale dans lequel s'inscrit ce travail. Ceci ne fait qu'accroître la nécessité de focalisation et d'efficience de nos efforts dans les négociations visant à la formulation d'un instrument mondial de lutte contre la cybercriminalité. Malheureusement, alors que la majorité du monde s'emploie à combattre la pandémie de COVID-19, les cybercriminels ont exploité la tendance générale, résultant de ce combat, à faire appel aux technologies numériques. La cybercriminalité constitue une menace directe pour la sécurité et le bien-être des sociétés et des habitants du monde entier. Nous coopérons de longue date pour renforcer notre capacité collective de lutte contre une telle exploitation et nous pouvons continuer de progresser en nous

fondant sur les succès remportés, en examinant soigneusement les possibilités de solutions pratiques. L'immédiateté de la menace de la cybercriminalité vient encore accroître la nécessité primordiale d'une action focalisée et délibérée de notre part dans les négociations visant à la production d'un instrument mondial de lutte contre la cybercriminalité.

Cet instrument devrait viser à renforcer la coopération internationale et à équiper les forces de l'ordre nationales d'outils pratiques pour combattre la cybercriminalité, ainsi que l'ont fait d'autres instruments des Nations Unies pour lutter contre d'autres formes de criminalité transnationale, notamment la corruption, le trafic des stupéfiants, la traite de personnes et le trafic de migrants. Il devrait également permettre aux autorités nationales de recueillir et d'obtenir des preuves électroniques relatives à tout type d'infraction criminelle, pas seulement les infractions cyberdépendantes, et promouvoir la coopération internationale en la matière. À l'instar de tous les instruments des Nations Unies visant la lutte contre la criminalité, les outils adoptés devraient être sujets à des limites et à des garanties appropriées, dans le contexte des dispositions nationales en vigueur, pour tenir compte de la vie privée et des libertés civiles tout en respectant pleinement les droits de l'homme. Le nouvel instrument de lutte contre la cybercriminalité devrait également répondre au besoin croissant d'assistance technique et offrir aux États Membres des modalités de demande de cette assistance.

Alors que les États Membres entament le processus d'élaboration du nouvel instrument, il est essentiel qu'ils sachent qu'ils n'œuvrent pas en vase clos. Si important qu'il soit de définir le champ de cet instrument, il est d'une importance égale de reconnaître ce qui se situe hors de ses limites. Des travaux utiles sur d'autres questions touchant à l'informatique au-delà de la cybercriminalité sont en cours au sein des Nations Unies et d'autres instances intergouvernementales et à multiples parties prenantes. Il est important que nos efforts ne fassent

pas double emploi avec ces travaux et n'y portent pas atteinte, afin d'éviter tant de susciter des conflits d'obligations que de nous détourner de notre objectif qui est de produire un instrument ciblé et pratique de lutte contre la cybercriminalité. Nous risquerions dans nos négociations, en essayant de traiter tous les problèmes liés à l'informatique dans cet instrument de justice pénale, de nous enliser dans des débats mal définis et tangentiels qui contribueraient peu à lutter contre la cybercriminalité et qui ne feraient que ralentir notre progression sur la voie de la formulation d'un instrument utile.

Les États Membres devraient en particulier s'abstenir d'aborder les vastes questions relatives à la cybergouvernance ou la cybersécurité dans un instrument consacré à la lutte contre la cybercriminalité. Bien que souvent perçues comme les deux faces d'une même médaille, la lutte contre la cybercriminalité est essentiellement du ressort des autorités gouvernementales, alors que la cybersécurité incombe à toute une gamme d'acteurs publics et privés. Le mandat du Comité spécial est focalisé sur l'élaboration d'un instrument de justice pénale visant à faciliter une riposte internationale aux activités cybercriminelles, ce qui comporte la définition de la conduite criminelle dans le cyberespace et des sanctions frappant cette conduite. Le Comité n'est pas habilité à imposer des normes mondiales relatives aux comportements en ligne non criminels. L'inclusion dans un traité sur la cybercriminalité de notions relatives à la cybergouvernance et à la cybersécurité s'écarterait de l'objectif visé qui est la production d'un instrument rationalisé et efficace qui recueillera un large appui de la part des États Membres.

Ainsi qu'il est réaffirmé dans la résolution 75/282 de l'Assemblée générale, il est essentiel que les négociations devant aboutir à la formulation d'un nouvel instrument de lutte contre la cybercriminalité ne fassent pas obstacle aux mécanismes existants, notamment aux instruments multinationaux et régionaux, qui prévoient déjà toute une panoplie d'outils pour

lutter de manière efficace contre la cybercriminalité[1]. La meilleure façon de forger un consensus en faveur de ce nouvel instrument et d'éviter les questions politiques et sources de division consiste à puiser dans les instruments existants qui ont fait leurs preuves. Nous devrions nous laisser guider par les résultats de la mise en œuvre des autres traités des Nations Unies en matière de justice pénale, tels que la Convention contre la criminalité transnationale organisée. Cette dernière s'est avérée des plus utiles parce qu'elle cible des types fondamentaux d'actes criminels organisés, tout en incluant des dispositions prévoyant une large coopération internationale qui peuvent s'appliquer à tout type d'infraction grave commise par trois personnes ou plus afin d'en tirer un profit. En conséquence, les parties ont eu recours à cette Convention des milliers de fois avec succès, notamment pour combattre des actes criminels tels que l'emploi de logiciels rançonneurs et l'exploitation sexuelle d'enfants.

Les États-Unis soulignent derechef l'importance du maintien d'un processus ouvert, inclusif et transparent qui permettra à tous les États Membres et à toutes les parties prenantes intéressées de négocier de bonne foi en vue de l'adoption de solutions pratiques, bien informées et à base consensuelle, ce qui, estiment-ils, constitue le meilleur moyen d'encourager une large adhésion à un nouvel instrument mondial de lutte contre la cybercriminalité.

Criminalisation des principales infractions cybercriminelles

Avant toute chose, tout nouvel instrument devrait conférer aux autorités nationales le pouvoir de recueillir et d'obtenir des preuves électroniques relatives à tout type d'infraction pénale. Il est impératif que les pays disposent de ce pouvoir pour être en mesure d'enquêter sur

[1] Résolution 75/282, Lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles. Texte adopté par l'Assemblée générale le 26 mai 2021, disponible à l'adresse suivante : https://undocs.org/en/A/RES/75/282.

presque tous les types d'infraction pénale et d'entamer des poursuites judiciaires de manière efficace à leur sujet, car rares sont aujourd'hui les infractions pénales qui sont commises complètement hors du domaine du numérique. L'instrument devrait également permettre une coopération internationale pour partager les preuves électroniques concernant tout type d'infraction, sous réserve d'une disposition souple relative à la double incrimination telle qu'elle figure dans les Conventions des Nations Unies contre la criminalité transnationale organisée et contre la corruption[2].

Il faut en outre, pour que la coopération internationale soit efficace, que les États Membres soient dotés de lois nationales qui érigent en infraction pénale les principales infractions relevant de la cybercriminalité. Il est essentiel de parvenir à une compréhension commune des principales infractions matérielles et d'appuyer les pouvoirs conférés en matière procédurale entre les États Membres pour éviter de créer des zones protégées où se réfugieraient les cybercriminels. Des études de l'ONUDC montrent que les pays conviennent généralement des comportements fondamentaux qu'il faudrait ériger en infractions pénales en vertu de lois spécifiques régissant la cybercriminalité, nombre d'accords multinationaux et de lois pénales nationales contenant des dispositions communes. De manière analogue, il existe une compréhension internationale des pouvoirs procéduraux devant appuyer la conduite d'enquêtes efficaces dans le domaine de la cybercriminalité. En conséquence, les praticiens disposent d'une somme d'expérience diverse accumulée s'étendant sur deux décennies en matière d'enquête dans

[2] Convention des Nations Unies contre la criminalité transnationale organisée : Article 18, paragraphe 9 ; Convention des Nations Unies contre la corruption : Article 46, paragraphe 9. Bien que les dispositions figurant dans les deux Conventions soient légèrement différentes, toutes deux laissent beaucoup de latitude aux États Parties récepteurs pour ce qui est de fournir une assistance, particulièrement en ce qui concerne les mesures coercitives.

le domaine de la cybercriminalité, qui démontre la viabilité pérenne des pouvoirs tant de droit matériel que procéduraux adoptés collectivement pour enquêter dans ce domaine.

Le nouvel instrument de lutte contre la cybercriminalité devrait définir les infractions criminelles auxquelles il s'applique, à savoir les infractions cyberdépendantes, lesquelles sont constituées par des actes criminels ayant pour cible un ordinateur ou des données informatiques, ainsi que certaines infractions commises à l'aide de moyens informatiques, à savoir les infractions criminelles dans la commission desquelles il a été fait usage d'un ordinateur. La première et la principale catégorie d'infractions devant être définies par le nouvel instrument est celle des infractions qui ne peuvent pas être commises sans un mésusage d'ordinateurs ou de réseaux informatiques et qui, par conséquent, n'existaient pas en tant qu'infractions pénales avant l'avènement de l'informatique. Des actes criminels cyberdépendants peuvent être commis entièrement dans le domaine du numérique. S'agissant des infractions pénales cyberdépendantes principales, telles que les attaques par déni de service ou les dégâts causés aux ordinateurs ou aux données, des lois spécifiques en matière informatique sont nécessaires car, dans la plupart des régimes juridiques, les lois pénales font l'objet d'une interprétation stricte et les lois traditionnelles portant sur des notions familières, telles que l'intrusion illicite et le vandalisme, sont souvent inadaptées aux infractions cybercriminelles. En outre, certaines dispositions des codes pénaux applicables aux infractions commises hors de réseaux informatiques peuvent ne pas s'appliquer facilement aux actes commis au moyen d'ordinateurs.

En revanche, nous devrions prendre garde de ne pas traiter les infractions pénales traditionnelles comme des « cyberinfractions » en raison du seul fait qu'il a été fait usage d'un ordinateur dans leur planification ou leur exécution. En dépit du mésusage d'un ordinateur dans la commission d'infractions, certaines conduites coupables peuvent relever de lois générales

parce qu'il n'y a rien de particulier ou d'unique à un système informatique en l'espèce. Inversement, certaines infractions commises à l'aide de moyens informatiques tombent pleinement sous le coup d'un instrument de lutte contre la cybercriminalité lorsque, par exemple, l'emploi d'un ordinateur accroît :

- La portée de l'infraction, faisant par exemple des milliers de victimes ou comportant le vol de millions de données de paiement ;
- La vitesse de l'attaque, du fait qu'un ordinateur augmente exponentiellement la capacité de commettre l'acte criminel ;
- L'ampleur des dommages ou préjudices subis par les victimes ; ou
- L'anonymat de l'auteur des faits.

En appliquant ces concepts, on pourra aussi considérer raisonnablement que certains cas d'infractions criminelles traditionnelles, telles que la fraude et l'exploitation d'enfants, se situent dans le champ de ces négociations. Les États Membres devraient toutefois se montrer judicieux dans la définition de l'ampleur des actes criminels commis à l'aide de moyens informatiques que nous souhaitons viser, de manière à ne pas déformer les concepts de justice pénale établis de longue date. Les lois et instruments pénaux établis ne perdent pas leur applicabilité du simple fait qu'une infraction comporte une « cybercomposante » quelconque.

L'instrument mondial de lutte contre la cybercriminalité devrait également appeler les parties à adopter des mesures législatives qui criminalisent les principales infractions cybercriminelles de manière technologiquement neutre, tout en offrant des garanties procédurales. La criminalisation des infractions de manière technologiquement neutre (c'est-à-dire la criminalisation *de l'activité* affectant la confidentialité, l'intégrité et la disponibilité de

données informatiques au lieu de la criminalisation *de la forme ou de la méthode particulières* utilisées, telles que l'hameçonnage ou le rançongiciel) assure que les dispositions judiciaires matérielles traitent non seulement des technologies et des techniques criminelles actuelles, mais également des technologies et techniques futures. Pour illustrer à quel point la technologie évolue rapidement, on notera que même le Projet d'étude approfondie sur la cybercriminalité de 2013, malgré sa volonté expresse de *profondeur*, manquait de détails sur les technologies ou les techniques qui n'étaient pas d'un usage largement répandu lors de la réalisation de l'étude ou qui ne faisaient qu'émerger, notamment les rançongiciels, l'internet des objets, la cryptomonnaie, et le développement rapide et la prédominance des technologies mobiles. Face à cette problématique, l'une des conclusions et recommandations dont ont convenu les États Membres siégeant au Groupe d'experts de l'ONU a été la suivante : « Les États Membres devraient s'assurer que leurs dispositions législatives résistent à l'épreuve du temps en ce qui concerne de futurs progrès technologiques, en adoptant à cet effet des lois aux formulations technologiquement neutres qui incriminent l'activité jugée illicite et non les moyens employés »[3]. Ceci revêt une importance toute particulière alors que nous tentons de formuler un instrument durable qui permettra de tenir compte de manière appropriée des technologies de demain et de répondre aux besoins des praticiens des forces de l'ordre, tant présents que futurs.

Compte tenu de ces principes, l'instrument mondial de lutte contre la cybercriminalité devrait ériger en infraction criminelle :

[3] UNODC/CCPCJ/EG.4/2021/2, Rapport sur la réunion du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, tenue à Vienne du 6 au 8 avril 2021, disponible à l'adresse suivante : https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2021/Report/V2102595.pdf.

- L’accès illégal, à savoir le fait d’accéder sans autorisation à un ordinateur ou à un système informatique ;
- L’interception illégale, à savoir l’interception illégale en temps réel du contenu de communications ou de données relatives au trafic y afférentes ;
- L’atteinte à l’intégrité des données ou des systèmes, par exemple au moyen de logiciels malveillants, d’attaques par déni de service, de logiciels rançonneurs, ou de suppression ou de modification de données ;
- Le mésusage de dispositifs, à savoir le trafic ou l’utilisation de données de cartes de crédit, de mots de passe et de données personnelles qui permettent d’accéder à des ressources ;
- Les infractions liées aux matériels d’abus sexuels sur enfants ;
- Les infractions liées à la fraude facilitée par l’informatique, à savoir la manipulation de systèmes ou de données informatiques à des fins frauduleuses telles que l’hameçonnage, la compromission d’adresses électroniques commerciales et la fraude aux enchères ;
- Les infractions liées aux atteintes aux droits d’auteur et aux droits connexes ; et
- Les dispositions applicables aux tentatives, à la complicité et au complot.

En outre, le blanchiment des produits de la cybercriminalité devrait lui aussi être érigé en infraction criminelle. Enfin, les personnes morales devraient être passibles de sanctions pénales ou civiles et administratives si elles commettent des cyberinfractions interdites par l’instrument.

Pouvoirs procéduraux relatifs au recueil et au partage des preuves électroniques

En sus de la criminalisation des infractions matérielles, l'instrument mondial de lutte contre la cybercriminalité devrait également prendre en considération la nécessité pour les autorités juridiques nationales de recueillir, de préserver et de partager les preuves électroniques, tout en assurant la régularité de la procédure et la protection des droits de l'homme et des libertés fondamentales. Certains États Membres ont noté que les pouvoirs procéduraux traditionnels prévus par leur législation nationale n'étaient peut-être pas applicables aux données intangibles ou que cette législation risquait de ne pas autoriser un recueil suffisamment rapide des preuves électroniques fugaces. Comme toujours, une législation vétuste ne permettra pas de relever les multiples défis des enquêtes sur les crimes électroniques, notamment face aux technologies novatrices telles que celles des services largement répandus de cryptage et d'informatique en nuage. Il est donc essentiel de conférer des pouvoirs procéduraux spécialisés autorisant le recueil des preuves électroniques, les textes juridiques requis à cette fin devant être rédigés en tenant compte des notions techniques applicables ainsi que des besoins pratiques des enquêteurs criminels. Plus spécifiquement, ces pouvoirs procéduraux devraient autoriser :

- La prompte préservation des données stockées sur ordinateur ;
- Les ordonnances de communication de données informatiques ;
- Les fouilles, les perquisitions et les saisies de données stockées sur ordinateur ;
- Le recueil en temps réel de données relatives au trafic ; et
- Le recueil en temps réel de données relatives au contenu dans les cas d'infraction criminelle grave.

En outre, le nouvel instrument devrait permettre la coopération pour le recueil et l'obtention de preuves électroniques pour tout type d'infraction criminelle et pas seulement pour les cyberinfractions. Les infractions criminelles importantes comportent, dans leur quasi-totalité,

des éléments de preuve électroniques, que ce soit sous la forme de données de téléphonie mobile, de courriel, de données transactionnelles ou d'autres données, qui sont pertinents pour les enquêtes ou les poursuites criminelles. Sur le plan intérieur, les États Membres ont besoin d'un cadre juridique moderne relatif à la preuve, qui autorise l'admissibilité des preuves électroniques dans les enquêtes et les poursuites criminelles, y inclus le partage de telles preuves avec les forces de l'ordre des partenaires internationaux.

Coopération internationale

Au-delà de la législation interne, la bonne coopération internationale dans le domaine de la cybercriminalité fait appel à des activités de coopération officielles fondées sur des traités, telles que l'entraide judiciaire, ainsi qu'à d'autres moyens, tels que la coopération traditionnelle autorisée entre les forces de police. Le nouvel instrument de lutte contre la cybercriminalité devrait s'inspirer, pour accroître la coopération internationale, des outils efficaces prévus par les traités en vigueur, en veillant à ne pas porter atteinte aux instruments existants et à la coopération internationale actuelle en matière de lutte mondiale contre la cybercriminalité. Les dispositions de l'instrument de lutte contre la cybercriminalité ayant trait à la coopération internationale, notamment à l'entraide judiciaire, à l'extradition, au transfert des procédures pénales, à la confiscation des produits de la criminalité, y inclus de la monnaie virtuelle, et à la restitution aux victimes des avoirs confisqués, à la double incrimination ainsi qu'à la coopération entre organes de répression, devraient suivre de près les dispositions des Conventions des Nations Unies contre la criminalité transnationale organisée et contre la corruption, notamment pour ce qui a trait aux garanties et aux protections appropriées prévues par ces instruments, dispositions qui sont appliquées avec succès par la grande majorité des États Membres de l'Organisation. En outre, la disposition relative à l'entraide judiciaire devrait prévoir une large assistance quant à l'obtention

des preuves électroniques concernant les infractions criminelles, qu'un système informatique ait ou non été utilisé dans la commission de ces infractions.

Assistance technique et renforcement des capacités

Les études de l'ONUDC notent que plus de 75 % des pays possèdent, au sein de leurs organismes d'application des lois, une entité spécialement consacrée aux questions touchant à la cybercriminalité et qu'environ 15 % disposent d'un organisme spécialisé de lutte contre la cybercriminalité. Ceci souligne la nature spécialisée des enquêtes sur les cyberinfractions, et notamment la nécessité de formations spécialisées. En outre, la complexité des infractions cybercriminelles et des éléments électroniques ou numériques des infractions traditionnelles s'est notablement accrue, ce qui impose des exigences supplémentaires en matière de formation et d'entretien des compétences des enquêteurs et des experts techniques hautement spécialisés.

L'insuffisance des capacités internes est la principale raison qui fait que les pays peuvent ne pas être en mesure de coopérer de manière efficace sur le plan international. Pour la plupart des pays, les échecs de la coopération internationale ne proviennent pas d'un manque de volonté, mais de limitations de la législation interne ou de l'insuffisance de compétences spécialisées des organismes d'application des lois. De nombreux États Membres ne sont pas dotés de ressources suffisantes en matière de capacités de lutte contre la cybercriminalité ou de traitement des preuves électroniques de la part de leurs forces de l'ordre. Par exemple, au vu de leurs priorités nationales existantes, certains États Membres font face à des difficultés en matière de formation et de rétention d'enquêteurs spécialisés et d'examinateurs judiciaires, ainsi qu'à des pénuries de matériel informatique et de logiciel. En conséquence, il existe un large consensus international sur le fait que l'assistance technique et le renforcement des capacités des organismes d'application des lois, notamment des enquêteurs, des procureurs et des magistrats, constituent

l’exigence la plus urgente pour pouvoir monter une riposte internationale efficace face à la cybercriminalité. En outre, étant donné que les preuves électroniques deviennent des composantes de pratiquement toutes les infractions criminelles, même les agents de la force publique « non spécialisés » devront posséder certaines connaissances de base des enquêtes touchant à l’informatique.

Les dispositions de l’instrument de lutte contre la cybercriminalité relatives à l’assistance technique et au renforcement des capacités devraient concerner notamment :

- Les mesures des États Membres visant à lancer, à développer ou à améliorer des programmes de formation de leurs personnels responsables de la prévention et de la répression de la cybercriminalité.
- La prise en considération par les États Membres, selon leurs capacités, de l’apport mutuel de la plus large assistance technique possible, tout particulièrement au profit des pays en développement et des pays qui peuvent être exposés de manière disproportionnée à des menaces de cybercriminalité, dans leurs plans et programmes respectifs de lutte contre la cybercriminalité.
- L’établissement de mécanismes par lesquels des contributions financières volontaires des États Membres pourraient appuyer la mise en œuvre d’un instrument de lutte contre la cybercriminalité.
- La prise en considération par les États Membres de l’apport de contributions volontaires au Programme mondial contre la cybercriminalité de l’ONUDC et aux initiatives de renforcement des capacités en matière de justice pénale y relatives.

Participation de la société, des entités et des organisations publiques

La lutte contre la cybercriminalité ne peut pas, vu la complexité et la multiplicité des problèmes, être entreprise par le biais d'initiatives cloisonnées. L'instrument de lutte contre la cybercriminalité devrait tenir compte de l'importance d'une participation active tant individuelle que collective, avec un souci d'égalité des sexes, participation qui, par exemple, fera intervenir dans la prévention de la cybercriminalité les organisations non gouvernementales, les organisations de la société civile, les institutions d'enseignement et de recherche et le secteur privé. Une telle participation peut sensibiliser le public aux menaces de la cybercriminalité, faire en sorte que le travail des États Membres soit entrepris dans la transparence, et contribuer à la prise en compte des questions de fond ayant trait à la vie privée, aux libertés civiles et aux droits de l'homme. En outre, l'efficacité de l'instrument dépend des contributions d'individus et d'entités qui possèdent des connaissances spécialisées dans le domaine de la cybercriminalité. Une participation robuste des spécialistes en la matière est en effet essentielle à la bonne mise en œuvre d'un instrument pratique et efficace de lutte contre la cybercriminalité.

Mécanismes de mise en œuvre

Il est encore trop tôt, au stade actuel, pour déterminer si un processus distinct est nécessaire pour examiner la future mise en œuvre de l'instrument et, dans l'affirmative, quelle devrait en être la forme. Il existe divers modèles ayant fait leurs preuves, qui pourront être envisagés. Vu le manque de ressources disponibles pour l'assistance technique, il conviendrait de retenir les méthodes qui font appel à des budgets relativement frugaux pour maximiser les apports de donateurs en faveur de cette assistance. L'une de ces méthodes pourrait consister à autoriser la Commission pour la prévention du crime et la justice pénale, établie par la résolution 1992/1 du Conseil économique et social, à connaître de toutes les questions ayant trait aux objectifs de l'instrument de lutte contre la cybercriminalité. Il existe des précédents convaincants

de ce genre de supervision, dans le cas de la Commission des stupéfiants, qui supervise l'application des trois conventions internationales sur le contrôle des drogues. Ainsi qu'il est noté dans la section *Participation de la société, des entités et des organisations publiques*, il est essentiel que l'on envisage une participation robuste de la société, des entités et des organisations publiques lors de la mise en œuvre de toute initiative découlant d'un instrument. Toutefois, il conviendrait de s'abstenir de débattre des mécanismes de mise en œuvre jusqu'à ce que le champ d'application ait été mieux défini.